



Cisco IOS Security Configuration Guide

Release 12.4T

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco IOS Security Configuration Guide

© 2008 Cisco Systems, Inc. All rights reserved.



About Cisco IOS and Cisco IOS XE Software Documentation

Last updated: August 6, 2008

This document describes the objectives, audience, conventions, and organization used in Cisco IOS and Cisco IOS XE software documentation, collectively referred to in this document as Cisco IOS documentation. Also included are resources for obtaining technical assistance, additional documentation, and other information from Cisco. This document is organized into the following sections:

- [Documentation Objectives, page i](#)
- [Audience, page i](#)
- [Documentation Conventions, page ii](#)
- [Documentation Organization, page iii](#)
- [Additional Resources and Documentation Feedback, page xi](#)

Documentation Objectives

Cisco IOS documentation describes the tasks and commands available to configure and maintain Cisco networking devices.

Audience

The Cisco IOS documentation set is intended for users who configure and maintain Cisco networking devices (such as routers and switches) but who may not be familiar with the configuration and maintenance tasks, the relationship among tasks, or the Cisco IOS commands necessary to perform particular tasks. The Cisco IOS documentation set is also intended for those users experienced with Cisco IOS who need to know about new features, new configuration options, and new software characteristics in the current Cisco IOS release.

Documentation Conventions

In Cisco IOS documentation, the term *router* may be used to refer to various Cisco products; for example, routers, access servers, and switches. These and other networking devices that support Cisco IOS software are shown interchangeably in examples and are used only for illustrative purposes. An example that shows one product does not necessarily mean that other products are not supported.

This section includes the following topics:

- [Typographic Conventions, page ii](#)
- [Command Syntax Conventions, page ii](#)
- [Software Conventions, page iii](#)
- [Reader Alert Conventions, page iii](#)

Typographic Conventions

Cisco IOS documentation uses the following typographic conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination ^D or Ctrl-D means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
<i>string</i>	A string is a nonquoted set of characters shown in italics. For example, when setting a Simple Network Management Protocol (SNMP) community string to <i>public</i> , do not use quotation marks around the string; otherwise, the string will include the quotation marks.

Command Syntax Conventions

Cisco IOS documentation uses the following command syntax conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter as shown.
<i>italic</i>	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional keyword or argument.
	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x y]	Square brackets enclosing keywords or arguments separated by a pipe indicate an optional choice.
{x y}	Braces enclosing keywords or arguments separated by a pipe indicate a required choice.
[x {y z}]	Braces and a pipe within square brackets indicate a required choice within an optional element.

Software Conventions

Cisco IOS uses the following program code conventions:

Convention	Description
Courier font	Courier font is used for information that is displayed on a PC or terminal screen.
Bold Courier font	Bold Courier font indicates text that the user must enter.
< >	Angle brackets enclose text that is not displayed, such as a password. Angle brackets also are used in contexts in which the italic font style is not supported; for example, ASCII text.
!	An exclamation point at the beginning of a line indicates that the text that follows is a comment, not a line of code. An exclamation point is also displayed by Cisco IOS software for certain processes.
[]	Square brackets enclose default responses to system prompts.

Reader Alert Conventions

The Cisco IOS documentation set uses the following conventions for reader alerts:



Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.



Timesaver

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Documentation Organization

This section describes the Cisco IOS documentation set, how it is organized, and how to access it on Cisco.com. Included are lists of configuration guides, command references, and supplementary references and resources that make up the documentation set. The following topics are included:

- [Cisco IOS Documentation Set, page iv](#)
- [Cisco IOS Documentation on Cisco.com, page iv](#)
- [Configuration Guides, Command References, and Supplementary Resources, page v](#)

Cisco IOS Documentation Set

Cisco IOS documentation consists of the following:

- Release notes and caveats provide information about platform, technology, and feature support for a release and describe severity 1 (catastrophic), severity 2 (severe), and severity 3 (moderate) defects in released Cisco IOS code. Review release notes before other documents to learn whether or not updates have been made to a feature.
- Sets of configuration guides and command references organized by technology and published for each standard Cisco IOS release.
 - Configuration guides—Compilations of documents that provide informational and task-oriented descriptions of Cisco IOS features.
 - Command references—Compilations of command pages that provide detailed information about the commands used in the Cisco IOS features and processes that make up the related configuration guides. For each technology, there is a single command reference that covers all Cisco IOS releases and that is updated at each standard release.
- Lists of all the commands in a specific release and all commands that are new, modified, removed, or replaced in the release.
- Command reference book for **debug** commands. Command pages are listed in alphabetical order.
- Reference book for system messages for all Cisco IOS releases.

Cisco IOS Documentation on Cisco.com

The following sections describe the documentation organization and how to access various document types.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

New Features List

The New Features List for each release provides a list of all features in the release with hyperlinks to the feature guides in which they are documented.

Feature Guides

Cisco IOS features are documented in feature guides. Feature guides describe one feature or a group of related features that are supported on many different software releases and platforms. Your Cisco IOS software release or platform may not support all the features documented in a feature guide. See the Feature Information table at the end of the feature guide for information about which features in that guide are supported in your software release.

Configuration Guides

Configuration guides are provided by technology and release and comprise a set of individual feature guides relevant to the release and technology.

Command References

Command reference books describe Cisco IOS commands that are supported in many different software releases and on many different platforms. The books are provided by technology. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/all_release/all_mcl.html.

Cisco IOS Supplementary Documents and Resources

Supplementary documents and resources are listed in [Table 2 on page xi](#).

Configuration Guides, Command References, and Supplementary Resources

[Table 1](#) lists, in alphabetical order, Cisco IOS and Cisco IOS XE software configuration guides and command references, including brief descriptions of the contents of the documents. The Cisco IOS command references are comprehensive, meaning that they include commands for both Cisco IOS software and Cisco IOS XE software, for all releases. The configuration guides and command references support many different software releases and platforms. Your Cisco IOS software release or platform may not support all these technologies.

For additional information about configuring and operating specific networking devices, go to the Product Support area of Cisco.com at <http://www.cisco.com/web/psa/products/index.html>.

[Table 2](#) lists documents and resources that supplement the Cisco IOS software configuration guides and command references. These supplementary resources include release notes and caveats; master command lists; new, modified, removed, and replaced command lists; system messages; and the debug command reference.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS AppleTalk Configuration Guide</i>	AppleTalk protocol.
<i>Cisco IOS XE AppleTalk Configuration Guide</i>	
<i>Cisco IOS AppleTalk Command Reference</i>	
<i>Cisco IOS Asynchronous Transfer Mode Configuration Guide</i>	LAN ATM, multiprotocol over ATM (MPoA), and WAN ATM.
<i>Cisco IOS Asynchronous Transfer Mode Command Reference</i>	

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS Bridging and IBM Networking Configuration Guide</i> <i>Cisco IOS Bridging Command Reference</i> <i>Cisco IOS IBM Networking Command Reference</i>	<ul style="list-style-type: none"> Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRSM). Data-link switching plus (DLSw+), serial tunnel (STUN), block serial tunnel (BSTUN); logical link control, type 2 (LLC2), synchronous data link control (SDLC); IBM Network Media Translation, including Synchronous Data Logical Link Control (SDLLC) and qualified LLC (QLLC); downstream physical unit (DSPU), Systems Network Architecture (SNA) service point, SNA frame relay access, advanced peer-to-peer networking (APPN), native client interface architecture (NCIA) client/server topologies, and IBM Channel Attach.
<i>Cisco IOS Broadband and DSL Configuration Guide</i> <i>Cisco IOS XE Broadband and DSL Configuration Guide</i> <i>Cisco IOS Broadband and DSL Command Reference</i>	Point-to-Point Protocol (PPP) over ATM (PPPoA) and PPP over Ethernet (PPPoE).
<i>Cisco IOS Carrier Ethernet Configuration Guide</i> <i>Cisco IOS Carrier Ethernet Command Reference</i>	Connectivity fault management (CFM), Ethernet Local Management Interface (ELMI), IEEE 802.3ad link bundling, Link Layer Discovery Protocol (LLDP), media endpoint discovery (MED), and operations, administration, and maintenance (OAM).
<i>Cisco IOS Configuration Fundamentals Configuration Guide</i> <i>Cisco IOS XE Configuration Fundamentals Configuration Guide</i> <i>Cisco IOS Configuration Fundamentals Command Reference</i>	Autoinstall, Setup, Cisco IOS command-line interface (CLI), Cisco IOS file system (IFS), Cisco IOS web browser user interface (UI), basic file transfer services, and file management.
<i>Cisco IOS DECnet Configuration Guide</i> <i>Cisco IOS XE DECnet Configuration Guide</i> <i>Cisco IOS DECnet Command Reference</i>	DECnet protocol.
<i>Cisco IOS Dial Technologies Configuration Guide</i> <i>Cisco IOS XE Dial Technologies Configuration Guide</i> <i>Cisco IOS Dial Technologies Command Reference</i>	Asynchronous communications, dial backup, dialer technology, dial-in terminal services and AppleTalk remote access (ARA), large scale dialout, dial-on-demand routing, dialout, modem and resource pooling, ISDN, multilink PPP (MLP), PPP, virtual private dialup network (VPDN).
<i>Cisco IOS Flexible NetFlow Configuration Guide</i> <i>Cisco IOS Flexible NetFlow Command Reference</i>	Flexible NetFlow.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS H.323 Configuration Guide</i>	Gatekeeper enhancements for managed voice services, Gatekeeper Transaction Message Protocol, gateway codec order preservation and shutdown control, H.323 dual tone multifrequency relay, H.323 version 2 enhancements, Network Address Translation (NAT) support of H.323 v2 Registration, Admission, and Status (RAS) protocol, tokenless call authorization, and VoIP gateway trunk and carrier-based routing.
<i>Cisco IOS High Availability Configuration Guide</i> <i>Cisco IOS XE High Availability Configuration Guide</i> <i>Cisco IOS High Availability Command Reference</i>	A variety of High Availability (HA) features and technologies that are available for different network segments (from enterprise access to service provider core) to facilitate creation of end-to-end highly available networks. Cisco IOS HA features and technologies can be categorized in three key areas: system-level resiliency, network-level resiliency, and embedded management for resiliency.
<i>Cisco IOS Integrated Session Border Controller Command Reference</i>	A VoIP-enabled device that is deployed at the edge of networks. An SBC is a toolkit of functions, such as signaling interworking, network hiding, security, and quality of service (QoS).
<i>Cisco IOS Intelligent Service Gateway Configuration Guide</i> <i>Cisco IOS Intelligent Service Gateway Command Reference</i>	Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, session state monitoring.
<i>Cisco IOS Interface and Hardware Component Configuration Guide</i> <i>Cisco IOS XE Interface and Hardware Component Configuration Guide</i> <i>Cisco IOS Interface and Hardware Component Command Reference</i>	LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration.
<i>Cisco IOS IP Addressing Services Configuration Guide</i> <i>Cisco IOS XE Addressing Services Configuration Guide</i> <i>Cisco IOS IP Addressing Services Command Reference</i>	Address Resolution Protocol (ARP), Network Address Translation (NAT), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Next Hop Address Resolution Protocol (NHRP).
<i>Cisco IOS IP Application Services Configuration Guide</i> <i>Cisco IOS XE IP Application Services Configuration Guide</i> <i>Cisco IOS IP Application Services Command Reference</i>	Enhanced Object Tracking (EOT), Gateway Load Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP), IP Services, Server Load Balancing (SLB), Stream Control Transmission Protocol (SCTP), TCP, Web Cache Communication Protocol (WCCP), User Datagram Protocol (UDP), and Virtual Router Redundancy Protocol (VRRP).
<i>Cisco IOS IP Mobility Configuration Guide</i> <i>Cisco IOS IP Mobility Command Reference</i>	Mobile ad hoc networks (MANet) and Cisco mobile networks.
<i>Cisco IOS IP Multicast Configuration Guide</i> <i>Cisco IOS XE IP Multicast Configuration Guide</i> <i>Cisco IOS IP Multicast Command Reference</i>	Protocol Independent Multicast (PIM) sparse mode (PIM-SM), bidirectional PIM (bidir-PIM), Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), Internet Group Management Protocol (IGMP), and Multicast VPN (MVPN).

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS IP Routing Protocols Configuration Guide</i> <i>Cisco IOS XE IP Routing Protocols Configuration Guide</i> <i>Cisco IOS IP Routing Protocols Command Reference</i>	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast, bidirectional forwarding detection (BFD), Enhanced Interior Gateway Routing Protocol (EIGRP), Interior Gateway Routing Protocol (IGRP), Intermediate System-to-Intermediate System (IS-IS), on-demand routing (ODR), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).
<i>Cisco IOS IP SLAs Configuration Guide</i> <i>Cisco IOS XE IP SLAs Configuration Guide</i> <i>Cisco IOS IP SLAs Command Reference</i>	Cisco IOS IP Service Level Agreements (IP SLAs).
<i>Cisco IOS IP Switching Configuration Guide</i> <i>Cisco IOS XE IP Switching Configuration Guide</i> <i>Cisco IOS IP Switching Command Reference</i>	Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS).
<i>Cisco IOS IPv6 Configuration Guide</i> <i>Cisco IOS XE IPv6 Configuration Guide</i> <i>Cisco IOS IPv6 Command Reference</i>	For IPv6 features, protocols, and technologies, go to the IPv6 “Start Here” document at the following URL: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html
<i>Cisco IOS ISO CLNS Configuration Guide</i> <i>Cisco IOS XE ISO CLNS Configuration Guide</i> <i>Cisco IOS ISO CLNS Command Reference</i>	ISO connectionless network service (CLNS).
<i>Cisco IOS LAN Switching Configuration Guide</i> <i>Cisco IOS XE LAN Switching Configuration Guide</i> <i>Cisco IOS LAN Switching Command Reference</i>	VLANs, Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, IEEE 802.1Q encapsulation, and multilayer switching (MLS).
<i>Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide</i> <i>Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference</i>	Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5-generation general packet radio service (GPRS) and 3-generation universal mobile telecommunication system (UMTS) network.
<i>Cisco IOS Mobile Wireless Home Agent Configuration Guide</i> <i>Cisco IOS Mobile Wireless Home Agent Command Reference</i>	Cisco Mobile Wireless Home Agent, an anchor point for mobile terminals for which mobile IP or proxy mobile IP services are provided.
<i>Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide</i> <i>Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference</i>	Cisco Packet Data Serving Node (PDSN), a wireless gateway that is between the mobile infrastructure and standard IP networks and that enables packet data services in a code division multiple access (CDMA) environment.
<i>Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide</i> <i>Cisco IOS Mobile Wireless Radio Access Networking Command Reference</i>	Cisco IOS radio access network products.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS Multiprotocol Label Switching Configuration Guide</i> <i>Cisco IOS XE Multiprotocol Label Switching Configuration Guide</i> <i>Cisco IOS Multiprotocol Label Switching Command Reference</i>	MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS Traffic Engineering (TE), and MPLS Embedded Management (EM) and MIBs.
<i>Cisco IOS Multi-Topology Routing Configuration Guide</i> <i>Cisco IOS Multi-Topology Routing Command Reference</i>	Unicast and multicast topology configurations, traffic classification, routing protocol support, and network management support.
<i>Cisco IOS NetFlow Configuration Guide</i> <i>Cisco IOS XE NetFlow Configuration Guide</i> <i>Cisco IOS NetFlow Command Reference</i>	Network traffic data analysis, aggregation caches, export features.
<i>Cisco IOS Network Management Configuration Guide</i> <i>Cisco IOS XE Network Management Configuration Guide</i> <i>Cisco IOS Network Management Command Reference</i>	Basic system management; system monitoring and logging; troubleshooting, logging, and fault management; Cisco Discovery Protocol; Cisco IOS Scripting with Tool Control Language (Tcl); Cisco networking services (CNS); DistributedDirector; Embedded Event Manager (EEM); Embedded Resource Manager (ERM); Embedded Syslog Manager (ESM); HTTP; Remote Monitoring (RMON); SNMP; and VPN Device Manager Client for Cisco IOS Software (XSM Configuration).
<i>Cisco IOS Novell IPX Configuration Guide</i> <i>Cisco IOS XE Novell IPX Configuration Guide</i> <i>Cisco IOS Novell IPX Command Reference</i>	Novell Internetwork Packet Exchange (IPX) protocol.
<i>Cisco IOS Optimized Edge Routing Configuration Guide</i> <i>Cisco IOS Optimized Edge Routing Command Reference</i>	Optimized edge routing (OER) monitoring, policy configuration, routing control, logging and reporting, and VPN IPsec/generic routing encapsulation (GRE) tunnel interface optimization.
<i>Cisco IOS Quality of Service Solutions Configuration Guide</i> <i>Cisco IOS XE Quality of Service Solutions Configuration Guide</i> <i>Cisco IOS Quality of Service Solutions Command Reference</i>	Class-based weighted fair queuing (CBWFQ), custom queuing, distributed traffic shaping (DTS), generic traffic shaping (GTS), IP- to-ATM class of service (CoS), low latency queuing (LLQ), modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), priority queuing, Security Device Manager (SDM), Multilink PPP (MLPPP) for QoS, header compression, AutoQoS, QoS features for voice, Resource Reservation Protocol (RSVP), weighted fair queuing (WFQ), and weighted random early detection (WRED).
<i>Cisco IOS Security Configuration Guide</i> <i>Cisco IOS XE Security Configuration Guide</i> <i>Cisco IOS Security Command Reference</i>	Access control lists (ACLs), authentication, authorization, and accounting (AAA), firewalls, IP security and encryption, neighbor router authentication, network access security, network data encryption with router authentication, public key infrastructure (PKI), RADIUS, TACACS+, terminal access security, and traffic filters.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS Service Selection Gateway Configuration Guide</i> <i>Cisco IOS Service Selection Gateway Command Reference</i>	Subscriber authentication, service access, and accounting.
<i>Cisco IOS Software Activation Configuration Guide</i> <i>Cisco IOS Software Activation Command Reference</i>	An orchestrated collection of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.
<i>Cisco IOS Software Modularity Installation and Configuration Guide</i> <i>Cisco IOS Software Modularity Command Reference</i>	Installation and basic configuration of software modularity images, including installations on single and dual route processors, installation rollbacks, software modularity binding, software modularity processes and patches.
<i>Cisco IOS Terminal Services Configuration Guide</i> <i>Cisco IOS Terminal Services Command Reference</i> <i>Cisco IOS XE Terminal Services Command Reference</i>	DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD).
<i>Cisco IOS Virtual Switch Command Reference</i>	<p>Virtual switch redundancy, high availability, and packet handling; converting between standalone and virtual switch modes; virtual switch link (VSL); Virtual Switch Link Protocol (VSLP).</p> <p>Note For information about virtual switch configuration, refer to the product-specific software configuration information for the Cisco Catalyst 6500 series switch or for the Metro Ethernet 6500 series switch.</p>
<i>Cisco IOS Voice Configuration Library</i> <i>Cisco IOS Voice Command Reference</i>	Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. The library includes documentation for IP telephony applications.
<i>Cisco IOS VPDN Configuration Guide</i> <i>Cisco IOS XE VPDN Configuration Guide</i> <i>Cisco IOS VPDN Command Reference</i>	Layer 2 Tunneling Protocol (L2TP) dial-out load balancing and redundancy, L2TP extended failover, L2TP security VPDN, multihop by Dialed Number Identification Service (DNIS), timer and retry enhancements for L2TP and Layer 2 Forwarding (L2F), RADIUS Attribute 82: tunnel assignment ID, shell-based authentication of VPDN users, tunnel authentication via RADIUS on tunnel terminator.
<i>Cisco IOS Wide-Area Networking Configuration Guide</i> <i>Cisco IOS XE Wide-Area Networking Configuration Guide</i> <i>Cisco IOS Wide-Area Networking Command Reference</i>	Frame Relay, Layer 2 Tunneling Protocol Version 3 (L2TPv3), Link Access Procedure, Balanced (LAPB), Switched Multimegabit Data Service (SMDS), and X.25.
<i>Cisco IOS Wireless LAN Configuration Guide</i> <i>Cisco IOS Wireless LAN Command Reference</i>	Broadcast key rotation, IEEE 802.11x support, IEEE 802.1x authenticator, IEEE 802.1x local authentication service for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Multiple Basic Service Set ID (BSSID), Wi-Fi Multimedia (WMM) required elements, and Wi-Fi Protected Access (WPA).

Table 2 Cisco IOS Supplementary Documents and Resources

Document Title	Description
<i>Cisco IOS Master Command List, All Releases</i>	Alphabetical list of all the commands documented in all Cisco IOS releases.
<i>Cisco IOS New, Modified, Removed, and Replaced Commands</i>	List of all the new, modified, removed, and replaced commands for a Cisco IOS release.
<i>Cisco IOS Software System Messages</i>	List of Cisco IOS system messages and descriptions. System messages may indicate problems with your system; be informational only; or may help diagnose problems with communications lines, internal hardware, or the system software.
<i>Cisco IOS Debug Command Reference</i>	Alphabetical list of debug commands including brief descriptions of use, command syntax, and usage guidelines.
Release Notes and Caveats	Information about new and changed features, system requirements, and other useful information about specific software releases; information about defects in specific Cisco IOS software releases.
MIBs	Files used for network monitoring. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator at the following URL: http://www.cisco.com/go/mibs
RFCs	Standards documents maintained by the Internet Engineering Task Force (IETF) that Cisco IOS documentation references where applicable. The full text of referenced RFCs may be obtained at the following URL: http://www.rfc-editor.org/

Additional Resources and Documentation Feedback

What's New in Cisco Product Documentation is published monthly and describes all new and revised Cisco technical documentation. The *What's New in Cisco Product Documentation* publication also provides information about obtaining the following resources:

- Technical documentation
- Cisco product security overview
- Product alerts and field notices
- Technical assistance

Cisco IOS technical documentation includes embedded feedback forms where you can rate documents and provide suggestions for improvement. Your feedback helps us improve our documentation.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007–2008 Cisco Systems, Inc. All rights reserved.



Using the Command-Line Interface in Cisco IOS and Cisco IOS XE Software

Last updated: August 6, 2008

This document provides basic information about the command-line interface (CLI) in Cisco IOS and Cisco IOS XE software and how you can use some of the CLI features. This document contains the following sections:

- [Initially Configuring a Device, page i](#)
- [Using the CLI, page ii](#)
- [Saving Changes to a Configuration, page xii](#)
- [Additional Information, page xii](#)

For more information about using the CLI, see the “[Using the Cisco IOS Command-Line Interface](#)” section of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information about the software documentation set, see the “[About Cisco IOS and Cisco IOS XE Software Documentation](#)” document.

Initially Configuring a Device

Initially configuring a device varies by platform. For information about performing an initial configuration, see the hardware installation documentation that is provided with the original packaging of the product or go to the Product Support area of Cisco.com at <http://www.cisco.com/web/psa/products/index.html>.

After you have performed the initial configuration and connected the device to your network, you can configure the device by using the console port or a remote access method, such as Telnet or Secure Shell (SSH), to access the CLI or by using the configuration method provided on the device, such as Security Device Manager.

Changing the Default Settings for a Console or AUX Port

There are only two changes that you can make to a console port and an AUX port:

- Change the port speed with the **config-register 0x** command. Changing the port speed is not recommended. The well-known default speed is 9600.
- Change the behavior of the port; for example, by adding a password or changing the timeout value.

**Note**

The AUX port on the Route Processor (RP) installed in a Cisco ASR1000 series router does not serve any useful customer purpose and should be accessed only under the advisement of a customer support representative.

Using the CLI

This section describes the following topics:

- [Understanding Command Modes, page ii](#)
- [Using the Interactive Help Feature, page v](#)
- [Understanding Command Syntax, page vi](#)
- [Understanding Enable and Enable Secret Passwords, page viii](#)
- [Using the Command History Feature, page viii](#)
- [Abbreviating Commands, page ix](#)
- [Using Aliases for CLI Commands, page ix](#)
- [Using the no and default Forms of Commands, page x](#)
- [Using the debug Command, page x](#)
- [Filtering Output Using Output Modifiers, page x](#)
- [Understanding CLI Error Messages, page xi](#)

Understanding Command Modes

The CLI command mode structure is hierarchical, and each mode supports a set of specific commands. This section describes the most common of the many modes that exist.

[Table 1](#) lists common command modes with associated CLI prompts, access and exit methods, and a brief description of how each mode is used.

Table 1 *CLI Command Modes*

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
User EXEC	Log in.	Router>	Issue the logout or exit command.	<ul style="list-style-type: none"> • Change terminal settings. • Perform basic tests. • Display device status.
Privileged EXEC	From user EXEC mode, issue the enable command.	Router#	Issue the disable command or the exit command to return to user EXEC mode.	<ul style="list-style-type: none"> • Issue show and debug commands. • Copy images to the device. • Reload the device. • Manage device configuration files. • Manage device file systems.
Global configuration	From privileged EXEC mode, issue the configure terminal command.	Router(config)#	Issue the exit command or the end command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, issue the interface command.	Router(config-if)#	Issue the exit command to return to global configuration mode or the end command to return to privileged EXEC mode.	Configure individual interfaces.
Line configuration	From global configuration mode, issue the line vty or line console command.	Router(config-line)#	Issue the exit command to return to global configuration mode or the end command to return to privileged EXEC mode.	Configure individual terminal lines.

Table 1 CLI Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
ROM monitor	From privileged EXEC mode, issue the reload command. Press the Break key during the first 60 seconds while the system is booting.	rommon # > The # symbol represents the line number and increments at each prompt.	Issue the continue command.	<ul style="list-style-type: none"> Run as the default operating mode when a valid image cannot be loaded. Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted. Perform password recovery when a CTRL-Break sequence is issued within 60 seconds of a power-on or reload event.
Diagnostic (available only on the Cisco ASR1000 series router)	<p>The router boots or enters diagnostic mode in the following scenarios. When a Cisco IOS process or processes fail, in most scenarios the router will reload.</p> <ul style="list-style-type: none"> A user-configured access policy was configured using the transport-map command, which directed the user into diagnostic mode. The router was accessed using an RP auxiliary port. A break signal (Ctrl-C, Ctrl-Shift-6, or the send break command) was entered, and the router was configured to enter diagnostic mode when the break signal was received. 	Router(diag)#	<p>If a Cisco IOS process failure is the reason for entering diagnostic mode, the failure must be resolved and the router must be rebooted to exit diagnostic mode.</p> <p>If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or using a method that is configured to connect to the Cisco IOS CLI.</p> <p>If the RP auxiliary port was used to access the router, use another port for access. Accessing the router through the auxiliary port is not useful for customer purposes.</p>	<ul style="list-style-type: none"> Inspect various states on the router, including the Cisco IOS state. Replace or roll back the configuration. Provide methods of restarting the Cisco IOS software or other processes. Reboot hardware, such as the entire router, an RP, an ESP, a SIP, a SPA, or possibly other hardware components. Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.

EXEC commands are not saved when the software reboots. Commands that you issue in a configuration mode can be saved to the startup configuration. If you save the running configuration to the startup configuration, these commands will execute when the software is rebooted. Global configuration mode is the highest level of configuration mode. From global configuration mode, you can enter a variety of other configuration modes, including protocol-specific modes.

ROM monitor mode is a separate mode that is used when the software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode. Use the question symbol (?) to view the commands that you can use while the device is in ROM monitor mode.

```
rommon 1 > ?
alias                set and display aliases command
boot                 boot up an external process
confreg              configuration register utility
cont                 continue executing a downloaded image
context              display the context of a loaded image
cookie               display contents of cookie PROM in hex
.
.
.
rommon 2 >
```

The following example shows how the command prompt changes to indicate a different command mode:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 1/1
Router(config-if)# ethernet
Router(config-line)# exit
Router(config)# end
Router#
```



Note

A keyboard alternative to the **end** command is Ctrl-Z.

Using the Interactive Help Feature

The CLI includes an interactive Help feature. [Table 2](#) describes how to use the Help feature.

Table 2 CLI Interactive Help Commands

Command	Purpose
help	Provides a brief description of the help feature in any command mode.
?	Lists all commands available for a particular command mode.
<i>partial command?</i>	Provides a list of commands that begin with the character string (no space between the command and the question mark).
<i>partial command</i> <Tab>	Completes a partial command name (no space between the command and <Tab>).
<i>command ?</i>	Lists the keywords, arguments, or both associated with the command (space between the command and the question mark).
<i>command keyword ?</i>	Lists the arguments that are associated with the keyword (space between the keyword and the question mark).

The following examples show how to use the help commands:

help

```
Router> help
```

Help may be requested at any point in a command by entering a question mark '?'. If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show pr?'.)

?

```
Router# ?
```

Exec commands:

access-enable	Create a temporary access-List entry
access-profile	Apply user-profile to interface
access-template	Create a temporary access-List entry
alps	ALPS exec commands
archive	manage archive files

```
<snip>
```

partial command?

```
Router(config)# zo?
```

```
zone zone-pair
```

partial command<Tab>

```
Router(config)# we<Tab> webvpn
```

command ?

```
Router(config-if)# pppoe ?
```

enable	Enable pppoe
max-sessions	Maximum PPPOE sessions

command keyword ?

```
Router(config-if)# pppoe enable ?
```

group	attach a BBA group
-------	--------------------

```
<cr>
```

Understanding Command Syntax

Command syntax is the format in which a command should be entered in the CLI. Commands include the name of the command, keywords, and arguments. Keywords are alphanumeric strings that are used literally. Arguments are placeholders for values that a user must supply. Keywords and arguments may be required or optional.

Specific conventions convey information about syntax and command elements. [Table 3](#) describes these conventions.

Table 3 *CLI Syntax Conventions*

Symbol/Text	Function	Notes
< > (angle brackets)	Indicate that the option is an argument.	Sometimes arguments are displayed without angle brackets.
A.B.C.D.	Indicates that you must enter a dotted decimal IP address.	Angle brackets (< >) are not always used to indicate that an IP address is an argument.
WORD (all capital letters)	Indicates that you must enter one word.	Angle brackets (< >) are not always used to indicate that a WORD is an argument.
LINE (all capital letters)	Indicates that you must enter more than one word.	Angle brackets (< >) are not always used to indicate that a LINE is an argument.
<cr> (carriage return)	Indicates the end of the list of available keywords and arguments, and also indicates when keywords and arguments are optional. When <cr> is the only option, you have reached the end of the branch or the end of the command if the command has only one branch.	—

The following examples show syntax conventions:

```

Router(config)# ethernet cfm domain ?
WORD    domain name
Router(config)# ethernet cfm domain dname ?
level
Router(config)# ethernet cfm domain dname level ?
<0-7>  maintenance level number
Router(config)# ethernet cfm domain dname level 7 ?
<cr>
Router(config)# snmp-server file-transfer access-group 10 ?
protocol protocol options
<cr>
Router(config)# logging host ?
Hostname or A.B.C.D  IP address of the syslog server
ipv6                  Configure IPv6 syslog server
Router(config)# snmp-server file-transfer access-group 10 ?
protocol protocol options
<cr>

```

Understanding Enable and Enable Secret Passwords

Some privileged EXEC commands are used for actions that impact the system, and it is recommended that you set a password for these commands to prevent unauthorized use. Two types of passwords, enable (not encrypted) and enable secret (encrypted), can be set. The following commands set these passwords and are issued in global configuration mode:

- **enable** *password*
- **enable secret** *password*

Using an enable secret password is recommended because it is encrypted and more secure than the enable password. When you use an enable secret password, text is encrypted (unreadable) before it is written to the config.text file. When you use an enable password, the text is written as entered (readable) to the config.text file.

Each type of password is case sensitive, can contain from 1 to 25 uppercase and lowercase alphanumeric characters, and can start with a number. Spaces are also valid password characters; for example, “two words” is a valid password. Leading spaces are ignored, but trailing spaces are recognized.

**Note**

Both password commands have numeric keywords that are single integer values. If you choose a number for the first character of your password followed by a space, the system will read the number as if it were the numeric keyword and not as part of your password.

When both passwords are set, the enable secret password takes precedence over the enable password.

To remove a password, use the **no** form of the commands: **no enable** *password* or **no enable secret** *password*.

For more information about password recovery procedures for Cisco products, see http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml.

Using the Command History Feature

The CLI command history feature saves the commands you enter during a session in a command history buffer. The default number of commands saved is 10, but the number is configurable within the range of 0 to 256. This command history feature is particularly useful for recalling long or complex commands.

To change the number of commands saved in the history buffer for a terminal session, issue the **terminal history size** command:

```
Router# terminal history size num
```

A command history buffer is also available in line configuration mode with the same default and configuration options. To set the command history buffer size for a terminal session in line configuration mode, issue the **history** command:

```
Router(config-line)# history [size num]
```

To recall commands from the history buffer, use the following methods:

- Press Ctrl-P or the up arrow key—Recalls commands beginning with the most recent command. Repeat the key sequence to recall successively older commands.

- Press Ctrl-N or the down arrow key—Recalls the most recent commands in the history buffer after they have been recalled using Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.



Note The arrow keys function only on ANSI-compatible terminals such as the VT100.

- Issue the **show history** command in user EXEC or privileged EXEC mode—Lists the most recent commands that you entered. The number of commands that are displayed is determined by the setting of the **terminal history size** and **history** commands.

The CLI command history feature is enabled by default. To disable this feature for a terminal session, issue the **terminal no history** command in user EXEC or privileged EXEC mode or the **no history** command in line configuration mode.

Abbreviating Commands

Typing a complete command name is not always required for the command to execute. The CLI recognizes an abbreviated command when the abbreviation contains enough characters to uniquely identify the command. For example, the **show version** command can be abbreviated as **sh ver**. It cannot be abbreviated as **s ver** because **s** could mean **show**, **set**, or **systat**. The **sh v** abbreviation also is not valid because the **show** command has **vrp** as a keyword in addition to **version**. (Command and keyword examples from Cisco IOS Release 12.4(13)T.)

Using Aliases for CLI Commands

To save time and the repetition of entering the same command multiple times, you can use a command alias. An alias can be configured to do anything that can be done at the command line, but an alias cannot move between modes, type in passwords, or perform any interactive functions.

Table 4 shows the default command aliases.

Table 4 Default Command Aliases

Command Alias	Original Command
h	help
lo	logout
p	ping
s	show
u or un	undebug
w	where

To create a command alias, issue the **alias** command in global configuration mode. The syntax of the command is **alias mode command-alias original-command**. Following are some examples:

- Router(config)# **alias exec prt partition**—privileged EXEC mode
- Router(config)# **alias configure sb source-bridge**—global configuration mode
- Router(config)# **alias interface rl rate-limit**—interface configuration mode

To view both default and user-created aliases, issue the **show alias** command.

For more information about the **alias** command, see

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html.

Using the no and default Forms of Commands

Most configuration commands have a **no** form that is used to reset a command to its default value or disable a feature or function. For example, the **ip routing** command is enabled by default. To disable this command, you would issue the **no ip routing** command. To re-enable IP routing, you would issue the **ip routing** command.

Configuration commands may also have a **default** form, which returns the command settings to their default values. For commands that are disabled by default, using the **default** form has the same effect as using the **no** form of the command. For commands that are enabled by default and have default settings, the **default** form enables the command and returns the settings to their default values.

The **no** and **default** forms of commands are described in the command pages of command references.

Using the debug Command

A **debug** command produces extensive output that helps you troubleshoot problems in your network. These commands are available for many features and functions within Cisco IOS and Cisco IOS XE software. Some **debug** commands are **debug all**, **debug aaa accounting**, and **debug mpls packets**. To use **debug** commands during a Telnet session with a device, you must first enter the **terminal monitor** command. To turn off debugging completely, you must enter the **undebug all** command.

For more information about **debug** commands, see the *Cisco IOS Debug Command Reference* at

http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html.



Caution

Debugging is a high priority and high CPU utilization process that can render your device unusable. Use **debug** commands only to troubleshoot specific problems. The best times to run debugging are during periods of low network traffic and when few users are interacting with the network. Debugging during these periods decreases the likelihood that the **debug** command processing overhead will affect network performance or user access or response times.

Filtering Output Using Output Modifiers

Many commands produce lengthy output that may use several screens to display. Using output modifiers, you can filter this output to show only the information that you want to see.

Three output modifiers are available and are described as follows:

- **begin** *regular expression*—Displays the first line in which a match of the regular expression is found and all lines that follow.
- **include** *regular expression*—Displays all lines in which a match of the regular expression is found.
- **exclude** *regular expression*—Displays all lines except those in which a match of the regular expression is found.

To use one of these output modifiers, type the command followed by the pipe symbol (|), the modifier, and the regular expression that you want to search for or filter. A regular expression is a case-sensitive alphanumeric pattern. It can be a single character or number, a phrase, or a more complex string.

The following example illustrates how to filter output of the **show interface** command to display only lines that include the expression “protocol.”

```
Router# show interface | include protocol

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

Understanding CLI Error Messages

You may encounter some error messages while using the CLI. [Table 5](#) shows the common CLI error messages.

Table 5 Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: “show con”	You did not enter enough characters for the command to be recognized.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Incomplete command.	You did not enter all the keywords or values required by the command.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Invalid input detected at “^” marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The keywords that you are allowed to enter for the command appear.

For more system error messages, see the following documents:

- [Cisco IOS Release 12.2SR System Message Guide](#)
- [Cisco IOS System Messages, Volume 1 of 2](#) (Cisco IOS Release 12.4)
- [Cisco IOS System Messages, Volume 2 of 2](#) (Cisco IOS Release 12.4)

Saving Changes to a Configuration

To save changes that you made to the configuration of a device, you must issue the **copy running-config startup-config** command or the **copy system:running-config nvram:startup-config** command. When you issue these commands, the configuration changes that you made are saved to the startup configuration and saved when the software reloads or power to the device is turned off or interrupted. The following example shows the syntax of the **copy running-config startup-config** command:

```
Router# copy running-config startup-config
Destination filename [startup-config]?
```

You press Enter to accept the startup-config filename (the default), or type a new filename and then press Enter to accept that name. The following output is displayed indicating that the configuration was saved:

```
Building configuration...
[OK]
Router#
```

On most platforms, the configuration is saved to NVRAM. On platforms with a Class A flash file system, the configuration is saved to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

Additional Information

- “Using the Cisco IOS Command-Line Interface” section of the *Cisco IOS Configuration Fundamentals Configuration Guide*:
http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html
or
“Using Cisco IOS XE Software” chapter of the *Cisco ASR1000 Series Aggregation Services Routers Software Configuration Guide*:
http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/using_cli.html
- Cisco Product Support Resources
<http://www.cisco.com/web/psa/products/index.html>
- Support area on Cisco.com (also search for documentation by task or product)
<http://www.cisco.com/en/US/support/index.html>
- *White Paper: Cisco IOS Reference Guide*
http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a008018305e.shtml
- Software Download Center (downloads; tools; licensing, registration, advisory, and general information) (requires Cisco.com User ID and password)
<http://www.cisco.com/kobayashi/sw-center/>
- Error Message Decoder, a tool to help you research and resolve error messages for Cisco IOS software
<http://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi>

- Command Lookup Tool, a tool to help you find detailed descriptions of Cisco IOS commands (requires Cisco.com user ID and password)

<http://tools.cisco.com/Support/CLILookup>

- Output Interpreter, a troubleshooting tool that analyzes command output of supported **show** commands

<https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007–2008 Cisco Systems, Inc. All rights reserved.



Security Overview

This chapter contains the following sections:

- [About This Guide](#)

Preview the topics in this guide.

- [Creating Effective Security Policies](#)

Learn tips and hints for creating a security policy for your organization. A security policy should be finalized and up to date *before* you configure any security features.

- [Identifying Security Risks and Cisco IOS Solutions](#)

Identify common security risks that might be present in your network, and find the right Cisco IOS security feature to prevent security break-ins.

About This Guide

The *Cisco IOS Security Configuration Guide* describes how to configure Cisco IOS security features for your Cisco networking devices. These security features can protect your network against degradation or failure and also against data loss or compromise resulting from intentional attacks and from unintended but damaging mistakes by well-meaning network users.

This guide is divided into seven parts:

- [Authentication, Authorization, and Accounting \(AAA\)](#)
- [Security Server Protocols](#)
- [Traffic Filtering, Firewalls, and Virus Detection](#)
- [IP Security \(IPSec\) and Internet Key Exchange \(IKE\)](#)
- [Public Key Infrastructure \(PKI\)](#)
- [Other Security Features](#)
- [Cisco IOS Secure Infrastructure](#)

[Appendixes](#) follow the seven main divisions.

The following sections briefly describe each of these sections and the appendixes.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Authentication, Authorization, and Accounting (AAA)

This part describes how to configure Cisco's authentication, authorization, and accounting (AAA) paradigm. AAA is an architectural framework for configuring a set of three independent security functions in a consistent, modular manner.

- **Authentication**—Provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol you select, encryption. Authentication is the way a user is identified prior to being allowed access to the network and network services. You configure AAA authentication by defining a named list of authentication methods and then applying that list to various interfaces.
- **Authorization**—Provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet.

Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights, with the appropriate user. AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared with the information contained in a database for a given user, and the result is returned to AAA to determine the user's actual capabilities and restrictions.

- **Accounting**—Provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes. Accounting enables you to track the services users are accessing, as well as the amount of network resources they are consuming.

**Note**

You can configure authentication outside of AAA. However, you must configure AAA if you want to use RADIUS, TACACS+, or Kerberos or if you want to configure a backup authentication method.

Security Server Protocols

In many circumstances, AAA uses security protocols to administer its security functions. If your router or access server is acting as a network access server, AAA is the means through which you establish communication between your network access server and your RADIUS, TACACS+, or Kerberos security server.

The chapters in this part describe how to configure the following security server protocols:

- **RADIUS**—A distributed client/server system implemented through AAA that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.
- **TACACS+**—A security application implemented through AAA that provides centralized validation of users attempting to gain access to a router or network access server. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation. TACACS+ provides for separate and modular authentication, authorization, and accounting facilities.
- **Kerberos**—A secret-key network authentication protocol implemented through AAA that uses the Data Encryption Standard (DES) cryptographic algorithm for encryption and authentication. Kerberos was designed to authenticate requests for network resources. Kerberos is based on the concept of a trusted third party that performs secure verification of users and services. The primary use of Kerberos is to verify that users and the network services they use are really who and what

they claim to be. To accomplish this, a trusted Kerberos server issues tickets to users. These tickets, which have a limited lifespan, are stored in a user's credential cache and can be used in place of the standard username-and-password authentication mechanism.

Traffic Filtering, Firewalls, and Virus Detection

This part describes how to configure your networking devices to filter traffic, function as a firewall, or detect potential viruses.

- Cisco implements traffic filters with access control lists (also called access lists). Access lists determine what traffic is blocked and what traffic is forwarded at router interfaces. Cisco provides both basic and advanced access list capabilities.
 - Basic access lists

An overview of basic access lists is in the chapter “Access Control Lists: Overview and Guidelines.” This chapter describes tips, cautions, considerations, recommendations, and general guidelines for configuring access lists for the various network protocols. You should configure basic access lists for all network protocols that will be routed through your networking device, such as IP, IPX, AppleTalk, and so forth.
 - Advanced access lists

The advanced access list capabilities and configuration are described in the remaining chapters in the “Traffic Filtering, Firewalls, and Virus Detection” part of this document. The advanced access lists provide sophisticated and dynamic traffic filtering capabilities for stronger, more flexible network security.
- Cisco IOS Firewall provides an extensive set of security features, allowing you to configure a simple or elaborate firewall, according to your particular requirements. The following features are key components of Cisco IOS Firewall:
 - Context-based Access Control (CBAC)

CBAC intelligently filters TCP and UDP packets based on application-layer protocol session information. You can configure CBAC to permit specified TCP and UDP traffic through a firewall only when the connection is initiated from within the network you want to protect. CBAC can inspect traffic for sessions that originate from either side of the firewall, and CBAC can be used for intranet, extranet, and Internet perimeters of your network.
 - Cisco IOS Intrusion Prevention System (IPS)

Cisco IOS IPS acts as an in-line intrusion detection sensor, “watching” packets and sessions as they flow through the router and scanning each packet to match any of the Cisco IOS IPS signatures. When Cisco IOS IPS detects suspicious activity, it responds before network security can be compromised and logs the event through Cisco IOS syslog messages or Security Device Event Exchange (SDEE).

Customers can download the Cisco IOS IPS (via a signature detection file [SDF]) to their router from Cisco.com via the VPN and Security Management Solution (VMS) IDS Management Console (MC) 2.3 network management device or via the Cisco Router and Security Device Manager (SDM). Thus VMS IDS MC or SDM can immediately begin scanning for new signatures.
 - Authentication Proxy

The Cisco IOS Firewall authentication proxy feature allows network administrators to apply specific security policies on a per-user basis. Previously, user identity and related authorized access were associated with a user's IP address, or a single security policy had to be applied to

an entire user group or sub network. Now, users can be identified and authorized on the basis of their per-user policy, and access privileges tailored on an individual basis are possible, as opposed to general policy applied across multiple users.

- Port to Application Mapping (PAM)

Port to Application Mapping (PAM) is a feature of Cisco Secure Integrated Software. PAM allows you to customize TCP or UDP port numbers for network services or applications. PAM uses this information to support network environments that run services using ports that are different from the registered or well-known ports associated with an application. For example, the information in the PAM table enables Context-based Access Control (CBAC) supported services to run on non-standard ports.

Firewalls are discussed in the chapters “Cisco IOS Firewall Overview” and “Configuring Context-Based Access Control.”

- Cisco addresses the increased threat and impact of worms and viruses to networked businesses with Cisco Network Admission Control (NAC). NAC enables Cisco routers to enforce access privileges when an endpoint attempts to connect to a network. This access decision is made on the basis of information about the endpoint device, such as its current antivirus state. The antivirus state includes information such as the version of antivirus software, virus definitions, and version of the scan engine.

NAC systems allow noncompliant devices to be denied access, placed in a quarantined area, or given restricted access to computing resources, thus keeping insecure nodes from infecting the network.

IP Security (IPSec) and Internet Key Exchange (IKE)

This section describes how to configure security for VPNs via IPSec and IKE:

- Configuring Security for VPNs with IPSec

This module describes how to configure IPSec. IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec provides data authentication and anti-replay services in addition to data confidentiality services.

- Configuring Internet Key Exchange for IPSec VPNs

This module describes how to configure IKE for use with IPSec VPNs. IKE is a key management protocol standard that is used in conjunction with the IPSec standard. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard.

Public Key Infrastructure (PKI)

This section describes how to implement and manage a Cisco IOS PKI, which provides certificate management to support security protocols such as IPSec, secure shell (SSH), and secure socket layer (SSL). This section is divided into the following modules:

- Cisco IOS PKI Overview: Understanding and Planning a PKI

This module identifies general concepts necessary to understand how a PKI functions.

- Deploying RSA Keys Within a PKI

This module explains how to set up and deploy Rivest, Shamir, and Adelman (RSA) keys within a PKI. An RSA key pair is required before you can obtain a certificate for your router; that is, the end host must generate a pair of RSA keys and exchange the public key with the certification authority (CA) to obtain a certificate and enroll in a PKI.

- **Configuring Revocation and Authorization of Certificates in a PKI**

This module describes how to configure revocation and authorization of certificates in a PKI. After a certificate is validated as a properly signed certificate, it is authorized (via methods such as, certificate maps, PKI-AAA, or a certificate-based ACL) and the revocation status is checked by the issuing CA to ensure that the certificate has not been revoked.

- **Configuring Certificate Enrollment for a PKI**

Certificate enrollment, which is the process of obtaining a certificate from a CA, occurs between the end host requesting the certificate and the CA. Each peer that participates in the PKI must enroll with a CA. This module describes the different methods available for certificate enrollment and describes how to set up each method for a participating PKI peer.

- **Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI**

This module describes how to use SDP in a PKI. SDP is a web-based certificate enrollment interface that can be used to easily deploy PKI between two end devices, such as a Cisco IOS client and a Cisco IOS certificate server. SDP provides a solution for users deploying a large number of peer devices, including certificates and configurations.

- **Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment**

This module describes how to set up and manage a Cisco IOS Certificate Server (CS) for PKI deployment. A CS embeds a simple certificate server, with limited CA functionality, into the Cisco IOS software.

- **Storing PKI Credentials External to the Router**

This module explains how to store RSA keys on device external to the router via a USB eToken. eTokens provide secure configuration distribution and allow users to store PKI credentials, such as RSA keys, for deployment.

Other Security Features

This section describes six security features in the following chapters:

- **Neighbor Router Authentication: Overview and Guidelines**

This chapter briefly describes the security benefits and operation of neighbor router authentication.

When neighbor authentication is configured on a router, the router authenticates its neighbor router before accepting any route updates from that neighbor. This ensures that a router always receives reliable routing update information from a trusted source.

- **Configuring IP Security Options**

This chapter describes how to configure IP Security Options (IPSO) as described in RFC 1108. IPSO is generally used to comply with the security policy of the U.S. government's Department of Defense.

- **Configuring Unicast Reverse Path Forwarding**

This chapter describes the Unicast Reverse Path Forwarding (Unicast RPF) feature, which helps mitigate problems caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address. For example, a number of common types of denial-of-service (DoS) attacks, including Smurf and Tribe Flood

Network (TFN), can take advantage of forged or rapidly changing source IP addresses to allow attackers to thwart efforts to locate or filter the attacks. For Internet service providers (ISPs) that provide public access, Unicast RPF deflects such attacks by forwarding only packets that have source addresses that are valid and consistent with the IP routing table. This action protects the network of the ISP, its customer, and the rest of the Internet.

- **Configuring Secure Shell**

This chapter describes the Secure Shell (SSH) feature. SSH is an application and a protocol that provides a secure replacement to a suite of Unix r-commands such as rsh, rlogin and rcp. (Cisco IOS supports rlogin.) The protocol secures the sessions using standard cryptographic mechanisms, and the application can be used similarly to the Berkeley rexec and rsh tools. There are currently two versions of SSH available: SSH Version 1 and SSH Version 2.

- **Configuring 802.1x Authentication Services**

This section describes how to configure local authentication and VPN access via the Institute of Electrical and Electronics Engineers (IEEE) 802.1X protocol framework.

- **WebVPN**

WebVPN provides end users with unrestricted, secure remote access to enterprise sites without having VPN installed on their end devices. Users can access the enterprise sites from anywhere on the Internet and can access enterprise applications such as e-mail and web browsing.

Cisco IOS Secure Infrastructure

- This section contains features that help users secure their network infrastructure. Some of the available features are as follows: Autosecure (which simplifies the security configuration of a router and hardens the router configuration); Image Verification (which enables routers to automatically detect when the integrity of an image is accidentally corrupted as a result of transmission errors or disk corruption); Role-Based CLI Access (which allows network administrators to exercise better control over access to Cisco networking devices), and “Configuring Security with Passwords, Privilege Levels, and Login Usernames for CLI Sessions on Networking Devices” (which is a guide to implementing a baseline level of security for your networking devices).

Appendixes

The appendixes describe the supported RADIUS attributes and TACACS+ attribute-value pairs as follows:

- **RADIUS Attributes**

RADIUS attributes are used to define specific AAA elements in a user profile, which is stored on the RADIUS daemon. This appendix lists the RADIUS attributes currently supported.

- **TACACS+ Attribute-Value Pairs**

TACACS+ attribute-value pairs are used to define specific AAA elements in a user profile, which is stored on the TACACS+ daemon. This appendix lists the TACACS+ attribute-value pairs currently supported.

Creating Effective Security Policies

An effective security policy works to ensure that your organization's network assets are protected from sabotage and from inappropriate access—both intentional and accidental.

All network security features should be configured in compliance with your organization's security policy. If you do not have a security policy, or if your policy is out of date, you should ensure that the policy is created or updated before you decide how to configure security on your Cisco device.

The following sections provide guidelines to help you create an effective security policy:

- [The Nature of Security Policies](#)
- [Two Levels of Security Policies](#)
- [Tips for Developing an Effective Security Policy](#)

The Nature of Security Policies

You should recognize these aspects of security policies:

- Security policies represent trade-offs.

With all security policies, there is some trade-off between user productivity and security measures that can be restrictive and time consuming. The goal of any security design is to provide maximum security with minimum impact on user access and productivity. Some security measures, such as network data encryption, do not restrict access and productivity. On the other hand, cumbersome or unnecessarily redundant verification and authorization systems can frustrate users and even prevent access to critical network resources.

- Security policies should be determined by business needs.

Business needs should dictate the security policy; a security policy should not determine how a business operates.

- Security policies are living documents.

Because organizations are constantly subject to change, security policies must be systematically updated to reflect new business directions, technological changes, and resource allocations.

Two Levels of Security Policies

You can think of a security policy as having two levels: a requirements level and an implementation level.

- At the requirements level, a policy defines the degree to which your network assets must be protected against intrusion or destruction and also estimates the cost (consequences) of a security breach. For example, the policy could state that only human resources personnel should be able to access personnel records, or that only IS personnel should be able to configure the backbone routers. The policy could also address the consequences of a network outage (due to sabotage), and the consequences of inadvertently making sensitive information public.
- At the implementation level, a policy defines guidelines to implement the requirements-level policy, using specific technology in a predefined way. For example, the implementation-level policy could require access lists to be configured so that only traffic from human resources host computers can access the server containing personnel records.

When creating a policy, define security requirements before defining security implementations so that you do not end up merely justifying particular technical solutions that might not actually be required.

Tips for Developing an Effective Security Policy

To develop an effective security policy, consider the recommendations in the following sections:

- [Identifying Your Network Assets to Protect](#)
- [Determining Points of Risk](#)
- [Limiting the Scope of Access](#)
- [Identifying Assumptions](#)
- [Determining the Cost of Security Measures](#)
- [Considering Human Factors](#)
- [Keeping a Limited Number of Secrets](#)
- [Implementing Pervasive and Scalable Security](#)
- [Understanding Typical Network Functions](#)
- [Remembering Physical Security](#)

Identifying Your Network Assets to Protect

The first step to developing a security policy is to understand and identify your organization's network assets. Network assets include the following:

- Networked hosts (such as PCs; includes the hosts' operating systems, applications, and data)
- Networking devices (such as routers)
- Network data (data that travels across the network)

You must both identify your network's assets and determine the degree to which each of these assets must be protected. For example, one subnetwork of hosts might contain extremely sensitive data that should be protected at all costs, while a different subnetwork of hosts might require only modest protection against security risks because there is less cost involved if the subnetwork is compromised.

Determining Points of Risk

You must understand how potential intruders can enter your organization's network or sabotage network operation. Special areas of consideration are network connections, dial-up access points, and misconfigured hosts. Misconfigured hosts, frequently overlooked as points of network entry, can be systems with unprotected login accounts (guest accounts), employ extensive trust in remote commands (such as rlogin and rsh), have illegal modems attached to them, and use easy-to-break passwords.

Limiting the Scope of Access

Organizations can create multiple barriers within networks, so that unlawful entry to one part of the system does not automatically grant entry to the entire infrastructure. Although maintaining a high level of security for the entire network can be prohibitively expensive (in terms of systems and equipment as well as productivity), you can often provide higher levels of security to the more sensitive areas of your network.

Identifying Assumptions

Every security system has underlying assumptions. For example, an organization might assume that its network is not tapped, that intruders are not very knowledgeable, that intruders are using standard software, or that a locked room is safe. It is important to identify, examine, and justify your assumptions: one hidden assumption is a potential security hole.

Determining the Cost of Security Measures

In general, providing security comes at a cost. This cost can be measured in terms of increased connection times or inconveniences to legitimate users accessing the assets, or in terms of increased network management requirements, and sometimes in terms of actual dollars spent on equipment or software upgrades.

Some security measures inevitably inconvenience some sophisticated users. Security can delay work, create expensive administrative and educational overhead, use significant computing resources, and require dedicated hardware.

When you decide which security measures to implement, you must understand their costs and weigh these against potential benefits. If the security costs are out of proportion to the actual dangers, it is a disservice to the organization to implement them.

Considering Human Factors

If security measures interfere with essential uses of the system, users resist these measures and sometimes even circumvent them. Many security procedures fail because their designers do not take this fact into account. For example, because automatically generated “nonsense” passwords can be difficult to remember, users often write them on the undersides of keyboards. A “secure” door that leads to a system’s only tape drive is sometimes propped open. For convenience, unauthorized modems are often connected to a network to avoid cumbersome dial-in security procedures. To ensure compliance with your security measures, users must be able to get their work done as well as understand and accept the need for security.

Any user can compromise system security to some degree. For example, an intruder might learn passwords by simply calling legitimate users on the telephone claiming to be a system administrator and asking for them. If users understand security issues and understand the reasons for them, they are far less likely to compromise security in this way.

Defining such human factors and any corresponding policies needs to be included as a formal part of your complete security policy.

At a minimum, users must be taught never to release passwords or other secrets over unsecured telephone lines (especially through cordless or cellular telephones) or electronic mail. They should be wary of questions asked by people who call them on the telephone. Some companies have implemented formalized network security training for their employees in which employees are not allowed access to the network until they have completed a formal training program.

Keeping a Limited Number of Secrets

Most security is based on secrets; for example, passwords and encryption keys are secrets. But the more secrets there are, the harder it is to keep all of them. It is prudent, therefore, to design a security policy that relies on a limited number of secrets. Ultimately, the most important secret an organization has is the information that can help someone circumvent its security.

Implementing Pervasive and Scalable Security

Use a systematic approach to security that includes multiple, overlapping security methods.

Almost any change that is made to a system can affect security. This is especially true when new services are created. System administrators, programmers, and users need to consider the security implications of every change they make. Understanding the security implications of a change takes practice; it requires lateral thinking and a willingness to explore every way that a service could potentially be manipulated. The goal of any security policy is to create an environment that is not susceptible to every minor change.

Understanding Typical Network Functions

Understand how your network system normally functions, know what is expected and unexpected behavior, and be familiar with how devices are usually used. This kind of awareness helps the organization detect security problems. Noticing unusual events can help catch intruders before they can damage the system. Software auditing tools can help detect, log, and track unusual events. In addition, an organization should know exactly what software it relies on to provide auditing trails, and a security system should not operate on the assumption that all software is bug free.

Remembering Physical Security

The physical security of your network devices and hosts cannot be neglected. For example, many facilities implement physical security by using security guards, closed circuit television, card-key entry systems, or other means to control physical access to network devices and hosts. Physical access to a computer or router usually gives a sophisticated user complete control over that device. Physical access to a network link usually allows a person to tap into that link, jam it, or inject traffic into it. Software security measures can often be circumvented when access to the hardware is not controlled.

Identifying Security Risks and Cisco IOS Solutions

Cisco IOS software provides a comprehensive set of security features to guard against specific security risks. This section describes a few common security risks that might be present in your network, and describes how to use Cisco IOS software to protect against each of these risks:

- [Preventing Unauthorized Access into Networking Devices](#)
- [Preventing Unauthorized Access into Networks](#)
- [Preventing Network Data Interception](#)
- [Preventing Fraudulent Route Updates](#)

Preventing Unauthorized Access into Networking Devices

If someone were to gain console or terminal access into a networking device, such as a router, switch, or network access server, that person could do significant damage to your network—perhaps by reconfiguring the device, or even by simply viewing the device's configuration information.

Typically, you want administrators to have access to your networking device; you do not want other users on your local-area network or those dialing in to the network to have access to the router.

Users can access Cisco networking devices by dialing in from outside the network through an asynchronous port, connecting from outside the network through a serial port, or connecting via a terminal or workstation from within the local network.

To prevent unauthorized access into a networking device, you should configure one or more of the following security features:

- At a minimum, you should configure passwords and privileges at each networking device for all device lines and ports, as described in the module “Configuring Security with Passwords, Privilege Levels, and Login Usernames for CLI Sessions on Networking Devices.” These passwords are stored on the networking device. When users attempt to access the device through a particular line or port, they must enter the password applied to the line or port before they can access the device.
- For an additional layer of security, you can also configure username/password pairs, stored in a database on the networking device, as described in the module “Configuring Security with Passwords, Privilege Levels, and Login Usernames for CLI Sessions on Networking Devices.” These pairs are assigned to lines or interfaces and authenticate each user before that user can access the device. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username/password pair.
- If you want to use username/password pairs, but you want to store them centrally instead of locally on each individual networking device, you can store them in a database on a security server. Multiple networking devices can then use the same database to obtain user authentication (and, if necessary, authorization) information. Cisco supports a variety of security server protocols, such as RADIUS, TACACS+, and Kerberos. If you decide to use the database on a security server to store login username/password pairs, you must configure your router or access server to support the applicable protocol; in addition, because most supported security protocols must be administered through the AAA security services, you will probably need to enable AAA. For more information about security protocols and AAA, refer to the chapters in the “Authentication, Authorization, and Accounting (AAA)” part of this document.



Note Cisco recommends that, whenever possible, AAA be used to implement authentication.

- If you want to authorize individual users for specific rights and privileges, you can implement AAA’s authorization feature, using a security protocol such as TACACS+ or RADIUS. For more information about security protocol features and AAA, refer to the chapters in the “Authentication, Authorization, and Accounting (AAA)” part of this document.
- If you want to have a backup authentication method, you must configure AAA. AAA allows you to specify the primary method for authenticating users (for example, a username/password database stored on a TACACS+ server) and then specify backup methods (for example, a locally stored username/password database.) The backup method is used if the primary method’s database cannot be accessed by the networking device. To configure AAA, refer to the chapters in the “Authentication, Authorization, and Accounting (AAA)” part of this document. You can configure up to four sequential backup methods.



Note If you do not have backup methods configured, you will be denied access to the device if the username/password database cannot be accessed for any reason.

- If you want to keep an audit trail of user access, configure AAA accounting as described in the chapter “Configuring Accounting.”

Preventing Unauthorized Access into Networks

If someone were to gain unauthorized access to your organization's internal network, that person could cause damage in many ways, perhaps by accessing sensitive files from a host, by planting a virus, or by hindering network performance by flooding your network with illegitimate packets.

This risk can also apply to a person within your network attempting to access another internal network such as a Research and Development subnetwork with sensitive and critical data. That person could intentionally or inadvertently cause damage; for example, that person might access confidential files or tie up a time-critical printer.

To prevent unauthorized access through a networking device into a network, you should configure one or more of these security features:

- **Traffic Filtering**

Cisco uses access lists to filter traffic at networking devices. Basic access lists allow only specified traffic through the device; other traffic is simply dropped. You can specify individual hosts or subnets that should be allowed into the network, and you can specify what type of traffic should be allowed into the network. Basic access lists generally filter traffic based on source and destination addresses, and protocol type of each packet.

Advanced traffic filtering is also available, providing additional filtering capabilities; for example, the Lock-and-Key Security feature requires each user to be authenticated via a username/password before that user's traffic is allowed onto the network.

All the Cisco IOS traffic filtering capabilities are described in the chapters in the "Traffic Filtering, Firewalls, and Virus Detection" part of this document.

- **Authentication**

You can require users to be authenticated before they gain access into a network. When users attempt to access a service or host (such as a web site or file server) within the protected network, they must first enter certain data such as a username and password, and possibly additional information such as their date of birth or mother's maiden name. After successful authentication (depending on the method of authentication), users will be assigned specific privileges, allowing them to access specific network assets. In most cases, this type of authentication would be facilitated by using CHAP or PAP over a serial PPP connection in conjunction with a specific security protocol, such as TACACS+ or RADIUS.

Just as in preventing unauthorized access to specific network devices, you need to decide whether or not you want the authentication database to reside locally or on a separate security server. In this case, a local security database is useful if you have very few routers providing network access. A local security database does not require a separate (and costly) security server. A remote, centralized security database is convenient when you have a large number of routers providing network access because it prevents you from having to update each router with new or changed username authentication and authorization information for potentially hundreds of thousands of dial-in users. A centralized security database also helps establish consistent remote access policies throughout a corporation.

Cisco IOS software supports a variety of authentication methods. Although AAA is the primary (and recommended) method for access control, Cisco IOS software provides additional features for simple access control that are outside the scope of AAA. For more information, refer to the chapter "Configuring Authentication."

Preventing Network Data Interception

When packets travel across a network, they are susceptible to being read, altered, or “hijacked.” (Hijacking occurs when a hostile party intercepts a network traffic session and poses as one of the session endpoints.)

If the data is traveling across an unsecured network such as the Internet, the data is exposed to a fairly significant risk. Sensitive or confidential data could be exposed, critical data could be modified, and communications could be interrupted if data is altered.

To protect data as it travels across a network, configure network data encryption, as described in the chapter “Configuring IPSec Network Security.”

IPSec provides the following network security services. These services are optional. In general, local security policy will dictate the use of one or more of the following services:

- **Data Confidentiality**—The IPSec sender can encrypt packets before transmitting them across a network.
- **Data Integrity**—The IPSec receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.
- **Data Origin Authentication**—The IPSec receiver can authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity service.
- **Anti-Replay**—The IPSec receiver can detect and reject replayed packets.

Cisco IPSec prevents routed traffic from being examined or tampered with while it travels across a network. This feature causes IP packets to be encrypted at a Cisco router, routed across a network as encrypted information, and decrypted at the destination Cisco router. In between the two routers, the packets are in encrypted form and therefore the packets’ contents cannot be read or altered. You define what traffic should be encrypted between the two routers, according to what data is more sensitive or critical.

If you want to protect traffic for protocols other than IP, you can encapsulate those other protocols into IP packets using GRE encapsulation, and then encrypt the IP packets.

Typically, you do not use IPSec for traffic that is routed through networks that you consider secure. Consider using IPSec for traffic that is routed across unsecured networks, such as the Internet, if your organization could be damaged if the traffic is examined or tampered with by unauthorized individuals.

Preventing Fraudulent Route Updates

All routing devices determine where to route individual packets by using information stored in route tables. This route table information is created using route updates obtained from neighboring routers.

If a router receives a fraudulent update, the router could be tricked into forwarding traffic to the wrong destination. This could cause sensitive data to be exposed, or could cause network communications to be interrupted.

To ensure that route updates are received only from known, trusted neighbor routers, configure neighbor router authentication as described in the chapter “Neighbor Router Authentication: Overview and Guidelines.”

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Authentication, Authorization, and Accounting (AAA)



AAA Overview

Access control is the way you control who is allowed access to the network server and what services they are allowed to use once they have access. Authentication, authorization, and accounting (AAA) network security services provide the primary framework through which you set up access control on your router or access server.

In This Chapter

This chapter includes the following sections:

- [About AAA Security Services](#)
- [Where to Begin](#)
- [What to Do Next](#)

About AAA Security Services

AAA is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing the following services:

- **Authentication**—Provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol you select, encryption.

Authentication is the way a user is identified prior to being allowed access to the network and network services. You configure AAA authentication by defining a named list of authentication methods, and then applying that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they will be performed; it must be applied to a specific interface before any of the defined authentication methods will be performed. The only exception is the default method list (which is named “default”). The default method list is automatically applied to all interfaces if no other method list is defined. A defined method list overrides the default method list.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

All authentication methods, except for local, line password, and enable authentication, must be defined through AAA. For information about configuring all authentication methods, including those implemented outside of the AAA security services, refer to the chapter “Configuring Authentication.”

- **Authorization**—Provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet.

AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared to the information contained in a database for a given user and the result is returned to AAA to determine the user’s actual capabilities and restrictions. The database can be located locally on the access server or router or it can be hosted remotely on a RADIUS or TACACS+ security server. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights with the appropriate user. All authorization methods must be defined through AAA.

As with authentication, you configure AAA authorization by defining a named list of authorization methods, and then applying that list to various interfaces. For information about configuring authorization using AAA, refer to the chapter “Configuring Authorization.”

- **Accounting**—Provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

Accounting enables you to track the services users are accessing as well as the amount of network resources they are consuming. When AAA accounting is activated, the network access server reports user activity to the RADIUS or TACACS+ security server (depending on which security method you have implemented) in the form of accounting records. Each accounting record is comprised of accounting AV pairs and is stored on the access control server. This data can then be analyzed for network management, client billing, and/or auditing. All accounting methods must be defined through AAA. As with authentication and authorization, you configure AAA accounting by defining a named list of accounting methods, and then applying that list to various interfaces. For information about configuring accounting using AAA, refer to the chapter “Configuring Accounting.”

In many circumstances, AAA uses protocols such as RADIUS, TACACS+, or Kerberos to administer its security functions. If your router or access server is acting as a network access server, AAA is the means through which you establish communication between your network access server and your RADIUS, TACACS+, or Kerberos security server.

Although AAA is the primary (and recommended) method for access control, Cisco IOS software provides additional features for simple access control that are outside the scope of AAA, such as local username authentication, line password authentication, and enable password authentication. However, these features do not provide the same degree of access control that is possible by using AAA.

This section includes the following sections:

- [Benefits of Using AAA](#)
- [AAA Philosophy](#)
- [Method Lists](#)

Benefits of Using AAA

AAA provides the following benefits:

- Increased flexibility and control of access configuration

- Scalability
- Standardized authentication methods, such as RADIUS, TACACS+, and Kerberos
- Multiple backup systems

**Note**

The deprecated protocols, TACACS and extended TACACS, are not compatible with AAA; if you select these security protocols, you will not be able to take advantage of the AAA security services.

AAA Philosophy

AAA is designed to enable you to dynamically configure the type of authentication and authorization you want on a per-line (per-user) or per-service (for example, IP, IPX, or VPDN) basis. You define the type of authentication and authorization you want by creating method lists, then applying those method lists to specific services or interfaces.

For information about applications that use AAA, such as per-user configuration and virtual profiles, refer to the chapters “Configuring Per-User Configuration” and “Configuring Virtual Profiles” in the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2.

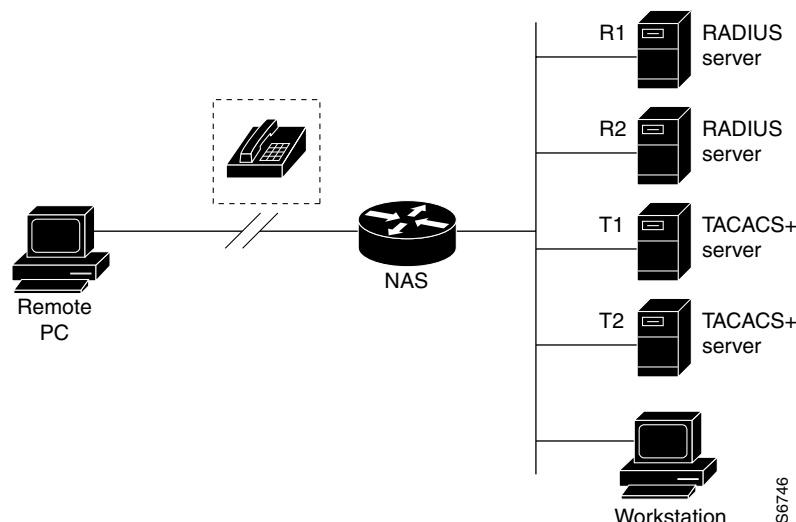
Method Lists

A method list is a sequential list that defines the authentication methods used to authenticate a user. Method lists enable you to designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. Cisco IOS software uses the first method listed to authenticate users; if that method does not respond, Cisco IOS software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or the authentication method list is exhausted, in which case authentication fails.

**Note**

Cisco IOS software attempts authentication with the next listed authentication method only when there is no response from the previous method. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops and no other authentication methods are attempted.

[Figure 1](#) shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers, and T1 and T2 are TACACS+ servers.

Figure 1 Typical AAA Network Configuration

Suppose the system administrator has defined a method list where R1 will be contacted first for authentication information, then R2, T1, T2, and finally the local username database on the access server itself. When a remote user attempts to dial in to the network, the network access server first queries R1 for authentication information. If R1 authenticates the user, it issues a PASS response to the network access server and the user is allowed to access the network. If R1 returns a FAIL response, the user is denied access and the session is terminated. If R1 does not respond, then the network access server processes that as an ERROR and queries R2 for authentication information. This pattern continues through the remaining designated methods until the user is either authenticated or rejected, or until the session is terminated. If all of the authentication methods return errors, the network access server will process the session as a failure, and the session will be terminated.

**Note**

A FAIL response is significantly different from an ERROR. A FAIL means that the user has not met the criteria contained in the applicable authentication database to be successfully authenticated. Authentication ends with a FAIL response. An ERROR means that the security server has not responded to an authentication query. Because of this, no authentication has been attempted. Only when an ERROR is detected will AAA select the next authentication method defined in the authentication method list.

Where to Begin

You must first decide what kind of security solution you want to implement. You need to assess the security risks in your particular network and decide on the appropriate means to prevent unauthorized entry and attack. For more information about assessing your security risks and possible security solutions, refer to the chapter “Security Overview.” Cisco recommends that you use AAA, no matter how minor your security needs might be.

This section includes the following subsections:

- [Overview of the AAA Configuration Process](#)
- [Enabling AAA](#)
- [Disabling AAA](#)

Overview of the AAA Configuration Process

Configuring AAA is relatively simple after you understand the basic process involved. To configure security on a Cisco router or access server using AAA, follow this process:

1. Enable AAA by using the **aaa new-model** global configuration command.
2. If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, TACACS+, or Kerberos.
3. Define the method lists for authentication by using an AAA authentication command.
4. Apply the method lists to a particular interface or line, if required.
5. (Optional) Configure authorization using the **aaa authorization** command.
6. (Optional) Configure accounting using the **aaa accounting** command.

For a complete description of the commands used in this chapter, refer to the chapter “Authentication Commands” of the *Cisco IOS Security Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

Enabling AAA



Note

Before you can use any of the services AAA network security services provide, you must enable AAA.

When you enable AAA, you can no longer access the commands to configure the older protocols, TACACS or extended TACACS. If you decided to use TACACS or extended TACACS in your security solution, do not enable AAA.

To enable AAA, use the following command in global configuration mode:

Command	Purpose
Router (config)# aaa new-model	Enables AAA.

Disabling AAA

You can disable AAA functionality with a single command if you decide that your security needs cannot be met by AAA but can be met by using TACACS, extended TACACS, or a line security method that can be implemented without AAA. To disable AAA, use the following command in global configuration mode:

Command	Purpose
Router(config)# no aaa new-model	Disables AAA.

What to Do Next

Once you have enabled AAA, you are ready to configure the other elements relating to your selected security solution. [Table 3](#) describes AAA configuration tasks and where to find more information.

Table 3 **AAA Access Control Security Solutions Methods**

Task	Chapter in the <i>Cisco IOS Security Configuration Guide</i>
Configuring local login authentication	“Configuring Authentication”
Controlling login using security server authentication	“Configuring Authentication”
Defining method lists for authentication	“Configuring Authentication”
Applying method lists to a particular interface or line	“Configuring Authentication”
Configuring RADIUS security protocol parameters	“Configuring RADIUS”
Configuring TACACS+ security protocol parameters	“Configuring TACACS+”
Configuring Kerberos security protocol parameters	“Configuring Kerberos”
Enabling TACACS+ authorization	“Configuring Authorization”
Enabling RADIUS authorization	“Configuring Authorization”
Viewing supported IETF RADIUS attributes	“RADIUS Attributes” (Appendix)
Viewing supported vendor-specific RADIUS attributes	“RADIUS Attributes” (Appendix)
Viewing supported TACACS+ AV pairs	“TACACS+ AV Pairs” (Appendix)
Enabling accounting	“Configuring Accounting”

If you have elected not to use the AAA security services, see the “Configuring Authentication” chapter for the non-AAA configuration task “Configuring Login Authentication.”

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Authentication



Configuring Authentication

Feature History

Release	Modification
Cisco IOS	For information about feature support in Cisco IOS software, use Cisco Feature Navigator.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Authentication verifies users before they are allowed access to the network and network services. The Cisco IOS software implementation of authentication is divided into two main categories:

- [AAA Authentication Methods Configuration Task List](#)
- [Non-AAA Authentication Methods](#)

Authentication, for the most part, is implemented through the AAA security services. Cisco recommends that, whenever possible, AAA be used to implement authentication.

This chapter describes both AAA and non-AAA authentication methods. For authentication configuration examples, refer to the “[Authentication Examples](#)” section at the end of this chapter. For a complete description of the AAA commands used in this chapter, refer to the “Authentication, Authorization, and Accounting (AAA)” part of the *Cisco IOS Security Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature, or refer to the software release notes for a specific release. For more information, see the section “Identifying Supported Platforms” in the chapter “Using Cisco IOS Software.”

In This Chapter

This chapter contains the following sections:

- [Named Method Lists for Authentication](#)
- [AAA Authentication Methods Configuration Task List](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Non-AAA Authentication Methods](#)
- [Authentication Examples](#)

Named Method Lists for Authentication

To configure AAA authentication, you must first define a named list of authentication methods, and then apply that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they will be performed; it must be applied to a specific interface before any of the defined authentication methods will be performed. The only exception is the default method list (which is named “default”). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

A method list is a sequential list describing the authentication methods to be queried in order to authenticate a user. Method lists enable you to designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. Cisco IOS software uses the first listed method to authenticate users. If that method fails to respond, the Cisco IOS software selects the next authentication method listed in the method list. This process continues until there is successful communication with a listed authentication method, or all methods defined in the method list are exhausted.

It is important to note that the Cisco IOS software attempts authentication with the next listed authentication method only when there is no response from the previous method. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops and no other authentication methods are attempted.

**Note**

Effective with Cisco IOS Release 12.3, the number of AAA method lists that can be configured is 250.

This section contains the following subsections:

- [Method Lists and Server Groups](#)
- [Method List Examples](#)
- [AAA Authentication General Configuration Procedure](#)

Method Lists and Server Groups

A server group is a way to group existing RADIUS or TACACS+ server hosts for use in method lists. [Figure 2](#) shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers and T1 and T2 are TACACS+ servers. R1 and R2 make up the group of RADIUS servers. T1 and T2 make up the group of TACACS+ servers.

Figure 2 **Typical AAA Network Configuration**



Using server groups, you can specify a subset of the configured server hosts and use them for a particular service. For example, server groups allow you to define R1 and R2 as a server group, and define T1 and T2 as a separate server group. For example, you can specify R1 and T1 in the method list for authentication login, while specifying R2 and T2 in the method list for PPP authentication.

Server groups also can include multiple host entries for the same server, as long as each entry has a unique identifier. The combination of an IP address and a UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. In other words, this unique identifier enables RADIUS requests to be sent to different UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, authentication—the second host entry configured acts as failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The RADIUS host entries will be tried in the order in which they are configured.)

For more information about configuring server groups and about configuring server groups based on Dialed Number Identification Service (DNIS) numbers, refer to the “Configuring RADIUS” or “Configuring TACACS+” chapter.

Method List Examples

Suppose the system administrator has decided on a security solution where all interfaces will use the same authentication methods to authenticate PPP connections. In the RADIUS group, R1 is contacted first for authentication information, then if there is no response, R2 is contacted. If R2 does not respond, T1 in the TACACS+ group is contacted; if T1 does not respond, T2 is contacted. If all designated servers fail to respond, authentication falls to the local username database on the access server itself. To implement this solution, the system administrator would create a default method list by entering the following command:

```
aaa authentication ppp default group radius group tacacs+ local
```

In this example, “default” is the name of the method list. The protocols included in this method list are listed after the name, in the order they are to be queried. The default list is automatically applied to all interfaces.

When a remote user attempts to dial in to the network, the network access server first queries R1 for authentication information. If R1 authenticates the user, it issues a PASS response to the network access server and the user is allowed to access the network. If R1 returns a FAIL response, the user is denied access and the session is terminated. If R1 does not respond, then the network access server processes that as an ERROR and queries R2 for authentication information. This pattern would continue through the remaining designated methods until the user is either authenticated or rejected, or until the session is terminated.

It is important to remember that a FAIL response is significantly different from an ERROR. A FAIL means that the user has not met the criteria contained in the applicable authentication database to be successfully authenticated. Authentication ends with a FAIL response. An ERROR means that the security server has not responded to an authentication query. Because of this, no authentication has been attempted. Only when an ERROR is detected will AAA select the next authentication method defined in the authentication method list.

Suppose the system administrator wants to apply a method list only to a particular interface or set of interfaces. In this case, the system administrator creates a named method list and then applies this named list to the applicable interfaces. The following example shows how the system administrator can implement an authentication method that will be applied only to interface 3:

```
aaa authentication ppp default group radius group tacacs+ local
aaa authentication ppp apple group radius group tacacs+ local none
interface async 3
 ppp authentication chap apple
```

In this example, “apple” is the name of the method list, and the protocols included in this method list are listed after the name in the order in which they are to be performed. After the method list has been created, it is applied to the appropriate interface. Note that the method list name (apple) in both the AAA and PPP authentication commands must match.

In the following example, the system administrator uses server groups to specify that only R2 and T2 are valid servers for PPP authentication. To do this, the administrator must define specific server groups whose members are R2 (172.16.2.7) and T2 (172.16.2.77), respectively. In this example, the RADIUS server group “rad2only” is defined as follows using the **aaa group server** command:

```
aaa group server radius rad2only
 server 172.16.2.7
```

The TACACS+ server group “tac2only” is defined as follows using the **aaa group server** command:

```
aaa group server tacacs+ tac2only
 server 172.16.2.77
```

The administrator then applies PPP authentication using the server groups. In this example, the default methods list for PPP authentication follows this order: **group rad2only**, **group tac2only**, and **local**:

```
aaa authentication ppp default group rad2only group tac2only local
```

AAA Authentication General Configuration Procedure

To configure AAA authentication, perform the following tasks:

1. Enable AAA by using the **aaa new-model** global configuration command. For more information about configuring AAA, refer to the chapter “AAA Overview”.
2. Configure security protocol parameters, such as RADIUS, TACACS+, or Kerberos if you are using a security server. For more information about RADIUS, refer to the chapter “Configuring RADIUS”. For more information about TACACS+, refer to the chapter “Configuring TACACS+”. For more information about Kerberos, refer to the chapter “Configuring Kerberos”.

3. Define the method lists for authentication by using an AAA authentication command.
4. Apply the method lists to a particular interface or line, if required.

AAA Authentication Methods Configuration Task List

This section discusses the following AAA authentication methods:

- [Configuring Login Authentication Using AAA](#)
- [Configuring PPP Authentication Using AAA](#)
- [Configuring AAA Scalability for PPP Requests](#)
- [Configuring ARAP Authentication Using AAA](#)
- [Configuring NASI Authentication Using AAA](#)
- [Specifying the Amount of Time for Login Input](#)
- [Enabling Password Protection at the Privileged Level](#)
- [Changing the Text Displayed at the Password Prompt](#)
- [Configuring Message Banners for AAA Authentication](#)
- [Configuring AAA Packet of Disconnect](#)
- [Enabling Double Authentication](#)
- [Enabling Automated Double Authentication](#)



Note

AAA features are not available for use until you enable AAA globally by issuing the **aaa new-model** command. For more information about enabling AAA, refer to the “AAA Overview” chapter.

For authentication configuration examples using the commands in this chapter, refer to the section “[Authentication Examples](#)” at the end of the this chapter.

Configuring Login Authentication Using AAA

The AAA security services facilitate a variety of login authentication methods. Use the **aaa authentication login** command to enable AAA authentication no matter which of the supported login authentication methods you decide to use. With the **aaa authentication login** command, you create one or more lists of authentication methods that are tried at login. These lists are applied using the **login authentication** line configuration command.

To configure login authentication by using AAA, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# aaa new-model	Enables AAA globally.
Step 2	Router(config)# aaa authentication login {default list-name} method1 [method2...]	Creates a local authentication list.

	Command	Purpose
Step 3	Router(config)# line [aux console tty vty] line-number [ending-line-number]	Enters line configuration mode for the lines to which you want to apply the authentication list.
Step 4	Router(config-line)# login authentication { default <i>list-name</i> }	Applies the authentication list to a line or set of lines.

The *list-name* is a character string used to name the list you are creating. The method argument refers to the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line.

For example, to specify that authentication should succeed even if (in this example) the TACACS+ server returns an error, enter the following command:

```
aaa authentication login default group tacacs+ none
```



Note

Because the **none** keyword enables *any* user logging in to successfully authenticate, it should be used only as a backup method of authentication.

To create a default list that is used when a named list is *not* specified in the **login authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces.

For example, to specify RADIUS as the default method for user authentication during login, enter the following command:

```
aaa authentication login default group radius
```

Table 4 lists the supported login authentication methods.

Table 4 AAA Authentication Login Methods

Keyword	Description
enable	Uses the enable password for authentication.
krb5	Uses Kerberos 5 for authentication.
krb5-telnet	Uses Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router. If selected, this keyword must be listed as the first method in the method list.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the aaa group server radius or aaa group server tacacs+ command.

**Note**

The **login** command only changes username and privilege level but does not execute a shell; therefore autocommands will not be executed. To execute autocommands under this circumstance, you need to establish a Telnet session back into the router (loop-back). Make sure that the router has been configured for secure Telnet sessions if you choose to implement autocommands this way.

This section includes the following sections:

- [Login Authentication Using Enable Password](#)
- [Login Authentication Using Kerberos](#)
- [Login Authentication Using Line Password](#)
- [Login Authentication Using Local Password](#)
- [Login Authentication Using Group RADIUS](#)
- [Login Authentication Using Group TACACS+](#)
- [Login Authentication Using group group-name](#)

Login Authentication Using Enable Password

Use the **aaa authentication login** command with the **enable method** keyword to specify the enable password as the login authentication method. For example, to specify the enable password as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication login default enable
```

Before you can use the enable password as the login authentication method, you need to define the enable password. For more information about defining enable passwords, refer to the chapter “Configuring Passwords and Privileges.”

Login Authentication Using Kerberos

Authentication via Kerberos is different from most other authentication methods: the user’s password is never sent to the remote access server. Remote users logging in to the network are prompted for a username. If the key distribution center (KDC) has an entry for that user, it creates an encrypted ticket granting ticket (TGT) with the password for that user and sends it back to the router. The user is then prompted for a password, and the router attempts to decrypt the TGT with that password. If it succeeds, the user is authenticated and the TGT is stored in the user’s credential cache on the router.

While **krb5** does use the KINIT program, a user does not need to run the KINIT program to get a TGT to authenticate to the router. This is because KINIT has been integrated into the login procedure in the Cisco IOS implementation of Kerberos.

Use the **aaa authentication login** command with the **krb5 method** keyword to specify Kerberos as the login authentication method. For example, to specify Kerberos as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication login default krb5
```

Before you can use Kerberos as the login authentication method, you need to enable communication with the Kerberos security server. For more information about establishing communication with a Kerberos server, refer to the chapter “Configuring Kerberos.”

Login Authentication Using Line Password

Use the **aaa authentication login** command with the **line method** keyword to specify the line password as the login authentication method. For example, to specify the line password as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication login default line
```

Before you can use a line password as the login authentication method, you need to define a line password. For more information about defining line passwords, refer to the section [“Configuring Line Password Protection”](#) in this chapter.

Login Authentication Using Local Password

Use the **aaa authentication login** command with the **local method** keyword to specify that the Cisco router or access server will use the local username database for authentication. For example, to specify the local username database as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication login default local
```

For information about adding users into the local username database, refer to the section [“Establishing Username Authentication”](#) in this chapter.

Login Authentication Using Group RADIUS

Use the **aaa authentication login** command with the **group radius method** to specify RADIUS as the login authentication method. For example, to specify RADIUS as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication login default group radius
```

Before you can use RADIUS as the login authentication method, you need to enable communication with the RADIUS security server. For more information about establishing communication with a RADIUS server, refer to the chapter “Configuring RADIUS.”

Configuring RADIUS Attribute 8 in Access Requests

Once you have used the **aaa authentication login** command to specify RADIUS and your login host has been configured to request its IP address from the NAS, you can send attribute 8 (Framed-IP-Address) in access-request packets by using the **radius-server attribute 8 include-in-access-req** command in global configuration mode. This command makes it possible for a NAS to provide the RADIUS server with a hint of the user IP address in advance of user authentication. For more information about attribute 8, refer to the appendix “RADIUS Attributes” at the end of the book.

Login Authentication Using Group TACACS+

Use the **aaa authentication login** command with the **group tacacs+ method** to specify TACACS+ as the login authentication method. For example, to specify TACACS+ as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication login default group tacacs+
```


Before you can use TACACS+ as the login authentication method, you need to enable communication with the TACACS+ security server. For more information about establishing communication with a TACACS+ server, refer to the chapter “Configuring TACACS+.”

Login Authentication Using group group-name

Use the **aaa authentication login** command with the **group group-name** method to specify a subset of RADIUS or TACACS+ servers to use as the login authentication method. To specify and define the group name and the members of the group, use the **aaa group server** command. For example, use the **aaa group server** command to first define the members of **group loginrad**:

```
aaa group server radius loginrad
  server 172.16.2.3
  server 172.16.2.17
  server 172.16.2.32
```

This command specifies RADIUS servers 172.16.2.3, 172.16.2.17, and 172.16.2.32 as members of the group *loginrad*.

To specify **group loginrad** as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication login default group loginrad
```

Before you can use a group name as the login authentication method, you need to enable communication with the RADIUS or TACACS+ security server. For more information about establishing communication with a RADIUS server, refer to the chapter “Configuring RADIUS.” For more information about establishing communication with a TACACS+ server, refer to the chapter “Configuring TACACS+.”

Configuring PPP Authentication Using AAA

Many users access network access servers through dialup via async or ISDN. Dialup via async or ISDN bypasses the CLI completely; instead, a network protocol (such as PPP or ARA) starts as soon as the connection is established.

The AAA security services facilitate a variety of authentication methods for use on serial interfaces running PPP. Use the **aaa authentication ppp** command to enable AAA authentication no matter which of the supported PPP authentication methods you decide to use.

To configure AAA authentication methods for serial lines using PPP, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# aaa new-model	Enables AAA globally.
Step 2	Router(config)# aaa authentication ppp {default list-name} method1 [method2...]	Creates a local authentication list.

	Command	Purpose
Step 3	Router(config)# interface <i>interface-type</i> <i>interface-number</i>	Enters interface configuration mode for the interface to which you want to apply the authentication list.
Step 4	Router(config-if)# ppp authentication { <i>protocol1</i> [<i>protocol2</i> ...]} [if-needed] [default <i>list-name</i>] [callin] [one-time] [optional]	Applies the authentication list to a line or set of lines. In this command, <i>protocol1</i> and <i>protocol2</i> represent the following protocols: CHAP, MS-CHAP, and PAP. PPP authentication is attempted first using the first authentication method, specified by <i>protocol1</i> . If <i>protocol1</i> is unable to establish authentication, the next configured protocol is used to negotiate authentication.

With the **aaa authentication ppp** command, you create one or more lists of authentication methods that are tried when a user tries to authenticate via PPP. These lists are applied using the **ppp authentication** line configuration command.

To create a default list that is used when a named list is *not* specified in the **ppp authentication** command, use the **default** keyword followed by the methods you want used in default situations.

For example, to specify the local username database as the default method for user authentication, enter the following command:

```
aaa authentication ppp default local
```

The *list-name* is any character string used to name the list you are creating. The method argument refers to the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line.

For example, to specify that authentication should succeed even if (in this example) the TACACS+ server returns an error, enter the following command:

```
aaa authentication ppp default group tacacs+ none
```



Note

Because **none** allows all users logging in to authenticate successfully, it should be used as a backup method of authentication.

Table 5 lists the supported login authentication methods.

Table 5 AAA Authentication PPP Methods

Keyword	Description
if-needed	Does not authenticate if user has already been authenticated on a TTY line.
krb5	Uses Kerberos 5 for authentication (can only be used for PAP authentication).
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.
group radius	Uses the list of all RADIUS servers for authentication.

Table 5 **AAA Authentication PPP Methods (continued)**

Keyword	Description
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the aaa group server radius or aaa group server tacacs+ command.

This section includes the following sections:

- [PPP Authentication Using Kerberos](#)
- [PPP Authentication Using Local Password](#)
- [PPP Authentication Using Group RADIUS](#)
- [PPP Authentication Using Group TACACS+](#)
- [PPP Authentication Using group group-name](#)

PPP Authentication Using Kerberos

Use the **aaa authentication ppp** command with the **krb5 method** keyword to specify Kerberos as the authentication method for use on interfaces running PPP. For example, to specify Kerberos as the method of user authentication when no other method list has been defined, enter the following command:

```
aaa authentication ppp default krb5
```

Before you can use Kerberos as the PPP authentication method, you need to enable communication with the Kerberos security server. For more information about establishing communication with a Kerberos server, refer to the chapter “Configuring Kerberos”.

**Note**

Kerberos login authentication works only with PPP PAP authentication.

PPP Authentication Using Local Password

Use the **aaa authentication ppp** command with the *method* keyword **local** to specify that the Cisco router or access server will use the local username database for authentication. For example, to specify the local username database as the method of authentication for use on lines running PPP when no other method list has been defined, enter the following command:

```
aaa authentication ppp default local
```

For information about adding users into the local username database, refer to the section “[Establishing Username Authentication](#)” in this chapter.

PPP Authentication Using Group RADIUS

Use the **aaa authentication ppp** command with the **group radius method** to specify RADIUS as the login authentication method. For example, to specify RADIUS as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication ppp default group radius
```

Before you can use RADIUS as the PPP authentication method, you need to enable communication with the RADIUS security server. For more information about establishing communication with a RADIUS server, refer to the chapter “Configuring RADIUS.”

Configuring RADIUS Attribute 44 in Access Requests

Once you have used the **aaa authentication ppp** command with the **group radius method** to specify RADIUS as the login authentication method, you can configure your router to send attribute 44 (Acct-Section-ID) in access-request packets by using the **radius-server attribute 44 include-in-access-req** command in global configuration mode. This command allows the RADIUS daemon to track a call from the beginning of the call to the end of the call. For more information on attribute 44, refer to the appendix “RADIUS Attributes” at the end of the book.

PPP Authentication Using Group TACACS+

Use the **aaa authentication ppp** command with the **group tacacs+ method** to specify TACACS+ as the login authentication method. For example, to specify TACACS+ as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication ppp default group tacacs+
```

Before you can use TACACS+ as the PPP authentication method, you need to enable communication with the TACACS+ security server. For more information about establishing communication with a TACACS+ server, refer to the chapter “Configuring TACACS+.”

PPP Authentication Using group group-name

Use the **aaa authentication ppp** command with the **group group-name method** to specify a subset of RADIUS or TACACS+ servers to use as the login authentication method. To specify and define the group name and the members of the group, use the **aaa group server** command. For example, use the **aaa group server** command to first define the members of **group ppprad**:

```
aaa group server radius ppprad
server 172.16.2.3
server 172.16.2.17
server 172.16.2.32
```

This command specifies RADIUS servers 172.16.2.3, 172.16.2.17, and 172.16.2.32 as members of the group *ppprad*.

To specify **group ppprad** as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication ppp default group ppprad
```

Before you can use a group name as the PPP authentication method, you need to enable communication with the RADIUS or TACACS+ security server. For more information about establishing communication with a RADIUS server, refer to the chapter “Configuring RADIUS”. For more information about establishing communication with a TACACS+ server, refer to the chapter “Configuring TACACS+.”

Configuring AAA Scalability for PPP Requests

You can configure and monitor the number of background processes allocated by the PPP manager in the network access server (NAS) to deal with AAA authentication and authorization requests. In previous Cisco IOS releases, only one background process was allocated to handle all AAA requests for PPP. This meant that parallelism in AAA servers could not be fully exploited. The AAA Scalability feature enables you to configure the number of processes used to handle AAA requests for PPP, thus increasing the number of users that can be simultaneously authenticated or authorized.

To allocate a specific number of background processes to handle AAA requests for PPP, use the following command in global configuration mode:

Command	Purpose
Router(config)# aaa processes <i>number</i>	Allocates a specific number of background processes to handle AAA authentication and authorization requests for PPP.

The argument *number* defines the number of background processes earmarked to process AAA authentication and authorization requests for PPP and can be configured for any value from 1 to 2147483647. Because of the way the PPP manager handles requests for PPP, this argument also defines the number of new users that can be simultaneously authenticated. This argument can be increased or decreased at any time.



Note

Allocating additional background processes can be expensive. You should configure the minimum number of background processes capable of handling the AAA requests for PPP.

Configuring ARAP Authentication Using AAA

With the **aaa authentication arap** command, you create one or more lists of authentication methods that are tried when AppleTalk Remote Access Protocol (ARAP) users attempt to log in to the router. These lists are used with the **arap authentication** line configuration command.

Use the following commands starting in global configuration mode:

	Command	Purpose
Step 1	Router(config)# aaa new-model	Enables AAA globally.
Step 2	Router(config)# aaa authentication arap { default <i>list-name</i> } <i>method1</i> [<i>method2...</i>]	Enables authentication for ARAP users.
Step 3	Router(config)# line <i>number</i>	(Optional) Changes to line configuration mode.
Step 4	Router(config-line)# autoselect arap	(Optional) Enables autoselection of ARAP.
Step 5	Router(config-line)# autoselect during-login	(Optional) Starts the ARAP session automatically at user login.
Step 6	Router(config-line)# arap authentication <i>list-name</i>	(Optional—not needed if default is used in the aaa authentication arap command) Enables TACACS+ authentication for ARAP on a line.

The *list-name* is any character string used to name the list you are creating. The method argument refers to the actual list of methods the authentication algorithm tries, in the sequence entered.

To create a default list that is used when a named list is *not* specified in the **arap authentication** command, use the **default** keyword followed by the methods you want to be used in default situations.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line.

**Note**

Because **none** allows all users logging in to authenticate successfully, it should be used as a backup method of authentication.

Table 6 lists the supported login authentication methods.

Table 6 **AAA Authentication ARAP Methods**

Keyword	Description
auth-guest	Allows guest logins only if the user has already logged in to EXEC.
guest	Allows guest logins.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the aaa group server radius or aaa group server tacacs+ command.

For example, to create a default AAA authentication method list used with ARAP, enter the following command:

```
aaa authentication arap default if-needed none
```

To create the same authentication method list for ARAP but name the list *MIS-access*, enter the following command:

```
aaa authentication arap MIS-access if-needed none
```

This section includes the following sections:

- [ARAP Authentication Allowing Authorized Guest Logins](#)
- [ARAP Authentication Allowing Guest Logins](#)
- [ARAP Authentication Using Line Password](#)
- [ARAP Authentication Using Local Password](#)
- [ARAP Authentication Using Group RADIUS](#)
- [ARAP Authentication Using Group TACACS+](#)
- [ARAP Authentication Using Group group-name](#)

ARAP Authentication Allowing Authorized Guest Logins

Use the **aaa authentication arap** command with the **auth-guest** keyword to allow guest logins only if the user has already successfully logged in to the EXEC. This method must be the first listed in the ARAP authentication method list but it can be followed by other methods if it does not succeed. For example, to allow all authorized guest logins—meaning logins by users who have already successfully logged in to the EXEC—as the default method of authentication, using RADIUS only if that method fails, enter the following command:

```
aaa authentication arap default auth-guest group radius
```

For more information about ARAP authorized guest logins, refer to the chapter “Configuring AppleTalk” in the *Cisco IOS AppleTalk and Novell IPX Configuration Guide*.



Note

By default, guest logins through ARAP are disabled when you initialize AAA. To allow guest logins, you must use the **aaa authentication arap** command with either the **guest** or the **auth-guest** keyword.

ARAP Authentication Allowing Guest Logins

Use the **aaa authentication arap** command with the **guest** keyword to allow guest logins. This method must be the first listed in the ARAP authentication method list but it can be followed by other methods if it does not succeed. For example, to allow all guest logins as the default method of authentication, using RADIUS only if that method fails, enter the following command:

```
aaa authentication arap default guest group radius
```

For more information about ARAP guest logins, refer to the chapter “Configuring AppleTalk” in the *Cisco IOS AppleTalk and Novell IPX Configuration Guide*.

ARAP Authentication Using Line Password

Use the **aaa authentication arap** command with the *method* keyword **line** to specify the line password as the authentication method. For example, to specify the line password as the method of ARAP user authentication when no other method list has been defined, enter the following command:

```
aaa authentication arap default line
```

Before you can use a line password as the ARAP authentication method, you need to define a line password. For more information about defining line passwords, refer to the section “[Configuring Line Password Protection](#)” in this chapter.

ARAP Authentication Using Local Password

Use the **aaa authentication arap** command with the *method* keyword **local** to specify that the Cisco router or access server will use the local username database for authentication. For example, to specify the local username database as the method of ARAP user authentication when no other method list has been defined, enter the following command:

```
aaa authentication arap default local
```

For information about adding users to the local username database, refer to the section “[Establishing Username Authentication](#)” in this chapter.

ARAP Authentication Using Group RADIUS

Use the **aaa authentication arap** command with the **group radius** *method* to specify RADIUS as the ARAP authentication method. For example, to specify RADIUS as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication arap default group radius
```

Before you can use RADIUS as the ARAP authentication method, you need to enable communication with the RADIUS security server. For more information about establishing communication with a RADIUS server, refer to the chapter “Configuring RADIUS.”

ARAP Authentication Using Group TACACS+

Use the **aaa authentication arap** command with the **group tacacs+** *method* to specify TACACS+ as the ARAP authentication method. For example, to specify TACACS+ as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication arap default group tacacs+
```

Before you can use TACACS+ as the ARAP authentication method, you need to enable communication with the TACACS+ security server. For more information about establishing communication with a TACACS+ server, refer to the chapter “Configuring TACACS+.”

ARAP Authentication Using Group group-name

Use the **aaa authentication arap** command with the **group group-name** *method* to specify a subset of RADIUS or TACACS+ servers to use as the ARAP authentication method. To specify and define the group name and the members of the group, use the **aaa group server** command. For example, use the **aaa group server** command to first define the members of **group araprad**:

```
aaa group server radius araprad
server 172.16.2.3
server 172.16.2.17
server 172.16.2.32
```

This command specifies RADIUS servers 172.16.2.3, 172.16.2.17, and 172.16.2.32 as members of the group *araprad*.

To specify **group araprad** as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication arap default group araprad
```

Before you can use a group name as the ARAP authentication method, you need to enable communication with the RADIUS or TACACS+ security server. For more information about establishing communication with a RADIUS server, refer to the chapter “Configuring RADIUS.” For more information about establishing communication with a TACACS+ server, refer to the chapter “Configuring TACACS+.”

Configuring NASL Authentication Using AAA

With the **aaa authentication nasi** command, you create one or more lists of authentication methods that are tried when NetWare Asynchronous Services Interface (NASI) users attempt to log in to the router. These lists are used with the **nasi authentication** line configuration command.

To configure NASI authentication using AAA, use the following commands starting in global configuration mode:

	Command	Purpose
Step 1	Router(config)# aaa new-model	Enables AAA globally.
Step 2	Router(config)# aaa authentication nasi { default <i>list-name</i> } <i>method1</i> [<i>method2...</i>]	Enables authentication for NASI users.
Step 3	Router(config)# line <i>number</i>	(Optional—not needed if default is used in the aaa authentication nasi command) Enters line configuration mode.
Step 4	Router(config-line)# nasi authentication <i>list-name</i>	(Optional—not needed if default is used in the aaa authentication nasi command) Enables authentication for NASI on a line.

The *list-name* is any character string used to name the list you are creating. The method argument refers to the actual list of methods the authentication algorithm tries, in the sequence entered.

To create a default list that is used when a named list is *not* specified in the **aaa authentication nasi** command, use the **default** keyword followed by the methods you want to be used in default situations.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line.



Note

Because **none** allows all users logging in to authenticate successfully, it should be used as a backup method of authentication.

Table 7 lists the supported NASI authentication methods.

Table 7 AAA Authentication NASI Methods

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the aaa group server radius or aaa group server tacacs+ command.

This section includes the following sections:

- [NASI Authentication Using Enable Password](#)
- [NASI Authentication Using Line Password](#)
- [NASI Authentication Using Local Password](#)

- [NASI Authentication Using Group RADIUS](#)
- [NASI Authentication Using Group TACACS+](#)
- [NASI Authentication Using group group-name](#)

NASI Authentication Using Enable Password

Use the **aaa authentication nasi** command with the *method* keyword **enable** to specify the enable password as the authentication method. For example, to specify the enable password as the method of NASI user authentication when no other method list has been defined, enter the following command:

```
aaa authentication nasi default enable
```

Before you can use the enable password as the authentication method, you need to define the enable password. For more information about defining enable passwords, refer to the chapter “Configuring Passwords and Privileges.”

NASI Authentication Using Line Password

Use the **aaa authentication nasi** command with the *method* keyword **line** to specify the line password as the authentication method. For example, to specify the line password as the method of NASI user authentication when no other method list has been defined, enter the following command:

```
aaa authentication nasi default line
```

Before you can use a line password as the NASI authentication method, you need to define a line password. For more information about defining line passwords, refer to the section “[Configuring Line Password Protection](#)” in this chapter.

NASI Authentication Using Local Password

Use the **aaa authentication nasi** command with the *method* keyword **local** to specify that the Cisco router or access server will use the local username database for authentication information. For example, to specify the local username database as the method of NASI user authentication when no other method list has been defined, enter the following command:

```
aaa authentication nasi default local
```

For information about adding users to the local username database, refer to the section “[Establishing Username Authentication](#)” in this chapter.

NASI Authentication Using Group RADIUS

Use the **aaa authentication nasi** command with the **group radius** *method* to specify RADIUS as the NASI authentication method. For example, to specify RADIUS as the method of NASI user authentication when no other method list has been defined, enter the following command:

```
aaa authentication nasi default group radius
```

Before you can use RADIUS as the NASI authentication method, you need to enable communication with the RADIUS security server. For more information about establishing communication with a RADIUS server, refer to the chapter “Configuring RADIUS.”

NASI Authentication Using Group TACACS+

Use the **aaa authentication nasi** command with the **group tacacs+ method** keyword to specify TACACS+ as the NASI authentication method. For example, to specify TACACS+ as the method of NASI user authentication when no other method list has been defined, enter the following command:

```
aaa authentication nasi default group tacacs+
```

Before you can use TACACS+ as the authentication method, you need to enable communication with the TACACS+ security server. For more information about establishing communication with a TACACS+ server, refer to the chapter “Configuring TACACS+.”

NASI Authentication Using group group-name

Use the **aaa authentication nasi** command with the **group group-name** method to specify a subset of RADIUS or TACACS+ servers to use as the NASI authentication method. To specify and define the group name and the members of the group, use the **aaa group server** command. For example, use the **aaa group server** command to first define the members of **group nasirad**:

```
aaa group server radius nasirad
server 172.16.2.3
server 172.16.2.17
server 172.16.2.32
```

This command specifies RADIUS servers 172.16.2.3, 172.16.2.17, and 172.16.2.32 as members of the group *nasirad*.

To specify **group nasirad** as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication nasi default group nasirad
```

Before you can use a group name as the NASI authentication method, you need to enable communication with the RADIUS or TACACS+ security server. For more information about establishing communication with a RADIUS server, refer to the chapter “Configuring RADIUS”. For more information about establishing communication with a TACACS+ server, refer to the chapter “Configuring TACACS+.”

Specifying the Amount of Time for Login Input

The **timeout login response** command allows you to specify how long the system will wait for login input (such as username and password) before timing out. The default login value is 30 seconds; with the **timeout login response** command, you can specify a timeout value from 1 to 300 seconds. To change the login timeout value from the default of 30 seconds, use the following command in line configuration mode:

Command	Purpose
Router(config-line)# timeout login response <i>seconds</i>	Specifies how long the system will wait for login information before timing out.

Enabling Password Protection at the Privileged Level

Use the **aaa authentication enable default** command to create a series of authentication methods that are used to determine whether a user can access the privileged EXEC command level. You can specify up to four authentication methods. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line.

Use the following command in global configuration mode:

Command	Purpose
Router(config)# aaa authentication enable default <i>method1 [method2...]</i>	<p>Enables user ID and password checking for users requesting privileged EXEC level.</p> <p>Note All aaa authentication enable default requests sent by the router to a RADIUS server include the username "\$enab15\$." Requests sent to a TACACS+ server will include the username that is entered for login authentication.</p>

The method argument refers to the actual list of methods the authentication algorithm tries, in the sequence entered. [Table 8](#) lists the supported enable authentication methods.

Table 8 AAA Authentication Enable Default Methods

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.
group radius	<p>Uses the list of all RADIUS hosts for authentication.</p> <p>Note The RADIUS method does not work on a per-username basis.</p>
group tacacs+	Uses the list of all TACACS+ hosts for authentication.
group <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the aaa group server radius or aaa group server tacacs+ command.

Changing the Text Displayed at the Password Prompt

Use the **aaa authentication password-prompt** command to change the default text that the Cisco IOS software displays when prompting a user to enter a password. This command changes the password prompt for the enable password as well as for login passwords that are not supplied by remote security servers. The **no** form of this command returns the password prompt to the following default value:

Password:

The **aaa authentication password-prompt** command does not change any dialog that is supplied by a remote TACACS+ or RADIUS server.

The **aaa authentication password-prompt** command works when RADIUS is used as the login method. You will be able to see the password prompt defined in the command shown even when the RADIUS server is unreachable. The **aaa authentication password-prompt** command does not work with

TACACS+. TACACS+ supplies the NAS with the password prompt to display to the users. If the TACACS+ server is reachable, the NAS gets the password prompt from the server and uses that prompt instead of the one defined in the **aaa authentication password-prompt** command. If the TACACS+ server is not reachable, the password prompt defined in the **aaa authentication password-prompt** command may be used.

Use the following command in global configuration mode:

Command	Purpose
Router(config)# aaa authentication password-prompt <i>text-string</i>	Changes the default text displayed when a user is prompted to enter a password.

Configuring Message Banners for AAA Authentication

AAA supports the use of configurable, personalized login and failed-login banners. You can configure message banners that will be displayed when a user logs in to the system to be authenticated using AAA and when, for whatever reason, authentication fails.

This section includes the following sections:

- [Configuring a Login Banner](#)
- [Configuring a Failed-Login Banner](#)

Configuring a Login Banner

To create a login banner, you need to configure a delimiting character, which notifies the system that the following text string is to be displayed as the banner, and then the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the banner. The delimiting character can be any single character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.

To configure a banner that will be displayed whenever a user logs in (replacing the default message for login), use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# aaa new-model	Enables AAA.
Step 2	Router(config)# aaa authentication banner <i>delimiter string delimiter</i>	Creates a personalized login banner.

The maximum number of characters that can be displayed in the login banner is 2996 characters.

Configuring a Failed-Login Banner

To create a failed-login banner, you need to configure a delimiting character, which notifies the system that the following text string is to be displayed as the banner, and then the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the failed-login banner. The delimiting character can be any single character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.

To configure a message that will be displayed whenever a user fails login (replacing the default message for failed login), use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config) # aaa new-model	Enables AAA.
Step 2	Router(config) # aaa authentication fail-message <i>delimiter string delimiter</i>	Creates a message to be displayed when a user fails login.

The maximum number of characters that can be displayed in the failed-login banner is 2996 characters.

Configuring AAA Packet of Disconnect

Packet of disconnect (POD) terminates connections on the network access server (NAS) when particular session attributes are identified. By using session information obtained from AAA, the POD client residing on a UNIX workstation sends disconnect packets to the POD server running on the network access server. The NAS terminates any inbound user session with one or more matching key attributes. It rejects requests when required fields are missing or when an exact match is not found.

To configure POD, perform the following tasks in global configuration mode:

	Command	Purpose
Step 1	Router(config) # aaa accounting network default <i>start-stop radius</i>	Enables AAA accounting records.
Step 2	Router(config) # aaa accounting delay-start	(Optional) Delays generation of the start accounting record until the Framed-IP-Address is assigned, allowing its use in the POD packet.
Step 3	Router(config) # aaa pod server server-key <i>string</i>	Enables POD reception.
Step 4	Router(config) # radius-server host <i>IP address</i> non-standard	Declares a RADIUS host that uses a vendor-proprietary version of RADIUS.

Enabling Double Authentication

Previously, PPP sessions could only be authenticated by using a single authentication method: either PAP or CHAP. Double authentication requires remote users to pass a second stage of authentication—after CHAP or PAP authentication—before gaining network access.

This second (“double”) authentication requires a password that is known to the user but *not* stored on the user’s remote host. Therefore, the second authentication is specific to a user, not to a host. This provides an additional level of security that will be effective even if information from the remote host is stolen. In addition, this also provides greater flexibility by allowing customized network privileges for each user.

The second stage authentication can use one-time passwords such as token card passwords, which are not supported by CHAP. If one-time passwords are used, a stolen user password is of no use to the perpetrator.

This section includes the following subsections:

- [How Double Authentication Works](#)

- [Configuring Double Authentication](#)
- [Accessing the User Profile After Double Authentication](#)

How Double Authentication Works

With double authentication, there are two authentication/authorization stages. These two stages occur after a remote user dials in and a PPP session is initiated.

In the first stage, the user logs in using the remote host name; CHAP (or PAP) authenticates the remote host, and then PPP negotiates with AAA to authorize the remote host. In this process, the network access privileges associated with the remote host are assigned to the user.



Note

We suggest that the network administrator restrict authorization at this first stage to allow only Telnet connections to the local host.

In the second stage, the remote user must Telnet to the network access server to be authenticated. When the remote user logs in, the user must be authenticated with AAA login authentication. The user then must enter the **access-profile** command to be reauthorized using AAA. When this authorization is complete, the user has been double authenticated, and can access the network according to per-user network privileges.

The system administrator determines what network privileges remote users will have after each stage of authentication by configuring appropriate parameters on a security server. To use double authentication, the user must activate it by issuing the **access-profile** command.



Caution

Double authentication can cause certain undesirable events if multiple hosts share a PPP connection to a network access server, as shown in [Figure 3](#).

First, if a user, Bob, initiates a PPP session and activates double authentication at the network access server (per [Figure 3](#)), any other user will automatically have the same network privileges as Bob until Bob's PPP session expires. This happens because Bob's authorization profile is applied to the network access server's interface during the PPP session and any PPP traffic from other users will use the PPP session Bob established.

Second, if Bob initiates a PPP session and activates double authentication, and then—before Bob's PPP session has expired—another user, Jane, executes the **access-profile** command (or, if Jane Telnets to the network access server and **autocommand access-profile** is executed), a reauthorization will occur and Jane's authorization profile will be applied to the interface—replacing Bob's profile. This can disrupt or halt Bob's PPP traffic, or grant Bob additional authorization privileges Bob should not have.

Figure 3 **Possibly Risky Topology: Multiple Hosts Share a PPP Connection to a Network Access Server**



Configuring Double Authentication

To configure double authentication, you must complete the following steps:

1. Enable AAA by using the **aaa-new model** global configuration command. For more information about enabling AAA, refer to the chapter “AAA Overview.”
2. Use the **aaa authentication** command to configure your network access server to use login and PPP authentication method lists, then apply those method lists to the appropriate lines or interfaces.
3. Use the **aaa authorization** command to configure AAA network authorization at login. For more information about configuring network authorization, refer to the “Configuring Authorization” chapter.
4. Configure security protocol parameters (for example, RADIUS or TACACS+). For more information about RADIUS, refer to the chapter “Configuring RADIUS”. For more information about TACACS+, refer to the chapter “Configuring TACACS+.”
5. Use access control list AV pairs on the security server that the user can connect to the local host only by establishing a Telnet connection.
6. (Optional) Configure the **access-profile** command as an autocommand. If you configure the autocommand, remote users will not have to manually enter the **access-profile** command to access authorized rights associated with their personal user profile. To learn about configuring autocommands, refer to the **autocommand** command in the *Cisco IOS Dial Technologies Command Reference: Network Services*.



Note

If the **access-profile** command is configured as an autocommand, users will still have to Telnet to the local host and log in to complete double authentication.

Follow these rules when creating the user-specific authorization statements (These rules relate to the default behavior of the **access-profile** command):

- Use valid AV pairs when configuring access control list AV pairs on the security server. For a list of valid AV pairs, refer to the chapter “Authentication Commands” in the *Cisco IOS Security Command Reference*.
- If you want remote users to use the interface’s existing authorization (that which existed prior to the second stage authentication/authorization), but you want them to have different access control lists (ACLs), you should specify *only* ACL AV pairs in the user-specific authorization definition. This might be desirable if you set up a default authorization profile to apply to the remote host, but want to apply specific ACLs to specific users.

- When these user-specific authorization statements are later applied to the interface, they can either be *added* to the existing interface configuration or they can *replace* the existing interface configuration—depending on which form of the **access-profile** command is used to authorize the user. You should understand how the **access-profile** command works before configuring the authorization statements.
- If you will be using ISDN or Multilink PPP, you must also configure virtual templates at the local host.

To troubleshoot double authentication, use the **debug aaa per-user** debug command. For more information about this command, refer to the *Cisco IOS Debug Command Reference*.

Accessing the User Profile After Double Authentication

In double authentication, when a remote user establishes a PPP link to the local host using the local host name, the remote host is CHAP (or PAP) authenticated. After CHAP (or PAP) authentication, PPP negotiates with AAA to assign network access privileges associated with the remote host to the user. (We suggest that privileges at this stage be restricted to allow the user to connect to the local host only by establishing a Telnet connection.)

When the user needs to initiate the second phase of double authentication, establishing a Telnet connection to the local host, the user enters a personal username and password (different from the CHAP or PAP username and password). This action causes AAA reauthentication to occur according to the personal username/password. The initial rights associated with the local host, though, are still in place. By using the **access-profile** command, the rights associated with the local host are replaced by or merged with those defined for the user in the user's profile.

To access the user profile after double authentication, use the following command in EXEC configuration mode:

Command	Purpose
Router> access-profile [merge replace] [ignore-sanity-checks]	Accesses the rights associated for the user after double authentication.

If you configured the **access-profile** command to be executed as an autocommand, it will be executed automatically after the remote user logs in.

Enabling Automated Double Authentication

You can make the double authentication process easier for users by implementing automated double authentication. Automated double authentication provides all of the security benefits of double authentication, but offers a simpler, more user-friendly interface for remote users. With double authentication, a second level of user authentication is achieved when the user Telnets to the network access server or router and enters a username and password. With automated double authentication, the user does not have to Telnet to the network access server; instead the user responds to a dialog box that requests a username and password or personal identification number (PIN). To use the automated double authentication feature, the remote user hosts must be running a companion client application. As of Cisco IOS Release 12.0, the only client application software available is the Glacier Bay application server software for PCs.

**Note**

Automated double authentication, like the existing double authentication feature, is for Multilink PPP ISDN connections only. Automated double authentication cannot be used with other protocols such as X.25 or SLIP.

Automated double authentication is an enhancement to the existing double authentication feature. To configure automated double authentication, you must first configure double authentication by completing the following steps:

1. Enable AAA by using the **aaa-new model** global configuration command. For more information about enabling AAA, refer to the chapter “AAA Overview.”
2. Use the **aaa authentication** command to configure your network access server to use login and PPP authentication method lists, then apply those method lists to the appropriate lines or interfaces.
3. Use the **aaa authorization** command to configure AAA network authorization at login. For more information about configuring network authorization, refer to the chapter “Configuring Authorization.”
4. Configure security protocol parameters (for example, RADIUS or TACACS+). For more information about RADIUS, refer to the chapter “Configuring RADIUS”. For more information about TACACS+, refer to the chapter “Configuring TACACS+.”
5. Use access control list AV pairs on the security server that the user can connect to the local host only by establishing a Telnet connection.
6. Configure the **access-profile** command as an autocommand. If you configure the autocommand, remote users will not have to manually enter the **access-profile** command to access authorized rights associated with their personal user profile. To learn about configuring autocommands, refer to the **autocommand** command in the *Cisco IOS Dial Technologies Command Reference*, Release 12.2.

**Note**

If the **access-profile** command is configured as an autocommand, users will still have to Telnet to the local host and log in to complete double authentication.

Follow these rules when creating the user-specific authorization statements (These rules relate to the default behavior of the **access-profile** command):

- Use valid AV pairs when configuring access control list AV pairs on the security server. For a list of valid AV pairs, refer to the chapter “Authentication Commands” in the *Cisco IOS Security Command Reference*.
- If you want remote users to use the interface’s existing authorization (that which existed prior to the second stage authentication/authorization), but you want them to have different access control lists (ACLs), you should specify *only* ACL AV pairs in the user-specific authorization definition. This might be desirable if you set up a default authorization profile to apply to the remote host, but want to apply specific ACLs to specific users.
- When these user-specific authorization statements are later applied to the interface, they can either be *added* to the existing interface configuration, or *replace* the existing interface configuration—depending on which form of the **access-profile** command is used to authorize the user. You should understand how the **access-profile** command works before configuring the authorization statements.
- If you will be using ISDN or Multilink PPP, you must also configure virtual templates at the local host.

To troubleshoot double authentication, use the **debug aaa per-user** debug command. For more information about this command, refer to the *Cisco IOS Debug Command Reference*.

After you have configured double authentication, you are ready to configure the automation enhancement.

To configure automated double authentication, use the following commands, starting in global configuration mode.

:

	Command	Purpose
Step 1	<code>Router(config)# ip trigger-authentication [timeout seconds] [port number]</code>	Enables automation of double authentication.
Step 2	<code>Router(config)# interface bri number</code> or <code>Router(config)# interface serial number:23</code>	Selects an ISDN BRI or ISDN PRI interface and enter the interface configuration mode.
Step 3	<code>Router(config-if)# ip trigger-authentication</code>	Applies automated double authentication to the interface.

To troubleshoot automated double authentication, use the following commands in privileged EXEC mode:

	Command	Purpose
Step 1	<code>Router# show ip trigger-authentication</code>	Displays the list of remote hosts for which automated double authentication has been attempted (successfully or unsuccessfully).
Step 2	<code>Router# clear ip trigger-authentication</code>	Clears the list of remote hosts for which automated double authentication has been attempted. (This clears the table displayed by the show ip trigger-authentication command.)
Step 3	<code>Router# debug ip trigger-authentication</code>	Displays debug output related to automated double authentication.

Non-AAA Authentication Methods

This section discusses the following non-AAA authentication tasks:

- [Configuring Line Password Protection](#)
- [Establishing Username Authentication](#)
- [Enabling CHAP or PAP Authentication](#)
- [Using MS-CHAP](#)

Configuring Line Password Protection

You can provide access control on a terminal line by entering the password and establishing password checking. To do so, use the following commands in line configuration mode:

	Command	Purpose
Step 1	<code>Router(config-line)# password password</code>	Assigns a password to a terminal or other device on a line.
Step 2	<code>Router(config-line)# login</code>	Enables password checking at login.

The password checker is case sensitive and can include spaces; for example, the password “Secret” is different from the password “secret,” and “two words” is an acceptable password.

You can disable line password verification by disabling password checking. To do so, use the following command in line configuration mode:

Command	Purpose
<code>Router(config-line)# no login</code>	Disables password checking or allow access to a line without password verification.

If you configure line password protection and then configure TACACS or extended TACACS, the TACACS username and password take precedence over line passwords. If you have not yet implemented a security policy, we recommend that you use AAA.

**Note**

The **login** command only changes username and privilege level but it does not execute a shell; therefore autocommands will not be executed. To execute autocommands under this circumstance, you need to establish a Telnet session back into the router (loop-back). Make sure that the router has been configured for secure Telnet sessions if you choose to implement autocommands this way.

Establishing Username Authentication

You can create a username-based authentication system, which is useful in the following situations:

- To provide a TACACS-like username and encrypted password-authentication system for networks that cannot support TACACS
- To provide special-case logins: for example, access list verification, no password verification, autocommand execution at login, and “no escape” situations

To establish username authentication, use the following commands in global configuration mode as needed for your system configuration:

	Command	Purpose
Step 1	<code>Router(config)# username name [nopassword password password password encryption-type encrypted password]</code> or <code>Router(config)# username name [access-class number]</code>	Establishes username authentication with encrypted passwords. or (Optional) Establishes username authentication by access list.
Step 2	<code>Router(config)# username name [privilege level]</code>	(Optional) Sets the privilege level for the user.

	Command	Purpose
Step 3	<code>Router(config)# username name [autocommand command]</code>	(Optional) Specifies a command to be executed automatically.
Step 4	<code>Router(config)# username name [noescape] [nohangup]</code>	(Optional) Sets a “no escape” login environment.

The keyword **noescape** prevents users from using escape characters on the hosts to which they are connected. The **nohangup** feature does not disconnect after using the autocommand.

**Caution**

Passwords will be displayed in clear text in your configuration unless you enable the **service password-encryption** command. For more information about the **service password-encryption** command, refer to the chapter “Passwords and Privileges Commands” in the *Cisco IOS Security Command Reference*.

Enabling CHAP or PAP Authentication

One of the most common transport protocols used in Internet service providers’ (ISPs’) dial solutions is the Point-to-Point Protocol (PPP). Traditionally, remote users dial in to an access server to initiate a PPP session. After PPP has been negotiated, remote users are connected to the ISP network and to the Internet.

Because ISPs want only customers to connect to their access servers, remote users are required to authenticate to the access server before they can start up a PPP session. Normally, a remote user authenticates by typing in a username and password when prompted by the access server. Although this is a workable solution, it is difficult to administer and awkward for the remote user.

A better solution is to use the authentication protocols built into PPP. In this case, the remote user dials in to the access server and starts up a minimal subset of PPP with the access server. This does not give the remote user access to the ISP’s network—it merely allows the access server to talk to the remote device.

PPP currently supports two authentication protocols: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). Both are specified in RFC 1334 and are supported on synchronous and asynchronous interfaces. Authentication via PAP or CHAP is equivalent to typing in a username and password when prompted by the server. CHAP is considered to be more secure because the remote user’s password is never sent across the connection.

PPP (with or without PAP or CHAP authentication) is also supported in dialout solutions. An access server utilizes a dialout feature when it initiates a call to a remote device and attempts to start up a transport protocol such as PPP.

See the chapter “Configuring Interfaces” in the *Cisco IOS Configuration Fundamentals Configuration Guide* for more information about CHAP and PAP.

**Note**

To use CHAP or PAP, you must be running PPP encapsulation.

When CHAP is enabled on an interface and a remote device attempts to connect to it, the access server sends a CHAP packet to the remote device. The CHAP packet requests or “challenges” the remote device to respond. The challenge packet consists of an ID, a random number, and the host name of the local router.

When the remote device receives the challenge packet, it concatenates the ID, the remote device's password, and the random number, and then encrypts all of it using the remote device's password. The remote device sends the results back to the access server, along with the name associated with the password used in the encryption process.

When the access server receives the response, it uses the name it received to retrieve a password stored in its user database. The retrieved password should be the same password the remote device used in its encryption process. The access server then encrypts the concatenated information with the newly retrieved password—if the result matches the result sent in the response packet, authentication succeeds.

The benefit of using CHAP authentication is that the remote device's password is never transmitted in clear text. This prevents other devices from stealing it and gaining illegal access to the ISP's network.

CHAP transactions occur only at the time a link is established. The access server does not request a password during the rest of the call. (The local device can, however, respond to such requests from other devices during a call.)

When PAP is enabled, the remote router attempting to connect to the access server is required to send an authentication request. If the username and password specified in the authentication request are accepted, the Cisco IOS software sends an authentication acknowledgment.

After you have enabled CHAP or PAP, the access server will require authentication from remote devices dialing in to the access server. If the remote device does not support the enabled protocol, the call will be dropped.

To use CHAP or PAP, you must perform the following tasks:

1. Enable PPP encapsulation.
2. Enable CHAP or PAP on the interface.
3. For CHAP, configure host name authentication and the secret or password for each remote system with which authentication is required.

This section includes the following sections:

- [Enabling PPP Encapsulation](#)
- [Enabling PAP or CHAP](#)
- [Inbound and Outbound Authentication](#)
- [Enabling Outbound PAP Authentication](#)
- [Refusing PAP Authentication Requests](#)
- [Creating a Common CHAP Password](#)
- [Refusing CHAP Authentication Requests](#)
- [Delaying CHAP Authentication Until Peer Authenticates](#)

Enabling PPP Encapsulation

To enable PPP encapsulation, use the following command in interface configuration mode:

Command	Purpose
<code>Router(config-if)# encapsulation ppp</code>	Enables PPP on an interface.

Enabling PAP or CHAP

To enable CHAP or PAP authentication on an interface configured for PPP encapsulation, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# ppp authentication { <i>protocol1</i> [<i>protocol2...</i>] [<i>if-needed</i>] [<i>default</i> <i>list-name</i>] [<i>callin</i>] [<i>one-time</i>]	Defines the authentication protocols supported and the order in which they are used. In this command, <i>protocol1</i> , <i>protocol2</i> represent the following protocols: CHAP, MS-CHAP, and PAP. PPP authentication is attempted first using the first authentication method, which is <i>protocol1</i> . If <i>protocol1</i> is unable to establish authentication, the next configured protocol is used to negotiate authentication.

If you configure **ppp authentication chap** on an interface, all incoming calls on that interface that initiate a PPP connection will have to be authenticated using CHAP; likewise, if you configure **ppp authentication pap**, all incoming calls that start a PPP connection will have to be authenticated via PAP. If you configure **ppp authentication chap pap**, the access server will attempt to authenticate all incoming calls that start a PPP session with CHAP. If the remote device does not support CHAP, the access server will try to authenticate the call using PAP. If the remote device does not support either CHAP or PAP, authentication will fail and the call will be dropped. If you configure **ppp authentication pap chap**, the access server will attempt to authenticate all incoming calls that start a PPP session with PAP. If the remote device does not support PAP, the access server will try to authenticate the call using CHAP. If the remote device does not support either protocol, authentication will fail and the call will be dropped. If you configure the **ppp authentication** command with the **callin** keyword, the access server will only authenticate the remote device if the remote device initiated the call.

Authentication method lists and the **one-time** keyword are only available if you have enabled AAA—they will not be available if you are using TACACS or extended TACACS. If you specify the name of an authentication method list with the **ppp authentication** command, PPP will attempt to authenticate the connection using the methods defined in the specified method list. If AAA is enabled and no method list is defined by name, PPP will attempt to authenticate the connection using the methods defined as the default. The **ppp authentication** command with the **one-time** keyword enables support for one-time passwords during authentication.

The **if-needed** keyword is only available if you are using TACACS or extended TACACS. The **ppp authentication** command with the **if-needed** keyword means that PPP will only authenticate the remote device via PAP or CHAP if they have not yet authenticated during the life of the current call. If the remote device authenticated via a standard login procedure and initiated PPP from the EXEC prompt, PPP will not authenticate via CHAP if **ppp authentication chap if-needed** is configured on the interface.



Caution

If you use a *list-name* that has not been configured with the **aaa authentication ppp** command, you disable PPP on the line.

For information about adding a **username** entry for each remote system from which the local router or access server requires authentication, see the section “[Establishing Username Authentication](#).”

Inbound and Outbound Authentication

PPP supports two-way authentication. Normally, when a remote device dials in to an access server, the access server requests that the remote device prove that it is allowed access. This is known as inbound authentication. At the same time, the remote device can also request that the access server prove that it is who it says it is. This is known as outbound authentication. An access server also does outbound authentication when it initiates a call to a remote device.

Enabling Outbound PAP Authentication

To enable outbound PAP authentication, use the following command in interface configuration mode:

Command	Purpose
<code>Router(config-if)# ppp pap sent-username username password password</code>	Enables outbound PAP authentication.

The access server uses the username and password specified by the **ppp pap sent-username** command to authenticate itself whenever it initiates a call to a remote device or when it has to respond to a remote device's request for outbound authentication.

Refusing PAP Authentication Requests

To refuse PAP authentication from peers requesting it, meaning that PAP authentication is disabled for all calls, use the following command in interface configuration mode:

Command	Purpose
<code>Router(config-if)# ppp pap refuse</code>	Refuses PAP authentication from peers requesting PAP authentication.

If the **refuse** keyword is not used, the router will not refuse any PAP authentication challenges received from the peer.

Creating a Common CHAP Password

For remote CHAP authentication only, you can configure your router to create a common CHAP secret password to use in response to challenges from an unknown peer; for example, if your router calls a rotary of routers (either from another vendor, or running an older version of the Cisco IOS software) to which a new (that is, unknown) router has been added. The **ppp chap password** command allows you to replace several username and password configuration commands with a single copy of this command on any dialer interface or asynchronous group interface.

To enable a router calling a collection of routers to configure a common CHAP secret password, use the following command in interface configuration mode:

Command	Purpose
<code>Router(config-if)# ppp chap password secret</code>	Enables a router calling a collection of routers to configure a common CHAP secret password.

Refusing CHAP Authentication Requests

To refuse CHAP authentication from peers requesting it, meaning that CHAP authentication is disabled for all calls, use the following command in interface configuration mode:

Command	Purpose
<code>Router(config-if)# ppp chap refuse [callin]</code>	Refuses CHAP authentication from peers requesting CHAP authentication.

If the **callin** keyword is used, the router will refuse to answer CHAP authentication challenges received from the peer, but will still require the peer to answer any CHAP challenges the router sends.

If outbound PAP has been enabled (using the **ppp pap sent-username** command), PAP will be suggested as the authentication method in the refusal packet.

Delaying CHAP Authentication Until Peer Authenticates

To specify that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router, use the following command in interface configuration mode:

Command	Purpose
<code>Router(config-if)# ppp chap wait secret</code>	Configures the router to delay CHAP authentication until after the peer has authenticated itself to the router.

This command (which is the default) specifies that the router will not authenticate to a peer requesting CHAP authentication until the peer has authenticated itself to the router. The **no ppp chap wait** command specifies that the router will respond immediately to an authentication challenge.

Using MS-CHAP

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is the Microsoft version of CHAP and is an extension of RFC 1994. Like the standard version of CHAP, MS-CHAP is used for PPP authentication; in this case, authentication occurs between a PC using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a network access server.

MS-CHAP differs from the standard CHAP as follows:

- MS-CHAP is enabled by negotiating CHAP Algorithm 0x80 in LCP option 3, Authentication Protocol.
- The MS-CHAP Response packet is in a format designed to be compatible with Microsoft Windows NT 3.5 and 3.51, Microsoft Windows 95, and Microsoft LAN Manager 2.x. This format does not require the authenticator to store a clear or reversibly encrypted password.
- MS-CHAP provides an authenticator-controlled authentication retry mechanism.
- MS-CHAP provides an authenticator-controlled change password mechanism.
- MS-CHAP defines a set of “reason-for failure” codes returned in the Failure packet message field.

Depending on the security protocols you have implemented, PPP authentication using MS-CHAP can be used with or without AAA security services. If you have enabled AAA, PPP authentication using MS-CHAP can be used in conjunction with both TACACS+ and RADIUS. Table 9 lists the vendor-specific RADIUS attributes (IETF Attribute 26) that enable RADIUS to support MS-CHAP.

Table 9 Vendor-Specific RADIUS Attributes for MS-CHAP

Vendor-ID Number	Vendor-Type Number	Vendor-Proprietary Attribute	Description
311	11	MSCHAP-Challenge	Contains the challenge sent by a network access server to an MS-CHAP user. It can be used in both Access-Request and Access-Challenge packets.
211	11	MSCHAP-Response	Contains the response value provided by a PPP MS-CHAP user in response to the challenge. It is only used in Access-Request packets. This attribute is identical to the PPP CHAP Identifier.

To define PPP authentication using MS-CHAP, use the following commands in interface configuration mode:

	Command	Purpose
Step 1	Router(config-if)# encapsulation ppp	Enables PPP encapsulation.
Step 2	Router(config-if)# ppp authentication ms-chap [if-needed] [list-name default] [callin] [one-time]	Defines PPP authentication using MS-CHAP.

If you configure **ppp authentication ms-chap** on an interface, all incoming calls on that interface that initiate a PPP connection will have to be authenticated using MS-CHAP. If you configure the **ppp authentication** command with the **callin** keyword, the access server will only authenticate the remote device if the remote device initiated the call.

Authentication method lists and the **one-time** keyword are only available if you have enabled AAA—they will not be available if you are using TACACS or extended TACACS. If you specify the name of an authentication method list with the **ppp authentication** command, PPP will attempt to authenticate the connection using the methods defined in the specified method list. If AAA is enabled and no method list is defined by name, PPP will attempt to authenticate the connection using the methods defined as the default. The **ppp authentication** command with the **one-time** keyword enables support for one-time passwords during authentication.

The **if-needed** keyword is only available if you are using TACACS or extended TACACS. The **ppp authentication** command with the **if-needed** keyword means that PPP will only authenticate the remote device via MS-CHAP if that device has not yet authenticated during the life of the current call. If the remote device authenticated through a standard login procedure and initiated PPP from the EXEC prompt, PPP will not authenticate through MS-CHAP if **ppp authentication chap if-needed** is configured.

**Note**

If PPP authentication using MS-CHAP is used with username authentication, you must include the MS-CHAP secret in the local username/password database. For more information about username authentication, refer to the “Establish Username Authentication” section.

Authentication Examples

The following sections provide authentication configuration examples:

- [RADIUS Authentication Examples](#)
- [TACACS+ Authentication Examples](#)
- [Kerberos Authentication Examples](#)
- [AAA Scalability Example](#)
- [Login and Failed Banner Examples](#)
- [AAA Packet of Disconnect Server Key Example](#)
- [Double Authentication Examples](#)
- [Automated Double Authentication Example](#)
- [MS-CHAP Example](#)

RADIUS Authentication Examples

This section provides two sample configurations using RADIUS.

The following example shows how to configure the router to authenticate and authorize using RADIUS:

```
aaa authentication login radius-login group radius local
aaa authentication ppp radius-ppp if-needed group radius
aaa authorization exec default group radius if-authenticated
aaa authorization network default group radius
line 3
login authentication radius-login
interface serial 0
ppp authentication radius-ppp
```

The lines in this sample RADIUS authentication and authorization configuration are defined as follows:

- The **aaa authentication login radius-login group radius local** command configures the router to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database.
- The **aaa authentication ppp radius-ppp if-needed group radius** command configures the Cisco IOS software to use PPP authentication using CHAP or PAP if the user has not already logged in. If the EXEC facility has authenticated the user, PPP authentication is not performed.
- The **aaa authorization exec default group radius if-authenticated** command queries the RADIUS database for information that is used during EXEC authorization, such as autocommands and privilege levels, but only provides authorization if the user has successfully authenticated.
- The **aaa authorization network default group radius** command queries RADIUS for network authorization, address assignment, and other access lists.
- The **login authentication radius-login** command enables the radius-login method list for line 3.

- The **ppp authentication radius-ppp** command enables the radius-ppp method list for serial interface 0.

The following example shows how to configure the router to prompt for and verify a username and password, authorize the user's EXEC level, and specify it as the method of authorization for privilege level 2. In this example, if a local username is entered at the username prompt, that username is used for authentication.

If the user is authenticated using the local database, EXEC authorization using RADIUS will fail because no data is saved from the RADIUS authentication. The method list also uses the local database to find an autocommand. If there is no autocommand, the user becomes the EXEC user. If the user then attempts to issue commands that are set at privilege level 2, TACACS+ is used to attempt to authorize the command.

```
aaa authentication login default group radius local
aaa authorization exec default group radius local
aaa authorization command 2 default group tacacs+ if-authenticated
radius-server host 172.16.71.146 auth-port 1645 acct-port 1646
radius-server attribute 44 include-in-access-req
radius-server attribute 8 include-in-access-req
```

The lines in this sample RADIUS authentication and authorization configuration are defined as follows:

- The **aaa authentication login default group radius local** command specifies that the username and password are verified by RADIUS or, if RADIUS is not responding, by the router's local user database.
- The **aaa authorization exec default group radius local** command specifies that RADIUS authentication information be used to set the user's EXEC level if the user authenticates with RADIUS. If no RADIUS information is used, this command specifies that the local user database be used for EXEC authorization.
- The **aaa authorization command 2 default group tacacs+ if-authenticated** command specifies TACACS+ authorization for commands set at privilege level 2, if the user has already successfully authenticated.
- The **radius-server host 172.16.71.146 auth-port 1645 acct-port 1646** command specifies the IP address of the RADIUS server host, the UDP destination port for authentication requests, and the UDP destination port for accounting requests.
- The **radius-server attribute 44 include-in-access-req** command sends RADIUS attribute 44 (Acct-Section-ID) in access-request packets.
- The **radius-server attribute 8 include-in-access-req** command sends RADIUS attribute 8 (Framed-IP-Address) in access-request packets.

TACACS+ Authentication Examples

The following example shows how to configure TACACS+ as the security protocol to be used for PPP authentication:

```
aaa new-model
aaa authentication ppp test group tacacs+ local
interface serial 0
ppp authentication chap pap test
tacacs-server host 10.1.2.3
tacacs-server key goaway
```

The lines in this sample TACACS+ authentication configuration are defined as follows:

- The **aaa new-model** command enables the AAA security services.
- The **aaa authentication** command defines a method list, “test,” to be used on serial interfaces running PPP. The keywords **group tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.
- The **interface** command selects the line.
- The **ppp authentication** command applies the test method list to this line.
- The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 10.1.2.3.
- The **tacacs-server key** command defines the shared encryption key to be “goaway.”

The following example shows how to configure AAA authentication for PPP:

```
aaa authentication ppp default if-needed group tacacs+ local
```

In this example, the keyword **default** means that PPP authentication is applied by default to all interfaces. The **if-needed** keyword means that if the user has already authenticated by going through the ASCII login procedure, then PPP is not necessary and can be skipped. If authentication is needed, the keywords **group tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.

The following example shows how to create the same authentication algorithm for PAP, but it calls the method list “MIS-access” instead of “default”:

```
aaa authentication ppp MIS-access if-needed group tacacs+ local
interface serial 0
ppp authentication pap MIS-access
```

In this example, because the list does not apply to any interfaces (unlike the default list, which applies automatically to all interfaces), the administrator must select interfaces to which this authentication scheme should apply by using the **interface** command. The administrator must then apply this method list to those interfaces by using the **ppp authentication** command.

Kerberos Authentication Examples

To specify Kerberos as the login authentication method, use the following command:

```
aaa authentication login default krb5
```

To specify Kerberos authentication for PPP, use the following command:

```
aaa authentication ppp default krb5
```

AAA Scalability Example

The following example shows a general security configuration using AAA with RADIUS as the security protocol. In this example, the network access server is configured to allocate 16 background processes to handle AAA requests for PPP.

```
aaa new-model
radius-server host alcatraz
radius-server key myRaDiUSpassWoRd
radius-server configure-nas
username root password ALongPassword
```

```

aaa authentication ppp dialins group radius local
aaa authentication login admins local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
aaa processes 16
line 1 16
  autoselect ppp
  autoselect during-login
  login authentication admins
  modem dialin
interface group-async 1
  group-range 1 16
  encapsulation ppp
  ppp authentication pap dialins

```

The lines in this sample RADIUS AAA configuration are defined as follows:

- The **aaa new-model** command enables AAA network security services.
- The **radius-server host** command defines the name of the RADIUS server host.
- The **radius-server key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **radius-server configure-nas** command defines that the Cisco router or access server will query the RADIUS server for static routes and IP pool definitions when the device first starts up.
- The **username** command defines the username and password to be used for the PPP Password Authentication Protocol (PAP) caller identification.
- The **aaa authentication ppp dialins group radius local** command defines the authentication method list “dialins,” which specifies that RADIUS authentication, then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP.
- The **aaa authentication login admins local** command defines another method list, “admins,” for login authentication.
- The **aaa authorization network default group radius local** command is used to assign an address and other network parameters to the RADIUS user.
- The **aaa accounting network default start-stop group radius** command tracks PPP usage.
- The **aaa processes** command allocates 16 background processes to handle AAA requests for PPP.
- The **line** command switches the configuration mode from global configuration to line configuration and identifies the specific lines being configured.
- The **autoselect ppp** command configures the Cisco IOS software to allow a PPP session to start up automatically on these selected lines.
- The **autoselect during-login** command is used to display the username and password prompt without pressing the Return key. After the user logs in, the autoselect function (in this case, PPP) begins.
- The **login authentication admins** command applies the “admins” method list for login authentication.
- The **modem dialin** command configures modems attached to the selected lines to only accept incoming calls.
- The **interface group-async** command selects and defines an asynchronous interface group.
- The **group-range** command defines the member asynchronous interfaces in the interface group.
- The **encapsulation ppp** command sets PPP as the encapsulation method used on the specified interfaces.

- The **ppp authentication pap dialins** command applies the “dialins” method list to the specified interfaces.

Login and Failed Banner Examples

The following example shows how to configure a login banner (in this case, the phrase “Unauthorized Access Prohibited”) that will be displayed when a user logs in to the system. The asterisk (*) is used as the delimiting character. (RADIUS is specified as the default login authentication method.)

```
aaa new-model
aaa authentication banner *Unauthorized Access Prohibited*
aaa authentication login default group radius
```

This configuration produces the following login banner:

```
Unauthorized Access Prohibited
Username:
```

The following example shows how to additionally configure a failed login banner (in this case, the phrase “Failed login. Try again.”) that will be displayed when a user tries to log in to the system and fails. The asterisk (*) is used as the delimiting character. (RADIUS is specified as the default login authentication method.)

```
aaa new-model
aaa authentication banner *Unauthorized Access Prohibited*
aaa authentication fail-message *Failed login. Try again.*
aaa authentication login default group radius
```

This configuration produces the following login and failed login banner:

```
Unauthorized Access Prohibited
Username:
Password:
Failed login. Try again.
```

AAA Packet of Disconnect Server Key Example

The following example shows how to configure POD (packet of disconnect), which terminates connections on the network access server (NAS) when particular session attributes are identified.

```
aaa new-model
aaa authentication ppp default radius
aaa accounting network default start-stop radius
aaa accounting delay-start
aaa pod server server-key xyz123
radius-server host 172.16.0.0 non-standard
radius-server key rad123
```

Double Authentication Examples

The examples in this section illustrate possible configurations to be used with double authentication. Your configurations could differ significantly, depending on your network and security requirements.

This section includes the following examples:

- [Configuration of the Local Host for AAA with Double Authentication Examples](#)
- [Configuration of the AAA Server for First-Stage \(PPP\) Authentication and Authorization Example](#)

- [Configuration of the AAA Server for Second-Stage \(Per-User\) Authentication and Authorization Examples](#)
- [Complete Configuration with TACACS+ Example](#)

**Note**

These configuration examples include specific IP addresses and other specific information. This information is for illustration purposes only: your configuration will use different IP addresses, different usernames and passwords, and different authorization statements.

Configuration of the Local Host for AAA with Double Authentication Examples

These two examples show how to configure a local host to use AAA for PPP and login authentication, and for network and EXEC authorization. One example is shown for RADIUS and one example for TACACS+.

In both examples, the first three lines configure AAA, with a specific server as the AAA server. The next two lines configure AAA for PPP and login authentication, and the last two lines configure network and EXEC authorization. The last line is necessary only if the **access-profile** command will be executed as an autocommand.

The following example shows router configuration with a RADIUS AAA server:

```
aaa new-model
radius-server host secureserver
radius-server key myradiuskey
aaa authentication ppp default group radius
aaa authentication login default group radius
aaa authorization network default group radius
aaa authorization exec default group radius
```

The following example shows router configuration with a TACACS+ server:

```
aaa new-model
tacacs-server host security
tacacs-server key mytacacskey
aaa authentication ppp default group tacacs+
aaa authentication login default group tacacs+
aaa authorization network default group tacacs+
aaa authorization exec default group tacacs+
```

Configuration of the AAA Server for First-Stage (PPP) Authentication and Authorization Example

This example shows a configuration on the AAA server. A partial sample AAA configuration is shown for RADIUS.

TACACS+ servers can be configured similarly. (See the section “[Complete Configuration with TACACS+ Example](#)” later in this chapter.)

This example defines authentication/authorization for a remote host named “hostx” that will be authenticated by CHAP in the first stage of double authentication. Note that the ACL AV pair limits the remote host to Telnet connections to the local host. The local host has the IP address 10.0.0.2.

The following example shows a partial AAA server configuration for RADIUS:

```
hostx Password = "welcome"
      User-Service-Type = Framed-User,
      Framed-Protocol = PPP,
      cisco-avpair = "lcp:interface-config=ip unnumbered ethernet 0",
      cisco-avpair = "ip:inacl#3=permit tcp any 172.21.114.0 0.0.0.255 eq telnet",
```



```
cisco-avpair = "ip:inacl#4=deny icmp any any",
cisco-avpair = "ip:route#5=55.0.0.0 255.0.0.0",
cisco-avpair = "ip:route#6=66.0.0.0 255.0.0.0",
cisco-avpair = "ipx:inacl#3=deny any"
```

Configuration of the AAA Server for Second-Stage (Per-User) Authentication and Authorization Examples

This section contains partial sample AAA configurations on a RADIUS server. These configurations define authentication and authorization for a user (Pat) with the username "patuser," who will be user-authenticated in the second stage of double authentication.

TACACS+ servers can be configured similarly. (See the section "[Complete Configuration with TACACS+ Example](#)" later in this chapter.)

Three examples show sample RADIUS AAA configurations that could be used with each of the three forms of the **access-profile** command.

The first example shows a partial sample AAA configuration that works with the default form (no keywords) of the **access-profile** command. Note that only ACL AV pairs are defined. This example also sets up the **access-profile** command as an autocommand.

```
patuser Password = "welcome"
User-Service-Type = Shell-User,
cisco-avpair = "shell:autocmd=access-profile"
User-Service-Type = Framed-User,
Framed-Protocol = PPP,
cisco-avpair = "ip:inacl#3=permit tcp any host 10.0.0.2 eq telnet",
cisco-avpair = "ip:inacl#4=deny icmp any any"
```

The second example shows a partial sample AAA configuration that works with the **access-profile merge** form of the **access-profile** command. This example also sets up the **access-profile merge** command as an autocommand.

```
patuser Password = "welcome"
User-Service-Type = Shell-User,
cisco-avpair = "shell:autocmd=access-profile merge"
User-Service-Type = Framed-User,
Framed-Protocol = PPP,
cisco-avpair = "ip:inacl#3=permit tcp any any"
cisco-avpair = "ip:route=10.0.0.0 255.255.0.0",
cisco-avpair = "ip:route=10.1.0.0 255.255.0.0",
cisco-avpair = "ip:route=10.2.0.0 255.255.0.0"
```

The third example shows a partial sample AAA configuration that works with the **access-profile replace** form of the **access-profile** command. This example also sets up the **access-profile replace** command as an autocommand.

```
patuser Password = "welcome"
User-Service-Type = Shell-User,
cisco-avpair = "shell:autocmd=access-profile replace"
User-Service-Type = Framed-User,
Framed-Protocol = PPP,
cisco-avpair = "ip:inacl#3=permit tcp any any",
cisco-avpair = "ip:inacl#4=permit icmp any any",
cisco-avpair = "ip:route=10.10.0.0 255.255.0.0",
cisco-avpair = "ip:route=10.11.0.0 255.255.0.0",
cisco-avpair = "ip:route=10.12.0.0 255.255.0.0"
```

Complete Configuration with TACACS+ Example

This example shows TACACS+ authorization profile configurations both for the remote host (used in the first stage of double authentication) and for specific users (used in the second stage of double authentication). This TACACS+ example contains approximately the same configuration information as shown in the previous RADIUS examples.

This sample configuration shows authentication/authorization profiles on the TACACS+ server for the remote host “hostx” and for three users, with the usernames “pat_default,” “pat_merge,” and “pat_replace.” The configurations for these three usernames illustrate different configurations that correspond to the three different forms of the **access-profile** command. The three user configurations also illustrate setting up the autocommand for each form of the **access-profile** command.

Figure 4 shows the topology. The example that follows the figure shows a TACACS+ configuration file.

Figure 4 **Example Topology for Double Authentication**



This sample configuration shows authentication/authorization profiles on the TACACS+ server for the remote host “hostx” and for three users, with the usernames “pat_default,” “pat_merge,” and “pat_replace.”

```
key = "mytacacskey"

default authorization = permit

#-----Remote Host (BRI)-----
#
# This allows the remote host to be authenticated by the local host
# during fist-stage authentication, and provides the remote host
# authorization profile.
#
#-----

user = hostx
{
    login = cleartext "welcome"
    chap = cleartext "welcome"

    service = ppp protocol = lcp {
        interface-config="ip unnumbered ethernet 0"
    }

    service = ppp protocol = ip {
        # It is important to have the hash sign and some string after
        # it. This indicates to the NAS that you have a per-user
        # config.

        inacl#3="permit tcp any 172.21.114.0 0.0.0.255 eq telnet"
        inacl#4="deny icmp any any"
```

```

        route#5="55.0.0.0 255.0.0.0"
        route#6="66.0.0.0 255.0.0.0"
    }

    service = ppp protocol = ipx {
        # see previous comment about the hash sign and string, in protocol = ip
        inacl#3="deny any"
    }

}

#----- "access-profile" default user "only acls" -----
#
# Without arguments, access-profile removes any access-lists it can find
# in the old configuration (both per-user and per-interface), and makes sure
# that the new profile contains ONLY access-list definitions.
#
#-----

user = pat_default
{
    login = cleartext "welcome"
    chap = cleartext "welcome"

    service = exec

    {
        # This is the autocommand that executes when pat_default logs in.
        autocmd = "access-profile"
    }

    service = ppp protocol = ip {
        # Put whatever access-lists, static routes, whatever
        # here.
        # If you leave this blank, the user will have NO IP
        # access-lists (not even the ones installed prior to
        # this)!

        inacl#3="permit tcp any host 10.0.0.2 eq telnet"
        inacl#4="deny icmp any any"
    }

    service = ppp protocol = ipx {
        # Put whatever access-lists, static routes, whatever
        # here.
        # If you leave this blank, the user will have NO IPX
        # access-lists (not even the ones installed prior to
        # this)!
    }

}

#----- "access-profile merge" user -----
#
# With the 'merge' option, first all old access-lists are removed (as before),
# but then (almost) all AV pairs are uploaded and installed. This will allow
# for uploading any custom static routes, sap-filters, and so on, that the user
# may need in his or her profile. This needs to be used with care, as it leaves
# open the possibility of conflicting configurations.

```

```

#
#-----

user = pat_merge
{
    login = cleartext "welcome"
    chap = cleartext "welcome"

    service = exec
    {
        # This is the autocommand that executes when pat_merge logs in.
        autocmd = "access-profile merge"
    }

    service = ppp protocol = ip
    {
        # Put whatever access-lists, static routes, whatever
        # here.
        # If you leave this blank, the user will have NO IP
        # access-lists (not even the ones installed prior to
        # this)!

        inacl#3="permit tcp any any"
        route#2="10.0.0.0 255.255.0.0"
        route#3="10.1.0.0 255.255.0.0"
        route#4="10.2.0.0 255.255.0.0"

    }

    service = ppp protocol = ipx
    {
        # Put whatever access-lists, static routes, whatever
        # here.
        # If you leave this blank, the user will have NO IPX
        # access-lists (not even the ones installed prior to
        # this)!

    }

}

#----- "access-profile replace" user -----
#
# With the 'replace' option, ALL old configuration is removed and ALL new
# configuration is installed.
#
# One caveat: access-profile checks the new configuration for address-pool and
# address AV pairs. As addresses cannot be renegotiated at this point, the
# command will fail (and complain) when it encounters such an AV pair.
# Such AV pairs are considered to be "invalid" for this context.
#-----

user = pat_replace
{
    login = cleartext "welcome"
    chap = cleartext "welcome"

    service = exec
    {
        # This is the autocommand that executes when pat_replace logs in.

```

```

        autocmd = "access-profile replace"
    }

    service = ppp protocol = ip
    {
        # Put whatever access-lists, static routes, whatever
        # here.
        # If you leave this blank, the user will have NO IP
        # access-lists (not even the ones installed prior to
        # this)!

        inacl#3="permit tcp any any"
        inacl#4="permit icmp any any"

        route#2="10.10.0.0 255.255.0.0"
        route#3="10.11.0.0 255.255.0.0"
        route#4="10.12.0.0 255.255.0.0"
    }

    service = ppp protocol = ipx
    {
        # put whatever access-lists, static routes, whatever
        # here.
        # If you leave this blank, the user will have NO IPX
        # access-lists (not even the ones installed prior to
        # this)!
    }
}

```

Automated Double Authentication Example

This example shows a complete configuration file for a Cisco 2509 router with automated double authentication configured. The configuration commands that apply to automated double authentication are preceded by descriptions with a double asterisk (**).

Current configuration:

```

!
version 11.3
no service password-encryption
!
hostname myrouter
!
!
! **The following AAA commands are used to configure double authentication:
!
! **The following command enables AAA:
aaa new-model
! **The following command enables user authentication via the TACACS+ AAA server:
aaa authentication login default group tacacs+
aaa authentication login console none
! **The following command enables device authentication via the TACACS+ AAA server:
aaa authentication ppp default group tacacs+
! **The following command causes the remote user's authorization profile to be
! downloaded from the AAA server to the Cisco 2509 router when required:
aaa authorization exec default group tacacs+
! **The following command causes the remote device's authorization profile to be
! downloaded from the AAA server to the Cisco 2509 router when required:
aaa authorization network default group tacacs+
enable password mypassword

```

```

!
ip host blue 172.21.127.226
ip host green 172.21.127.218
ip host red 172.21.127.114
ip domain-name example.com
ip name-server 171.69.2.75
! **The following command globally enables automated double authentication:
ip trigger-authentication timeout 60 port 7500
isdn switch-type basic-5ess
!
!
interface Ethernet0
 ip address 172.21.127.186 255.255.255.248
 no ip route-cache
 no ip mroute-cache
 no keepalive
 ntp disable
 no cdp enable
!
interface Virtual-Template1
 ip unnumbered Ethernet0
 no ip route-cache
 no ip mroute-cache
!
interface Serial0
 ip address 172.21.127.105 255.255.255.248
 encapsulation ppp
 no ip mroute-cache
 no keepalive
 shutdown
 clockrate 2000000
 no cdp enable
!
interface Serial1
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 no cdp enable
!
! **Automated double authentication occurs via the ISDN BRI interface BRI0:
interface BRI0
 ip unnumbered Ethernet0
! **The following command turns on automated double authentication at this interface:
 ip trigger-authentication
! **PPP encapsulation is required:
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 dialer idle-timeout 500
 dialer map ip 172.21.127.113 name myrouter 60074
 dialer-group 1
 no cdp enable

```

```

! **The following command specifies that device authentication occurs via PPP CHAP:
ppp authentication chap
!
router eigrp 109
 network 172.21.0.0
 no auto-summary
!
ip default-gateway 172.21.127.185
no ip classless
ip route 172.21.127.114 255.255.255.255 172.21.127.113
! **Virtual profiles are required for double authentication to work:
virtual-profile virtual-template 1
dialer-list 1 protocol ip permit
no cdp run
! **The following command defines where the TACACS+ AAA server is:
tacacs-server host 171.69.57.35 port 1049
tacacs-server timeout 90
! **The following command defines the key to use with TACACS+ traffic (required):
tacacs-server key mytacacskey
snmp-server community public RO
!
line con 0
 exec-timeout 0 0
 login authentication console
line aux 0
 transport input all
line vty 0 4
 exec-timeout 0 0
 password lab
!
end

```

MS-CHAP Example

The following example shows how to configure a Cisco AS5200 Universal Access Server (enabled for AAA and communication with a RADIUS security server) for PPP authentication using MS-CHAP:

```

aaa new-model
aaa authentication login admins local
aaa authentication ppp dialins group radius local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius

username root password ALongPassword

radius-server host alcatraz
radius-server key myRaDiUSpassWoRd

interface group-async 1
 group-range 1 16
 encapsulation ppp
 ppp authentication ms-chap dialins

line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem dialin

```

The lines in this sample RADIUS AAA configuration are defined as follows:

- The **aaa new-model** command enables AAA network security services.
- The **aaa authentication login admins local** command defines another method list, “admins”, for login authentication.
- The **aaa authentication ppp dialins group radius local** command defines the authentication method list “dialins,” which specifies that RADIUS authentication then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP.
- The **aaa authorization network default group radius local** command is used to assign an address and other network parameters to the RADIUS user.
- The **aaa accounting network default start-stop group radius** command tracks PPP usage.
- The **username** command defines the username and password to be used for the PPP Password Authentication Protocol (PAP) caller identification.
- The **radius-server host** command defines the name of the RADIUS server host.
- The **radius-server key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **interface group-async** command selects and defines an asynchronous interface group.
- The **group-range** command defines the member asynchronous interfaces in the interface group.
- The **encapsulation ppp** command sets PPP as the encapsulation method used on the specified interfaces.
- The **ppp authentication ms-chap dialins** command selects MS-CHAP as the method of PPP authentication and applies the “dialins” method list to the specified interfaces.
- The **line** command switches the configuration mode from global configuration to line configuration and identifies the specific lines being configured.
- The **autoselect ppp** command configures the Cisco IOS software to allow a PPP session to start up automatically on these selected lines.
- The **autoselect during-login** command is used to display the username and password prompt without pressing the Return key. After the user logs in, the autoselect function (in this case, PPP) begins.
- The **login authentication admins** command applies the “admins” method list for login authentication.
- The **modem dialin** command configures modems attached to the selected lines to only accept incoming calls.



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



AAA Double Authentication Secured by Absolute Timeout

First Published: March 1, 2004

Last Updated: January 2, 2008

The AAA Double Authentication Secured by Absolute Timeout feature allows you to secure the double authentication mechanism by protecting it with a per-user session timeout. This feature optimizes the connection to the network by service providers to only connections that are authorized, and it increases the security of the overall access to the network by ensuring that no unwanted sessions are connected.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for AAA Double Authentication Secured by Absolute Timeout](#)” section on page 10.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for AAA Double Authentication Secured by Absolute Timeout, page 2](#)
- [Restrictions for AAA Double Authentication Secured by Absolute Timeout, page 2](#)
- [Information About AAA Double Authentication Secured by Absolute Timeout, page 2](#)
- [How to Apply AAA Double Authentication Secured by Absolute Timeout, page 2](#)
- [Examples for AAA Double Authentication Secured by Absolute Timeout, page 5](#)
- [Additional References, page 8](#)
- [Feature Information for AAA Double Authentication Secured by Absolute Timeout, page 10](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2004–2008 Cisco Systems, Inc. All rights reserved.

Prerequisites for AAA Double Authentication Secured by Absolute Timeout

- You need access to a Cisco RADIUS or TACACS+ server and should be familiar with configuring RADIUS or TACACS+.
- You should be familiar with configuring authentication, authorization, and accounting (AAA).
- You should be familiar with enabling AAA automated double authentication.

Restrictions for AAA Double Authentication Secured by Absolute Timeout

- The AAA Double Authentication Secured by Absolute Timeout feature, like the existing double authentication feature, is for PPP connections only. Automated double authentication cannot be used with other protocols, such as X.25 or Serial Line Internet Protocol (SLIP).
- There may be a minimal impact on performance if a TACACS+ server is used. However, there is no performance impact if a RADIUS server is used.

Information About AAA Double Authentication Secured by Absolute Timeout

To configure the AAA Double Authentication Secured by Absolute Timeout feature, you should understand the following concept:

- [AAA Double Authentication, page 2](#)

AAA Double Authentication

With the current AAA double authentication mechanism, a user must pass the first authentication using a host username and password. The second authentication, after Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP), uses a login username and password. In the first authentication, a PPP session timeout will be applied to the virtual access interface if it is configured locally or remotely. The AAA Double Authentication Secured by Absolute Timeout feature allows you to secure the double authentication mechanism by protecting it with a per-user session timeout. The per-user timeout, which can be customized, supersedes the generic absolute timeout value. This method works on the same principle as per-user access control lists (ACLs) in double authentication.

How to Apply AAA Double Authentication Secured by Absolute Timeout

This section contains the following procedures:

- [Applying AAA Double Authentication Secured by Absolute Timeout, page 3](#)
- [Verifying AAA Double Authentication Secured by Absolute Timeout, page 3](#)

Applying AAA Double Authentication Secured by Absolute Timeout

To apply the absolute timeout, you need to configure “Session-Timeout” in the login user profile as a link control protocol (LCP) per-user attribute. There is no new or modified command-line interface (CLI) for this feature, but before you use the **access-profile** command when enabling AAA double authentication, you must first reauthorize LCP per-user attributes (for example, Session-Timeout) and then reauthorize Network Control Protocols (NCPs) to apply other necessary criteria, such as ACLs and routes. See the “[Examples for AAA Double Authentication Secured by Absolute Timeout](#)” section on [page 5](#).



Note

Timeout configuration in a TACACS+ user profile is a little different from the configuration in a RADIUS user profile. In a RADIUS profile, only one “Session-Timeout” is configured, along with the autocommand “access-profile.” The timeout will be applied to the EXEC session and to the PPP session. In TACACS+, however, the timeout must be configured under the service types “exec” and “ppp” (LCP) to apply a timeout to the EXEC session and to the PPP session. If the timeout is configured only under the service type “ppp,” the timeout value is not available while doing an EXEC authorization—and the timeout will not be applied to the EXEC session.

Verifying AAA Double Authentication Secured by Absolute Timeout

To verify that AAA double authentication has been secured by absolute timeout and to see information about various attributes associated with the authentication, perform the following steps. These **show** and **debug** commands can be used in any order.

SUMMARY STEPS

1. **enable**
 2. **show users**
 3. **show interfaces virtual-access *number* [configuration]**
 4. **debug aaa authentication**
 5. **debug aaa authorization**
 6. **debug aaa per-user**
 7. **debug ppp authentication**
 8. **debug radius**
- or
- debug tacacs**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show users enable Example: Router# show users	Displays information about the active lines on the router.
Step 3	show interfaces virtual-access <i>number</i> [configuration] Example: Router# show interfaces virtual-access 2 configuration	Displays status, traffic data, and configuration information about a specified virtual access interface.
Step 4	debug aaa authentication Example: Router# debug aaa authentication	Displays information about AAA TACACS+ authentication.
Step 5	debug aaa authorization Example: Router# debug aaa authorization	Displays information about AAA TACACS+ authorization.
Step 6	debug aaa per-user Example: Router# debug aaa per-user	Displays the attributes that are applied to each user as the user authenticates.
Step 7	debug ppp authentication Example: Router# debug ppp authentication	Displays whether a user is passing authentication.
Step 8	debug radius Example: Router# debug radius or debug tacacs Example: Router# debug tacacs	Displays information associated with the RADIUS server. or Displays information associated with the TACACS+ server.

Examples

The following sample output is from the **show users** command:

```
Router# show users
```

Line	User	Host(s)	Idle	Location
* 0 con 0	aaapbx2	idle	00:00:00	aaacon2 10
8 vty 0	broker_def	idle	00:00:08	192.168.1.8

Interface	User	Mode	Idle	Peer Address
Vi2	broker_default	VDP	00:00:01	192.168.1.8 <=====
Se0:22	aaapbx2	Sync PPP	00:00:23	

The following sample output is from the **show interfaces virtual-access** command:

```
Router# show interfaces virtual-access 2 configuration
```

Virtual-Access2 is a Virtual Profile (sub)interface

Derived configuration: 150 bytes

```
!
interface Virtual-Access2
  ip unnumbered Serial0:23
  no ip route-cache
  timeout absolute 3 0
! The above line shows that the per-user session timeout has been applied.
  ppp authentication chap
  ppp timeout idle 180000
! The above line shows that the absolute timeout has been applied.
```

Examples for AAA Double Authentication Secured by Absolute Timeout

This section includes the following examples:

- [RADIUS User Profile: Example, page 5](#)
- [TACACS+ User Profile: Example, page 6](#)

RADIUS User Profile: Example

The following sample output shows that a RADIUS user profile has been applied and that AAA double authentication has been secured by an absolute timeout:

```
aaapbx2 Password = "cisco",
  Service-Type = Framed,
  Framed-Protocol = PPP,
  Session-Timeout = 180,
  Idle-Timeout = 180000,
  cisco-avpair = "ip:inacl#1=permit tcp any any eq telnet"
  cisco-avpair = "ip:inacl#2=permit icmp any any"

broker_default Password = "cisco",
  Service-Type = Administrative,
  cisco-avpair = "shell:autocmd=access-profile",
  Session-Timeout = 360,
```

```
cisco-avpair = "ip:inacl#1=permit tcp any any"
cisco-avpair = "ip:inacl#2=permit icmp any any"
```

```
broker_merge Password = "cisco",
  Service-Type = Administrative,
  cisco-avpair = "shell:autocmd=access-profile merge",
  Session-Timeout = 360,
  cisco-avpair = "ip:inacl#1=permit tcp any any"
  cisco-avpair = "ip:inacl#2=permit icmp any any"
  cisco-avpair = "ip:route#3=10.4.0.0 255.0.0.0"
  cisco-avpair = "ip:route#4=10.5.0.0 255.0.0.0"
  cisco-avpair = "ip:route#5=10.6.0.0 255.0.0.0"

broker_replace Password = "cisco",
  Service-Type = Administrative,
  cisco-avpair = "shell:autocmd=access-profile replace",
  Session-Timeout = 360,
  cisco-avpair = "ip:inacl#1=permit tcp any any"
  cisco-avpair = "ip:inacl#2=permit icmp any any"
  cisco-avpair = "ip:route#3=10.4.0.0 255.0.0.0"
  cisco-avpair = "ip:route#4=10.5.0.0 255.0.0.0"
  cisco-avpair = "ip:route#5=10.6.0.0 255.0.0.0"
```

TACACS+ User Profile: Example

The following sample output shows that a TACACS+ user profile has been applied and that AAA double authentication has been secured by an absolute timeout.

Remote Host

The following allows the remote host to be authenticated by the local host during first-stage authentication and provides the remote host authorization profile.

```
user = aaapbx2
  chap = cleartext Cisco
  pap = cleartext cisco
  login = cleartext cisco

service = ppp protocol = lcp
  idletime = 3000
  timeout = 3

service = ppp protocol = ip
  inacl#1="permit tcp any any eq telnet"

service = ppp protocol = ipx
```

access-profile Command Without Any Arguments

Using the **access-profile** command without any arguments causes the removal of any access lists that are found in the old configuration (both per-user and per-interface) and ensures that the new profile contains only access-list definitions.

```
user = broker_default
  login = cleartext Cisco
  chap = cleartext "cisco"

service = exec

  autocmd = "access-profile"
```



```
! This is the autocommand that executes when broker_default logs in.
timeout = 6

service = ppp protocol = lcp
timeout = 6

service = ppp protocol = ip
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!

inacl#1="permit tcp any any"
inacl#2="permit icmp host 10.0.0.0 any"

service = ppp protocol = ipx
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
```

access-profile Command with merge Keyword

With the “merge” option, all old access lists are removed (as before), but then almost any AV pair is allowed to be uploaded and installed. This merge will allow for the uploading of any custom static routes, Service Advertisement Protocol (SAP) filters, and other requirements that the user may need in his or her profile. This merge must be used with care because it leaves everything open in terms of conflicting configurations.

```
user = broker_merge
login = cleartext Cisco
chap = cleartext "cisco"

service = exec

autocmd = "access-profile merge"
! This is the autocommand that executes when broker_merge logs in.
timeout = 6

service = ppp protocol = lcp
timeout = 6

service = ppp protocol = ip
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!

route#1="10.4.0.0 255.0.0.0"
route#2="10.5.0.0 255.0.0.0"
route#3="10.6.0.0 255.0.0.0"
inacl#5="permit tcp any any"
inacl#6="permit icmp host 10.60.0.0 any"

service = ppp protocol = ipx
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!
```

access-profile Command with the replace Keyword

If you use the **access-profile** command with the **replace** keyword, the command works as it does currently; that is, any old configuration is removed and any new configuration is installed.

**Note**

When the **access-profile** command is configured, the new configuration is checked for address pools and address attribute-value (AV) pairs. Because addresses cannot be renegotiated at this point, the command will fail to work when it encounters such an address AV pair.

```

user = broker_replace

login = cleartext Cisco
chap = cleartext "cisco"

service = exec

autocmd = "access-profile replace"
! This is the autocommand that executes when broker_replace logs in.
timeout = 6

service = ppp protocol = lcp
timeout = 6

service = ppp protocol = ip
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!

route#1="10.7.0.0 255.0.0.0"
route#2="10.8.0.0 255.0.0.0"
route#3="10.9.0.0 255.0.0.0"
inacl#4="permit tcp any any"

service = ppp protocol = ipx
! Put access lists, static routes, and other requirements that are
! needed here. Read the software specifications for details. If you leave
! this blank, the user will have no access lists (not even the ones that were
! installed prior to the creation of this user profile)!

```

**Note**

Timeout configuration in a TACACS+ user profile is a little different from the configuration in a RADIUS user profile. In a RADIUS profile, only one “Session-Timeout” is configured, along with the autocommand **access-profile**. The timeout will be applied to the EXEC session and to the PPP session. In TACACS+, however, the timeout must be configured under the service types “exec” and “ppp” (LCP) to apply a timeout to the EXEC session and to the PPP session. If the timeout is configured only under the service type “ppp,” the timeout value is not available while doing an EXEC authorization—and the timeout will not be applied to the EXEC session.

Additional References

The following sections provide references related to AAA Double Authentication Secured by Absolute Timeout.

Related Documents

Related Topic	Document Title
Configuring AAA	“Authentication, Authorization, and Accounting” section of the Cisco IOS Security Configuration Guide , Release 12.4
Enabling AAA Double Authentication	“Configuring Authentication” chapter of the “Authentication, Authorization, and Accounting” section of the Cisco IOS Security Configuration Guide , Release 12.4
Configuring RADIUS	“Configuring RADIUS” chapter of the “Security Server Protocols” section of the Cisco IOS Security Configuration Guide , Release 12.4
Configuring TACACS+	“Configuring TACACS+” chapter of the “Security Server Protocols” section of the Cisco IOS Security Configuration Guide , Release 12.4
Security Commands	Cisco IOS Security Command Reference , Release 12.4

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Feature Information for AAA Double Authentication Secured by Absolute Timeout

Table 1 lists the release history for this feature. Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for AAA Double Authentication Secured by Absolute Timeout

Feature Name	Releases	Feature Information
AAA Double Authentication Secured by Absolute Timeout	12.3(7)T 12.2(28)SB	The AAA Double Authentication Secured by Absolute Timeout feature allows you to secure the double authentication mechanism by protecting it with a per-user session timeout. This feature optimizes the connection to the network by service providers to only connections that are authorized, and it increases the security of the overall access to the network by ensuring that no unwanted sessions are connected.



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2004–2008 Cisco Systems, Inc. All rights reserved.



Login Password Retry Lockout

The Login Password Retry Lockout feature allows system administrators to lock out a local authentication, authorization, and accounting (AAA) user account after a configured number of unsuccessful attempts by the user to log in.

Feature History for Login Password Retry Lockout

Release	Modification
12.3(14)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Login Password Retry Lockout, page 1](#)
- [Restrictions for Login Password Retry Lockout, page 2](#)
- [Information About Login Password Retry Lockout, page 2](#)
- [How to Configure Login Password Retry Lockout, page 2](#)
- [Configuration Examples for Login Password Retry Lockout, page 6](#)
- [Additional References, page 7](#)
- [Command Reference, page 8](#)
- [Glossary, page 9](#)

Prerequisites for Login Password Retry Lockout

- You must be running a Cisco IOS image that contains the AAA component.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Restrictions for Login Password Retry Lockout

- Authorized users can lock themselves out because there is no distinction between an attacker who is guessing passwords and an authorized user who is entering the password incorrectly multiple times.
- A denial of service (DoS) attack is possible, that is, an authorized user could be locked out by an attacker if the username of the authorized user is known to the attacker.

Information About Login Password Retry Lockout

To configure the Login Password Retry Lockout feature, you should understand the following concept:

- [Locking Out a Local AAA User Account, page 2](#)

Locking Out a Local AAA User Account

The Login Password Retry Lockout feature allows system administrators to lock out a local AAA user account after a configured number of unsuccessful attempts by the user to log in using the username that corresponds to the AAA user account. A locked-out user cannot successfully log in again until the user account is unlocked by the administrator.

A system message is generated when a user is either locked by the system or unlocked by the system administrator. The following is an example of such a system message:

```
%AAA-5-USER_LOCKED: User user1 locked out on authentication failure.
```

The system administrator cannot be locked out.



Note

The system administrator is a special user who has been configured using the maximum privilege level (root privilege—level 15). A user who has been configured using a lesser privilege level can change the privilege level using the **enable** command. If the user can change to the root privilege (level 15), that user is able to act as a system administrator.

This feature is applicable to any login authentication method, such as ASCII, Challenge Handshake Authentication Protocol (CHAP), and Password Authentication Protocol (PAP).



Note

No messages are displayed to users after authentication failures that are due to the locked status (that is, there is no distinction between a normal authentication failure and an authentication failure due to the locked status of the user).

How to Configure Login Password Retry Lockout

This section contains the following procedures:

- [Configuring Login Password Retry Lockout, page 3](#)
- [Unlocking a Locked-Out User, page 4](#)
- [Clearing the Unsuccessful Attempts of a User, page 5](#)

- [Monitoring and Maintaining Login Password Retry Lockout, page 5](#)

Configuring Login Password Retry Lockout

To configure Login Password Retry Lockout, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **username** *name* [**privilege** *level*] **password** *encryption-type password*
4. **aaa new-model**
5. **aaa local authentication attempts max-fail** *number-of-unsuccessful-attempts*
6. **aaa authentication login default** *method*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	username name [privilege level] password encryption-type password Example: Router (config)# username user1 privilege 15 password 0 cisco	Establishes a username-based authentication system.
Step 4	aaa new-model Example: Router (config)# aaa new-model	Enables the AAA access control model.
Step 5	aaa local authentication attempts max-fail number-of-unsuccessful-attempts Example: Router (config)# aaa local authentication attempts max-fail 3	Specifies the maximum number of unsuccessful attempts before a user is locked out.
Step 6	aaa authentication login default method Example: Router (config)# aaa authentication login default local	Method list for login, specifying to authenticate using the local AAA user database.

Unlocking a Locked-Out User

To unlock the locked-out user, perform the following steps.

**Note**

This task can be performed only by users having root privilege (level 15).

SUMMARY STEPS

1. enable
2. clear aaa local user logout {username username | all}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	clear aaa local user lockout {username username all} Example: Router# clear aaa local user lockout username user1	Unlocks a locked-out user.

Clearing the Unsuccessful Attempts of a User

To clear the unsuccessful attempts of a user that have already been logged, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **clear aaa local user fail-attempts {username username | all}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	clear aaa local user fail-attempts {username username all} Example: Router# clear aaa local user fail-attempts username user1	Clears the unsuccessful attempts of the user. <ul style="list-style-type: none"> This command is useful for cases in which the user configuration was changed and the unsuccessful attempts that are already logged must be cleared.

Monitoring and Maintaining Login Password Retry Lockout

To monitor and maintain the Login Password Retry Lockout configuration, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show aaa local user locked**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show aaa local user locked Example: Router# show aaa local user locked	Displays a list of the locked-out users.

Configuration Examples for Login Password Retry Lockout

This section provides the following configuration examples:

- [Login Password Retry Lockout: Example, page 6](#)
- [show aaa local user lockout Command: Example, page 7](#)

Login Password Retry Lockout: Example

The following **show running-config** command output illustrates that the maximum number of failed user attempts has been set for 2:

```
Router # show running-config

Building configuration...

Current configuration : 1214 bytes
!
version 12.3
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname LAC-2
!
boot-start-marker
boot-end-marker
!
!
username sysadmin
username sysad privilege 15 password 0 cisco
username user1 password 0 cisco
aaa new-model
aaa local authentication attempts max-fail 2
!
!
aaa authentication login default local
aaa dnis map enable
aaa session-id common
```

show aaa local user lockout Command: Example

The following output shows that user1 is locked out:

```
Router# show aaa local user lockout
```

Local-user	Lock time
user1	04:28:49 UTC Sat Jun 19 2004

Additional References

The following sections provide references related to Login Password Retry Lockout.

Related Documents

Related Topic	Document Title
Cisco IOS security commands	Cisco IOS Security Command Reference, Release 12.3T

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information

about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **aaa local authentication attempts max-fail**
- **clear aaa local user fail-attempts**
- **clear aaa local user logout**

Glossary

- **Local AAA method**—Method by which it is possible to configure a local user database on a router and to have AAA provision authentication or authorization of users from this database.
- **Local AAA user**—User who is authenticated using the Local AAA method.



Note

Refer to [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



MSCHAP Version 2

First Published: January 23, 2003

Last Updated: April 17, 2006

The MSCHAP Version 2 feature (introduced in Cisco IOS Release 12.2(2)XB5) allows Cisco routers to utilize Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) authentication for PPP connections between a computer using a Microsoft Windows operating system and a network access server (NAS).

For Cisco IOS Release 12.4(6)T, MSCHAP V2 now supports a new feature: AAA Support for MSCHAPv2 Password Aging. Prior to Cisco IOS Release 12.4(6)T, when Password Authentication Protocol (PAP)-based clients sent username and password values to the authentication, authorization, and accounting (AAA) subsystem, AAA generated an authentication request to the RADIUS server. If the password expired, the RADIUS server replied with an authentication failure message. The reason for the authentication failure was not passed back to AAA subsystem; thus, users were denied access because of authentication failure but were not informed why they were denied access.

The Password Aging feature, available in Cisco IOS Release 12.4(6)T, notifies crypto-based clients that the password has expired and provides a generic way for the user to change the password. The Password Aging feature supports only crypto-based clients.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for MSCHAP Version 2](#)” section on page 11.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Contents

This document includes the following sections:

- [Prerequisites for MSCHAP Version 2, page 2](#)
- [Restrictions for MSCHAP Version 2, page 2](#)
- [Information About MSCHAP Version 2, page 3](#)
- [How to Configure MSCHAP Version 2, page 3](#)
- [Configuration Examples, page 6](#)
- [Additional References, page 8](#)
- [Command Reference, page 11](#)
- [Feature Information for MSCHAP Version 2, page 11](#)

Prerequisites for MSCHAP Version 2

- Configure an interface type and enter interface configuration mode by using the **interface** command.
- Configure the interface for PPP encapsulation by using the **encapsulation** command.
- Be sure that the client operating system supports all MSCHAP V2 capabilities.
- For Cisco IOS Release 12.4(6)T, the Password Aging feature only supports RADIUS authentication for crypto-based clients.
- To ensure that the MSCHAP Version 2 features correctly interpret the authentication failure attributes sent by the RADIUS server, you must configure the **ppp max-bad-auth** command and set the number of authentication retries at two or more.
- In order for the MSCHAP Version 2 feature to support the ability to change a password, the authentication failure attribute, which is sent by the RADIUS server, must be correctly interpreted as described in “[Configuring MSCHAP V2 Authentication](#)” section on page 3.

In addition, the **radius server vsa send authentication** command must be configured, allowing the RADIUS client to send a vendor-specific attribute to the RADIUS server. The Change Password feature is supported only for RADIUS authentication.

- The Microsoft Windows 2000, Microsoft Windows XP, and Microsoft Windows NT operating systems have a known caveat that prevents the Change Password feature from working. You must download a patch from Microsoft at the following URL:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q326770>

For more information on completing these tasks, see the section “PPP Configuration” in the [Cisco IOS Dial Technologies Configuration Guide](#), Release 12.2. The RADIUS server must be configured for authentication. Refer to vendor-specific documentation for information on configuring RADIUS authentication on the RADIUS server.

Restrictions for MSCHAP Version 2

- MSCHAP V2 authentication is not compatible with MSCHAP V1 authentication.
- The change password option is supported only for RADIUS authentication and is not available for local authentication.

Information About MSCHAP Version 2

MSCHAP V2 authentication is the default authentication method used by the Microsoft Windows 2000 operating system. Cisco routers that support this authentication method enable Microsoft Windows 2000 operating system users to establish remote PPP sessions without configuring an authentication method on the client.

MSCHAP V2 authentication introduced an additional feature not available with MSCHAP V1 or standard CHAP authentication: the Change Password feature. This feature allows the client to change the account password if the RADIUS server reports that the password has expired.

**Note**

MSCHAP V2 authentication is an updated version of MSCHAP that is similar to but incompatible with MSCHAP Version 1 (V1). MSCHAP V2 introduces mutual authentication between peers and a Change Password feature.

How to Configure MSCHAP Version 2

See the following sections for configuration tasks for the MSCHAP Version 2 feature.


- [“Configuring MSCHAP V2 Authentication” section on page 3](#) (required)
- [“Verifying MSCHAP V2 Configuration” section on page 5](#) (optional)
- [“Configuring Password Aging for Crypto-Based Clients” section on page 5](#) (optional)

Configuring MSCHAP V2 Authentication

To configure the NAS to accept MSCHAP V2 authentication for local or RADIUS authentication and to allow proper interpretation of authentication failure attributes and vendor-specific RADIUS attributes for RADIUS authentication, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server vsa send authentication**
4. **interface** *type number*
5. **ppp max-bad-auth** *number*
6. **ppp authentication ms-chap-v2**
7. **end**

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	radius-server vsa send authentication Example: Router(config)# radius-server vsa send authentication	Configures the NAS to recognize and use vendor-specific attributes.
Step 4	interface type number Example: Router(config)# interface FastEthernet 0/1	Configures an interface type and enters interface configuration mode.
Step 5	ppp max-bad-auth number Example: Router(config-if)# ppp max-bad-auth 2	Configures a point-to-point interface to reset immediately after an authentication failure or within a specified number of authentication retries. <ul style="list-style-type: none"> The default value for the <i>number</i> argument is 0 seconds (immediately). The range is between 0 and 255. <div>  Note The <i>number</i> argument must be set to a value of at least 2 for authentication failure attributes to be interpreted by the NAS. </div>
Step 6	ppp authentication ms-chap-v2 Example: Router(config-if)# ppp authentication ms-chap-v2	Enables MSCHAP V2 authentication on a NAS.
Step 7	end Example: Router(config-if)# end	Returns to privileged EXEC mode.

Verifying MSCHAP V2 Configuration

To verify that the MSCHAP Version 2 feature is configured properly, perform the following steps.

SUMMARY STEPS

1. **show running-config interface** *type number*
2. **debug ppp negotiation**
3. **debug ppp authentication**

DETAILED STEPS

	Command or Action	Purpose
Step 1	show running-config interface <i>type number</i> Example: Router# show running-config interface Asynch65	Verifies the configuration of MSCHAP V2 as the authentication method for the specified interface.
Step 2	debug ppp negotiation Example: Router# debug ppp negotiation	Verifies successful MSCHAP V2 negotiation.
Step 3	debug ppp authentication Example: Router# debug ppp authentication	Verifies successful MSCHAP V2 authentication.

Configuring Password Aging for Crypto-Based Clients

The AAA security services facilitate a variety of login authentication methods. Use the **aaa authentication login** command to enable AAA authentication no matter which of the supported login authentication methods you decide to use. With the **aaa authentication login** command, you create one or more lists of authentication methods that are tried at login. These lists are applied using the **login authentication** line configuration command.

After the RADIUS server requests a new password, AAA queries the crypto client, which in turn prompts the user to enter a new password.

To configure login authentication and password aging for crypto-based clients, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** {**default** | *list-name*} **passwd-expiry** *method1* [*method2*...]
5. **crypto map** *map-name* **client authentication list** *list-name*

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Router(config)# aaa new-model	Enables AAA globally.
Step 4	aaa authentication login {default list-name} passwd-expiry method1 [method2...] Example: Router(config)# aaa authentication login userauthen passwd-expiry group radius	Enables password aging for crypto-based clients on a local authentication list.
Step 5	crypto map map-name client authentication list list-name Example: Router(config)# crypto map clientmap client authentication list userauthen	Configures user authentication (a list of authentication methods) on an existing crypto map.

Configuration Examples

This section provides the following configuration examples:

- [“Configuring Local Authentication: Example” section on page 6](#)
- [“Configuring RADIUS Authentication: Example” section on page 7](#)
- [“Configuring Password Aging with Crypto Authentication: Example” section on page 7](#)

Configuring Local Authentication: Example

The following example configures PPP on an asynchronous interface and enables MSCHAP V2 authentication locally:

```
interface Async65
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 async mode dedicated
 no peer default ip address
 ppp max-bad-auth 3
 ppp authentication ms-chap-v2
 username client password secret
```

Configuring RADIUS Authentication: Example

The following example configures PPP on an asynchronous interface and enables MSCHAP V2 authentication via RADIUS:

```
interface Async65
  ip address 10.0.0.2 255.0.0.0
  encapsulation ppp
  async mode dedicated
  no peer default ip address
  ppp max-bad-auth 3
  ppp authentication ms-chap-v2
  exit
aaa authentication ppp default group radius
radius-server host 10.0.0.2 255.0.0.0
radius-server key secret
radius-server vsa send authentication
```

Configuring Password Aging with Crypto Authentication: Example

The following example configures password aging by using AAA with a crypto-based client:

```
aaa authentication login userauthen passwd-expiry group radius
!
aaa session-id common
!
crypto isakmp policy 3
  encr 3des
  authentication pre-share
  group 2
!
crypto isakmp client configuration group 3000client
  key cisco123
  dns 10.1.1.10
  wins 10.1.1.20
  domain cisco.com
  pool ippool
  acl 153
!
crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
crypto dynamic-map dynmap 10
  set transform-set myset
!
crypto map clientmap client authentication list userauthen
!
radius-server host 10.140.15.203 auth-port 1645 acct-port 1646
radius-server domain-stripping prefix-delimiter $
radius-server key cisco123
radius-server vsa send authentication
radius-server vsa send authentication 3gpp2
!
end
```

Additional References

The following sections provide references related to the MSCHAP Version 2 feature.

Related Documents

Related Topic	Document Title
Configuring PPP interfaces	The section “PPP Configuration” in the <i>Cisco IOS Dial Technologies Configuration Guide</i> , Release 12.2.
Descriptions of the tasks and commands necessary to configure and maintain Cisco networking devices	<i>Cisco IOS Dial Technologies Command Reference</i> , Release 12.2
Lists of IOS Security Commands	<i>Cisco IOS Security Command Reference</i> , Release 12.2
Configuring PPP authentication using AAA	The section “Configuring PPP Authentication Using AAA” in the chapter “Configuring Authentication” in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.2
Configuring RADIUS Authentication	The chapter “Configuring RADIUS” in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.2

Standards

Standard	Title
No new or modified standards are supported by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1661	Point-to-Point Protocol (PPP)
RFC 2548	Microsoft Vendor-specific RADIUS Attributes
RFC 2759	<i>Microsoft PPP CHAP Extensions, Version 2</i>

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **aaa authentication login**
- **ppp authentication ms-chap-v2**

Feature Information for MSCHAP Version 2

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for MSCHAP Version 2

Feature Name	Releases	Feature Information
MSCHAP Version 2	12.2(2)XB5 12.2(13)T 12.4(6)T	<p>The MSCHAP Version 2 feature (introduced in Cisco IOS Release 12.2(2)XB5) allows Cisco routers to utilize Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) authentication for PPP connections between a computer using a Microsoft Windows operating system and a network access server (NAS).</p> <p>In 12.2(2)XB5, this feature was introduced.</p> <p>In 12.2(13)T, this feature was integrated into Cisco IOS Release 12.2(13)T.</p> <p>In 12.4(6)T, this feature was updated to include the crypto-based Password Aging feature.</p>

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



RADIUS EAP Support

First Published: October 15, 2001

Last Updated: February 28, 2006

The RADIUS EAP Support feature allows users to apply to the client authentication methods that may not be supported by the network access server; this is done via the Extensible Authentication Protocol (EAP). Before this feature was introduced, support for various authentication methods for PPP connections required custom vendor-specific work and changes to the client and NAS.

History for the RADIUS EAP Support Feature

Release	Modification
12.2(2)XB5	This feature was introduced on the Cisco 2650, Cisco 3640, Cisco 3660, Cisco AS5300, and Cisco AS400 platforms.
12.2(13)T	This feature was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Feature Overview, page 2](#)
- [Prerequisites, page 3](#)
- [Configuration Tasks, page 3](#)
- [Configuration Examples, page 4](#)
- [Additional References, page 6](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Command Reference, page 8](#)
- [Glossary, page 9](#)

Feature Overview

EAP is an authentication protocol for PPP that supports multiple authentication mechanisms that are negotiated during the authentication phase (instead of the link control protocol [LCP] phase). EAP allows a third-party authentication server to interact with a PPP implementation through a generic interface.

How EAP Works

By default, EAP runs in proxy mode. This means that EAP allows the entire authentication process to be negotiated by the NAS to a back-end server that may reside on or be accessed via a RADIUS server. After EAP is negotiated between the client and the NAS during LCP exchange, all further authentication messages are transparently transmitted between the client and the back-end server. The NAS is no longer directly involved in the authentication process; that is, the NAS works as a proxy, sending EAP messages between the remote peers.



Note

EAP can also run in a local mode; the session is authenticated using the Message Digest 5 (MD5) algorithm and obeys the same authentication rules as Challenge Handshake Authentication Protocol (CHAP). To disable proxy mode and authenticate locally, you must use the **ppp eap local** command.

Newly Supported Attributes

The RADIUS EAP Support feature introduces support for the following RADIUS attributes:

Number	IETF Attribute	Description
79	EAP-Message	Encapsulates one fragment of an EAP message, which includes the PPP type, request-id, length, and EAP-type fields.
80	Message Authenticator	Ensures source integrity of the message; all messages that are received with invalid checksums are silently discarded by either end. This attribute contains an HMAC-MD5 checksum of the entire RADIUS request or response message and uses the RADIUS server secret as the key.

Benefits

The RADIUS EAP Support feature makes it possible to apply to the client various authentication methods within PPP (including proprietary authentication) that are not supported by the NAS. Thus, customers can use standard support mechanisms for authentication schemes, such as token cards and public key, to strengthen end-user and device authenticated access to their networks.

Restrictions

When EAP is running in proxy mode, there may be a significant increase in the authentication time because every packet from the peer must be sent to the RADIUS server and every EAP packet from the RADIUS server must be sent back to the client. Although this extra processing will cause delays, you can increase the default authentication timeout value by using the **ppp timeout authentication** command.

Prerequisites

Before enabling EAP RADIUS on the client, you must perform the following tasks:

- Configure an interface type and enter interface configuration mode by using the **interface** command.
- Configure the interface for PPP encapsulation by using the **encapsulation** command.

For more information on completing these tasks, refer to the chapter “Configuring Media-Independent PPP and Multilink PPP” in the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.4.

Configuration Tasks

See the following sections for configuration tasks for the RADIUS EAP Support feature. Each task in the list is identified as either required or optional.

- [Configuring EAP, page 3](#) (required)
- [Verifying EAP, page 4](#) (optional)

Configuring EAP

To configure EAP on an interface configured for PPP encapsulation, use the following commands in interface configuration mode:

Command	Purpose
Router(config-if)# ppp authentication eap	Enables EAP as the authentication protocol.
Router(config-if)# ppp eap identity <i>string</i>	(Optional) Specifies the EAP identity when requested by the peer.
Router(config-if)# ppp eap password [<i>number</i>] <i>string</i>	(Optional) Sets the EAP password for peer authentication. Note This command should only be configured on the client.
Router(config-if)# ppp eap local	(Optional) Authenticates locally instead of using a RADIUS back-end server, which is the default. Note This command should only be configured on the NAS.

Command	Purpose
Router(config-if)# ppp eap wait	(Optional) Waits for the caller to authenticate itself first. By default, the client always authenticates itself before the caller does. Note This command should only be configured on the NAS.
Router(config-if)# ppp eap refuse [callin]	(Optional) Refuses to authenticate using EAP. If the callin keyword is enabled, only incoming calls will not be authenticated. Note This command should only be configured on the NAS.

Verifying EAP

To verify EAP configurations on your client or NAS, use at least one of the following commands in privileged EXEC configuration mode:

Command	Purpose
Router# show users	Displays information about the active lines on the router.
Router# show interfaces	Displays statistics for all interfaces configured on the router or access server.
Router# show running-config	Ensures that your configurations appear as part of the running configuration.

Configuration Examples

This section provides the following configuration examples:

- [EAP Local Configuration on Client Example, page 4](#)
- [EAP Proxy Configuration for NAS Example, page 5](#)

EAP Local Configuration on Client Example

The following example is a sample configuration for a client configured for EAP:

```
interface Ethernet0/0
 ip address 10.1.1.202 255.255.255.0
 no ip mroute-cache
 half-duplex
!
interface BRI0/0
 ip address 192.168.101.100 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 dialer map ip 192.168.101.101 56167
 dialer-group 1
 isdn switch-type basic-5ess
 ppp eap identity user
 ppp eap password 7 141B1309
!
```



```

!
ip default-gateway 10.1.1.1
ip classless
ip route 192.168.101.101 255.255.255.255 BRI0/0
no ip http server
!
dialer-list 1 protocol ip permit

```

EAP Proxy Configuration for NAS Example

The following example is a sample configuration for a NAS configured to use EAP proxy:

```

aaa authentication login default group radius
aaa authentication login NOAUTH none
aaa authentication ppp default if-needed group radius
aaa session-id common
enable secret 5 $1$x5D0$cfTL/D8Be.34PgTbdGdgl/
!
username dtw5 password 0 lab
username user password 0 lab

ip subnet-zero
no ip domain-lookup
ip host lab24-boot 172.19.192.254
ip host lb 172.19.192.254
!
isdn switch-type primary-5ess
!
controller T1 3
    framing esf
    linecode b8zs
    pri-group timeslots 1-24
!
interface Ethernet0
    ip address 10.1.1.108 255.255.255.0
    no ip route-cache
    no ip mroute-cache
!
interface Serial3:23
    ip address 192.168.101.101 255.255.255.0
    encapsulation ppp
    dialer map ip 192.168.101.100 60213
    dialer-group 1
    isdn switch-type primary-5ess
    isdn T321 0
    ppp authentication eap
    ppp eap password 7 011F0706
!
!
ip default-gateway 10.0.190.1
ip classless
ip route 192.168.101.0 255.255.255.0 Serial3:23
no ip http server
!
dialer-list 1 protocol ip permit
!
radius-server host 10.1.1.201 auth-port 1645 acct-port 1646 key lab
radius-server retransmit 3
call rsvp-sync
!
mgcp profile default
!

```

```
!  
line con 0  
  exec-timeout 0 0  
  logging synchronous  
  login authentication NOAUTH  
line 1 48  
line aux 0  
ine vty 0 4  
lpassword lab
```

Additional References

The following sections provide references related to RADIUS EAP Support.

Related Documents

Related Topic	Document Title
Configuring PPP Authentication Using AAA	“Configuring Authentication” chapter in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4
Configuring RADIUS	<i>Cisco IOS Security Configuration Guide</i> , Release 12.4
PPP Configuration	<i>Cisco IOS Dial Technologies Configuration Guide</i> , Release 12.4
Dial Technologies commands	<i>Cisco IOS Dial Technologies Command Reference</i> , Release 12.4T
Security Commands	<i>Cisco IOS Security Command Reference</i> , Release 12.4T

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2284	<i>PPP Extensible Authentication Protocol (EAP)</i>
RFC 1938	<i>A One-Time Password System</i>
RFC 2869	<i>RADIUS Extensions</i>

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **ppp authentication**
- **ppp eap identity**
- **ppp eap local**
- **ppp eap password**
- **ppp eap refuse**
- **ppp eap wait**

Glossary

attribute—A RADIUS Internet Engineering Task Force (IETF) attribute is one of the original set of 255 standard attributes that are used to communicate authentication, authorization, and accounting (AAA) information between a client and a server. Because IETF attributes are standard, the attribute data is predefined and well known; thus all clients and servers that exchange AAA information via IETF attributes must agree on attribute data such as the exact meaning of the attributes and the general bounds of the values for each attribute.

CHAP—Challenge Handshake Authentication Protocol. Security feature that is supported on lines using PPP encapsulation and prevents unauthorized access. CHAP does not itself prevent unauthorized access; it merely identifies the remote end. The router or access server then determines whether that user is allowed access.

EAP—Extensible Authentication Protocol. A PPP authentication protocol that supports multiple authentication mechanisms that are negotiated during the authentication phase (instead of the Link Control Protocol [LCP] phase). EAP allows a third-party authentication server to interact with the PPP implementation through a generic interface.

LCP—link control protocol. Protocol that establishes, configures, and tests data-link connections for use by PPP.

MD5 (HMAC variant)—Message Digest 5. A hash algorithm used to authenticate packet data. HMAC is a key hashing for message authentication.

NAS—network access server. A device providing local network access to users across a remote access network such as the public switched telephone network (PSTN).

PAP—Password Authentication Protocol. Authentication protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike CHAP, PAP passes the password and host name or username in the clear (unencrypted). PAP does not itself prevent unauthorized access; it merely identifies the remote end. The router or access server then determines if that user is allowed access. PAP is supported only on PPP lines.

PPP—Point-to-Point Protocol. A protocol that encapsulates network layer protocol information over point-to-point links. PPP is defined in RFC 1661.

RADIUS—Remote Authentication Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time.

**Note**

See [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



RADIUS Packet of Disconnect

Feature History

Release	Modification
12.1(2)XH	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.2(2)XB	Support for the voice applications as well as support for the Cisco AS5350, Cisco AS5400, and Cisco 3600 series routers was added.
12.2(2)XB1	Support for the Cisco AS5800 was added.
12.2(11)T	This feature was integrated into Cisco IOS Release 12.2(11)T and support for the Cisco AS5850 was added.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

This document describes the RADIUS Packet of Disconnect feature in Cisco IOS Release 12.2(11)T. It includes the following sections.

[Feature Overview, page 2](#)

[Supported Platforms, page 4](#)

[Supported Standards, MIBs, and RFCs, page 6](#)

[Prerequisites, page 6](#)

[Configuration Tasks, page 6](#)

[Configuration Examples, page 9](#)

[Command Reference, page 9](#)

[Glossary, page 10](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Feature Overview

This feature consists of a method for terminating a call that has already been connected. This “Packet of Disconnect” (POD) is a RADIUS `access_request` packet and is intended to be used in situations where the authenticating agent server wants to disconnect the user after the session has been accepted by the RADIUS `access_accept` packet. This may be needed in at least two situations:

- Detection of fraudulent use, which cannot be performed before accepting the call. A price structure so complex that the maximum session duration cannot be estimated before accepting the call. This may be the case when certain types of discounts are applied or when multiple users use the same subscription simultaneously.
- To prevent unauthorized servers from disconnecting users, the authorizing agent that issues the POD packet must include three parameters in its packet of disconnect request. For a call to be disconnected, all parameters must match their expected values at the gateway. If the parameters do not match, the gateway discards the packet of disconnect packet and sends a NACK (negative acknowledgement message) to the agent.

The parameters are the following:

- An `h323-conf-id` vendor-specific attribute (VSA) with the same content as received from the gateway for this call.
- An `h323-call-origin` VSA with the same content as received from the gateway for the leg of interest.
- A 16-byte MD5 hash value that is carried in the *authentication* field of the POD request.

Benefits

- Ability to terminate an in-progress voice call

Restrictions

Proper matching identification information must be communicated by the:

- billing server and gateway configuration
- the gateway’s original accounting start request
- the server’s POD request

Related Features and Technologies

- AAA, documented in the *Cisco IOS Security Configuration Guide*, Release 12.2

Related Documents

- *Cisco IOS Security Configuration Guide*, Release 12.2
- *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2
- *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2

- *Cisco IOS Voice, Video, and Fax Command Reference*, Release 12.2

Supported Platforms

- Cisco 3600 series
- Cisco AS5300
- Cisco AS5350
- Cisco AS5400
- Cisco AS5800
- Cisco AS5850

Table 1 *Release and Platform Support for this Feature*

Platform	First Limited Cisco IOS Lifetime Release	First Cisco IOS T Release
Cisco 3600 Series	12.2(2)XB	12.2(11)T
Cisco 5300	12.1(2)XH	12.1(3)T
Cisco 5350	12.2(2)XB	12.2(11)T
Cisco 5400	12.2(2)XB	12.2(11)T
Cisco 5800	12.1(2)XH	12.1(3)T
Cisco 5850	X	12.2(11)T
RADIUS Packet of Disconnect	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
RADIUS Packet of Disconnect	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB web site on Cisco.com at

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

RFCs

- RFC 2865, *Remote Authentication Dial-in User Service*

Prerequisites

- Configure AAA as described in *Cisco IOS Security Configuration Guide*, Cisco IOS Release 12.2.
- Use Cisco IOS Release 12.2(11)T or later.

Configuration Tasks

See the following sections for configuration tasks for this Packet of Disconnect feature. Each task in the list is identified as either required or optional.

- [Configuring AAA POD Server](#) (required)
- [Verifying AAA POD Server](#) (optional)

Configuring AAA POD Server

To configure POD, perform the following tasks in global configuration mode:

	Command	Purpose
Step 1	<pre>Router(config)# aaa pod server [port port-number] [auth-type {any all session-key}] server-key [encryption-type] <i>string</i></pre>	<p>Enables inbound user sessions to be disconnected when specific session attributes are presented.</p> <p>port <i>port-number</i>—(Optional) The network access server User Datagram Protocol (UDP) port to use for POD requests. Default value is 1700.</p> <p>auth-type—(Optional) The type of authorization required for disconnecting sessions.</p> <p>any—Session that matches all of the attributes sent in the POD packet is disconnected. The POD packet may contain one or more of four key attributes (user-name, framed-IP-address, session-ID, and session-key).</p> <p>all—Only a session that matches all four key attributes is disconnected. All is the default.</p> <p>session-key—Session with a matching session-key attribute is disconnected. All other attributes are ignored.</p> <p>server-key—Configures the shared-secret text string.</p> <p>encryption-type—(Optional) Single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Defined encryption types are 0, which means that the text immediately following is not encrypted, and 7, which means that the text is encrypted using an encryption algorithm defined by Cisco.</p> <p><i>string</i>—The shared-secret text string that is shared between the network access server and the client workstation. This shared-secret string must be the same on both systems.</p>

Verifying AAA POD Server

To verify that the gateway is configured correctly to perform as an AAA POD server, enter the **show running-configuration** command in privileged EXEC mode to display the command settings for the router.

```
Router# show running-configuration
!
aaa authentication login h323 group radius
aaa authorization exec h323 group radius
aaa accounting update newinfo
aaa accounting connection h323 start-stop group radius
aaa pod server server-key cisco
aaa session-id common
!
```

Troubleshooting Tips

- Ensure that the POD port is configured correctly in both the gateway(using **aaa pod server** command) and the radius server. Both should be the same.
- Ensure that the shared-secret key configured in the gateway (using **aaa pod server** command) and in the AAA server are the same.
- Turn on **debug aaa pod** command to see what's going on. This will let you know if the gateway receives the POD packet from the server and if so, it will display any errors encountered.

The following example shows output from a successful POD request, when using the **show debug** command.

```
Router# debug aaa pod
AAA POD packet processing debugging is on
Router# show debug
General OS:
  AAA POD packet processing debugging is on
Router#
Apr 25 17:15:59.318:POD:172.19.139.206 request queued
Apr 25 17:15:59.318:voice_pod_request:
Apr 25 17:15:59.318:voip_populate_pod_attr_list:
Apr 25 17:15:59.318:voip_pod_get_guid:
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr_len=50
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr=h323-conf-id
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr_len=50 value_len=35
Apr 25 17:15:59.318:voip_pod_get_guid:conf-id=FFA7785F F7F607BB
00000000 993FB1F4 n_bytes=35
Apr 25 17:15:59.318:voip_pod_get_guid:GUID = FFA7785F F7F607BB 00000000

993FB1F4
Apr 25 17:15:59.318:voip_populate_pod_attr_list:
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr_len=23
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr=h323-originate
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr_len=23 value_len=6
Apr 25 17:15:59.318:voip_get_call_direction:
Apr 25 17:15:59.318:voip_get_call_direction:returning answer
Apr 25 17:15:59.318:voip_eval_pod_attr:
Apr 25 17:15:59.318:cc_api_trigger_disconnect:
Apr 25 17:15:59.322:POD:Sending ACK to 172.19.139.206/1700
Apr 25 17:15:59.322:voip_pod_clean:
```

Configuration Examples

This section provides a configuration example for a gateway performing as an AAA POD server:

- [AAA POD Server Example](#)

AAA POD Server Example

```
Router(config)# aaa pod server server-key xyz123
```

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **aaa pod server**
- **debug aaa pod**

Glossary

AAA—authentication, authorization, and accounting.

NACK—negative acknowledgement message.

POD—packet of disconnect. An access_reject packet sent from a RADIUS server to the gateway in order to disconnect a call which has been connected already. After validation of the packet, the gateway disconnects the user. The packet contains the information to disconnect the call.

POD server—a Cisco gateway configured to accept and process POD requests from a RADIUS authentication/authorization agent.

RADIUS—Remote Authentication Dial-In User Service. An authentication and accounting system used by many Internet service providers.

UDP—User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

VoIP—voice over IP. The ability to carry normal telephony-style voice over an IP-based Internet with POTS-like functionality, reliability, and voice quality. VoIP is a blanket term that generally refers to the Cisco standards-based (for example, H.323) approach to IP voice traffic.

VSA—vendor-specific attribute.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Configuring Authorization

Feature History

Release	Modification
Cisco IOS	For information about feature support in Cisco IOS software, use Cisco Feature Navigator.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

AAA authorization enables you to limit the services available to a user. When AAA authorization is enabled, the network access server uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's session. Once this is done, the user will be granted access to a requested service only if the information in the user profile allows it.

For a complete description of the authorization commands used in this chapter, refer to the chapter "Authorization Commands" in the *Cisco IOS Security Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the chapter "Identifying Supported Platforms" section in the "Using Cisco IOS Software."

In This Chapter

This chapter contains the following sections:

- [Named Method Lists for Authorization](#)
- [AAA Authorization Methods](#)
- [Method Lists and Server Groups](#)
- [AAA Authorization Types](#)
- [AAA Authorization Prerequisites](#)
- [AAA Authorization Configuration Task List](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Authorization Attribute-Value Pairs](#)
- [Authorization Configuration Examples](#)

Named Method Lists for Authorization

Method lists for authorization define the ways that authorization will be performed and the sequence in which these methods will be performed. A method list is simply a named list describing the authorization methods to be queried (such as RADIUS or TACACS+), in sequence. Method lists enable you to designate one or more security protocols to be used for authorization, thus ensuring a backup system in case the initial method fails. Cisco IOS software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or all methods defined are exhausted.



Note

The Cisco IOS software attempts authorization with the next listed method only when there is no response from the previous method. If authorization fails at any point in this cycle—meaning that the security server or local username database responds by denying the user services—the authorization process stops and no other authorization methods are attempted.

Method lists are specific to the authorization type requested:

- **Auth-proxy**—Applies specific security policies on a per-user basis. For detailed information on the authentication proxy feature, refer to the chapter “Configuring Authentication Proxy” in the “Traffic Filtering and Firewalls” part of this book.
- **Commands**—Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- **EXEC**—Applies to the attributes associated with a user EXEC terminal session.
- **Network**—Applies to network connections. This can include a PPP, SLIP, or ARAP connection.
- **Reverse Access**—Applies to reverse Telnet sessions.

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type.

Once defined, method lists must be applied to specific lines or interfaces before any of the defined methods will be performed. The only exception is the default method list (which is named “default”). If the **aaa authorization** command for a particular authorization type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, local authorization takes place by default.

AAA Authorization Methods

AAA supports five different methods of authorization:

- **TACACS+**—The network access server exchanges authorization information with the TACACS+ security daemon. TACACS+ authorization defines specific rights for users by associating attribute-value pairs, which are stored in a database on the TACACS+ security server, with the appropriate user.

- **If-Authenticated**—The user is allowed to access the requested function provided the user has been authenticated successfully.
- **None**—The network access server does not request authorization information; authorization is not performed over this line/interface.
- **Local**—The router or access server consults its local database, as defined by the **username** command, for example, to authorize specific rights for users. Only a limited set of functions can be controlled via the local database.
- **RADIUS**—The network access server requests authorization information from the RADIUS security server. RADIUS authorization defines specific rights for users by associating attributes, which are stored in a database on the RADIUS server, with the appropriate user.

Method Lists and Server Groups

A server group is a way to group existing RADIUS or TACACS+ server hosts for use in method lists. [Figure 5](#) shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers, and T1 and T2 are TACACS+ servers. R1 and R2 make up the group of RADIUS servers. T1 and T2 make up the group of TACACS+ servers.

Figure 5 *Typical AAA Network Configuration*



Using server groups, you can specify a subset of the configured server hosts and use them for a particular service. For example, server groups allow you to define R1 and R2 as separate server groups, and T1 and T2 as separate server groups. This means you can specify either R1 and T1 in the method list or R2 and T2 in the method list, which provides more flexibility in the way that you assign RADIUS and TACACS+ resources.

Server groups also can include multiple host entries for the same server, as long as each entry has a unique identifier. The combination of an IP address and a UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. In other words, this unique identifier enables RADIUS requests to be sent to different UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, authorization—the second host entry configured acts as fail-over

backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The RADIUS host entries will be tried in the order they are configured.)

For more information about configuring server groups and about configuring server groups based on DNIS numbers, refer to the chapter “Configuring RADIUS” or the chapter “Configuring TACACS+”

AAA Authorization Types

Cisco IOS software supports five different types of authorization:

- **Auth-proxy**—Applies specific security policies on a per-user basis. For detailed information on the authentication proxy feature, refer to the “Configuring Authentication Proxy” chapter in the “Traffic Filtering and Firewalls” section of this book.
- **Commands**—Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- **EXEC**—Applies to the attributes associated with a user EXEC terminal session.
- **Network**—Applies to network connections. This can include a PPP, SLIP, or ARAP connection.
- **Reverse Access**—Applies to reverse Telnet sessions.
- **Configuration**—Applies to downloading configurations from the AAA server.
- **IP Mobile**—Applies to authorization for IP mobile services.

AAA Authorization Prerequisites

Before configuring authorization using named method lists, you must first perform the following tasks:

- Enable AAA on your network access server. For more information about enabling AAA on your Cisco router or access server, refer to the “AAA Overview” chapter.
- Configure AAA authentication. Authorization generally takes place after authentication and relies on authentication to work properly. For more information about AAA authentication, refer to the “Configuring Authentication” chapter.
- Define the characteristics of your RADIUS or TACACS+ security server if you are issuing RADIUS or TACACS+ authorization. For more information about configuring your Cisco network access server to communicate with your RADIUS security server, refer to the chapter “Configuring RADIUS”. For more information about configuring your Cisco network access server to communicate with your TACACS+ security server, refer to the chapter “Configuring TACACS+”.
- Define the rights associated with specific users by using the **username** command if you are issuing local authorization. For more information about the **username** command, refer to the *Cisco IOS Security Command Reference*.

AAA Authorization Configuration Task List

This section describes the following configuration tasks:

- [Configuring AAA Authorization Using Named Method Lists](#)

- [Disabling Authorization for Global Configuration Commands](#)
- [Configuring Authorization for Reverse Telnet](#)

For authorization configuration examples using the commands in this chapter, refer to the section “[Authorization Configuration Examples](#)” at the end of the this chapter.

Configuring AAA Authorization Using Named Method Lists

To configure AAA authorization using named method lists, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# aaa authorization { auth-proxy network exec commands <i>level</i> reverse-access configuration ipmobile } { default <i>list-name</i> } [<i>method1</i> [<i>method2</i> ...]]	Creates an authorization method list for a particular authorization type and enable authorization.
Step 2	Router(config)# line [aux console tty vty] <i>line-number</i> [<i>ending-line-number</i>] or Router(config)# interface <i>interface-type interface-number</i>	Enters the line configuration mode for the lines to which you want to apply the authorization method list. Alternately, enters the interface configuration mode for the interfaces to which you want to apply the authorization method list.
Step 3	Router(config-line)# authorization { arap commands <i>level</i> exec reverse-access } { default <i>list-name</i> } or Router(config-line)# ppp authorization { default <i>list-name</i> }	Applies the authorization list to a line or set of lines. Alternately, applies the authorization list to an interface or set of interfaces.

This section includes the following sections:

- [Authorization Types](#)
- [Authorization Methods](#)

Authorization Types

Named authorization method lists are specific to the indicated type of authorization.

To create a method list to enable authorization that applies specific security policies on a per-user basis, use the **auth-proxy** keyword. For detailed information on the authentication proxy feature, refer to the chapter “Configuring Authentication Proxy” in the “Traffic Filtering and Firewalls” part of this book.

To create a method list to enable authorization for all network-related service requests (including SLIP, PPP, PPP NCPs, and ARAP), use the **network** keyword.

To create a method list to enable authorization to determine if a user is allowed to run an EXEC shell, use the **exec** keyword.

To create a method list to enable authorization for specific, individual EXEC commands associated with a specific privilege level, use the **commands** keyword. (This allows you to authorize all commands associated with a specified command level from 0 to 15.)

To create a method list to enable authorization for reverse Telnet functions, use the **reverse-access** keyword.

For information about the types of authorization supported by the Cisco IOS software, refer to the “[AAA Authorization Types](#)” section of this chapter.

Authorization Methods

To have the network access server request authorization information via a TACACS+ security server, use the **aaa authorization** command with the **group tacacs+ method** keyword. For more specific information about configuring authorization using a TACACS+ security server, refer to the chapter “Configuring TACACS+.” For an example of how to enable a TACACS+ server to authorize the use of network services, including PPP and ARA, see the section “[TACACS+ Authorization Examples](#)” at the end of this chapter.

To allow users to have access to the functions they request as long as they have been authenticated, use the **aaa authorization** command with the **if-authenticated method** keyword. If you select this method, all requested functions are automatically granted to authenticated users.

There may be times when you do not want to run authorization from a particular interface or line. To stop authorization activities on designated lines or interfaces, use the **none method** keyword. If you select this method, authorization is disabled for all actions.

To select local authorization, which means that the router or access server consults its local user database to determine the functions a user is permitted to use, use the **aaa authorization** command with the **local method** keyword. The functions associated with local authorization are defined by using the **username** global configuration command. For a list of permitted functions, refer to the chapter “Configuring Authentication.”

To have the network access server request authorization via a RADIUS security server, use the **radius method** keyword. For more specific information about configuring authorization using a RADIUS security server, refer to the chapter “Configuring RADIUS.”

To have the network access server request authorization via a RADIUS security server, use the **aaa authorization** command with the **group radius method** keyword. For more specific information about configuring authorization using a RADIUS security server, refer to the chapter “Configuring RADIUS”. For an example of how to enable a RADIUS server to authorize services, see the “[RADIUS Authorization Example](#)” section at the end of this chapter.



Note

Authorization method lists for SLIP follow whatever is configured for PPP on the relevant interface. If no lists are defined and applied to a particular interface (or no PPP settings are configured), the default setting for authorization applies.

Disabling Authorization for Global Configuration Commands

The **aaa authorization** command with the keyword **commands** attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level. Because there are configuration commands that are identical to some EXEC-level commands, there can be some confusion in the authorization process. Using **no aaa authorization config-commands** stops the network access server from attempting configuration command authorization.

To disable AAA authorization for all global configuration commands, use the following command in global configuration mode:

Command	Purpose
Router(config)# no aaa authorization config-commands	Disables authorization for all global configuration commands.

Configuring Authorization for Reverse Telnet

Telnet is a standard terminal emulation protocol used for remote terminal connection. Normally, you log in to a network access server (typically through a dialup connection) and then use Telnet to access other network devices from that network access server. There are times, however, when it is necessary to establish a reverse Telnet session. In reverse Telnet sessions, the Telnet connection is established in the opposite direction—from inside a network to a network access server on the network periphery to gain access to modems or other devices connected to that network access server. Reverse Telnet is used to provide users with dialout capability by allowing them to Telnet to modem ports attached to a network access server.

It is important to control access to ports accessible through reverse Telnet. Failure to do so could, for example, allow unauthorized users free access to modems where they can trap and divert incoming calls or make outgoing calls to unauthorized destinations.

Authentication during reverse Telnet is performed through the standard AAA login procedure for Telnet. Typically the user has to provide a username and password to establish either a Telnet or reverse Telnet session. Reverse Telnet authorization provides an additional (optional) level of security by requiring authorization in addition to authentication. When enabled, reverse Telnet authorization can use RADIUS or TACACS+ to authorize whether or not this user is allowed reverse Telnet access to specific asynchronous ports, after the user successfully authenticates through the standard Telnet login procedure.

Reverse Telnet authorization offers the following benefits:

- An additional level of protection by ensuring that users engaged in reverse Telnet activities are indeed authorized to access a specific asynchronous port using reverse Telnet.
- An alternative method (other than access lists) to manage reverse Telnet authorization.

To configure a network access server to request authorization information from a TACACS+ or RADIUS server before allowing a user to establish a reverse Telnet session, use the following command in global configuration mode:

Command	Purpose
<code>Router(config)# aaa authorization reverse-access method1 [method2 ...]</code>	Configures the network access server to request authorization information before allowing a user to establish a reverse Telnet session.

This feature enables the network access server to request reverse Telnet authorization information from the security server, whether RADIUS or TACACS+. You must configure the specific reverse Telnet privileges for the user on the security server itself.

Authorization Attribute-Value Pairs

RADIUS and TACACS+ authorization both define specific rights for users by processing attributes, which are stored in a database on the security server. For both RADIUS and TACACS+, attributes are defined on the security server, associated with the user, and sent to the network access server where they are applied to the user's connection.

For a list of supported RADIUS attributes, refer to the appendix "RADIUS Attributes". For a list of supported TACACS+ AV pairs, refer to the appendix "TACACS+ Attribute-Value Pairs."

Authorization Configuration Examples

The following sections provide authorization configuration examples:

- [Named Method List Configuration Example](#)
- [TACACS+ Authorization Examples](#)
- [RADIUS Authorization Example](#)
- [Reverse Telnet Authorization Examples](#)

Named Method List Configuration Example

The following example shows how to configure a Cisco AS5300 (enabled for AAA and communication with a RADIUS security server) for AAA services to be provided by the RADIUS server. If the RADIUS server fails to respond, then the local database will be queried for authentication and authorization information, and accounting services will be handled by a TACACS+ server.

```
aaa new-model
aaa authentication login admins local
aaa authentication ppp dialins group radius local
aaa authorization network scoobee group radius local
aaa accounting network charley start-stop group radius

username root password ALongPassword

radius-server host alcatraz
radius-server key myRaDiUSpassWoRd

interface group-async 1
 group-range 1 16
 encapsulation ppp
 ppp authentication chap dialins
 ppp authorization scoobee
 ppp accounting charley

line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem dialin
```

The lines in this sample RADIUS AAA configuration are defined as follows:

- The **aaa new-model** command enables AAA network security services.
- The **aaa authentication login admins local** command defines a method list, admins, for login authentication.
- The **aaa authentication ppp dialins group radius local** command defines the authentication method list “dialins,” which specifies that RADIUS authentication then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP.
- The **aaa authorization network scoobee group radius local** command defines the network authorization method list named scoobee, which specifies that RADIUS authorization will be used on serial lines using PPP. If the RADIUS server fails to respond, then local network authorization will be performed.

- The **aaa accounting network charley start-stop group radius** command defines the network accounting method list named charley, which specifies that RADIUS accounting services (in this case, start and stop records for specific events) will be used on serial lines using PPP.
- The **username** command defines the username and password to be used for the PPP Password Authentication Protocol (PAP) caller identification.
- The **radius-server host** command defines the name of the RADIUS server host.
- The **radius-server key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **interface group-async** command selects and defines an asynchronous interface group.
- The **group-range** command defines the member asynchronous interfaces in the interface group.
- The **encapsulation ppp** command sets PPP as the encapsulation method used on the specified interfaces.
- The **ppp authentication chap dialins** command selects Challenge Handshake Authentication Protocol (CHAP) as the method of PPP authentication and applies the “dialins” method list to the specified interfaces.
- The **ppp authorization scoobee** command applies the scoobee network authorization method list to the specified interfaces.
- The **ppp accounting charley** command applies the charley network accounting method list to the specified interfaces.
- The **line** command switches the configuration mode from global configuration to line configuration and identifies the specific lines being configured.
- The **autoselect ppp** command configures the Cisco IOS software to allow a PPP session to start up automatically on these selected lines.
- The **autoselect during-login** command is used to display the username and password prompt without pressing the Return key. After the user logs in, the autoselect function (in this case, PPP) begins.
- The **login authentication admins** command applies the admins method list for login authentication.
- The **modem dialin** command configures modems attached to the selected lines to only accept incoming calls.

TACACS+ Authorization Examples

The following examples show how to use a TACACS+ server to authorize the use of network services, including PPP and ARA. If the TACACS+ server is not available or an error occurs during the authorization process, the fallback method (none) is to grant all authorization requests:

```
aaa authorization network default group tacacs+ none
```

The following example shows how to allow network authorization using TACACS+:

```
aaa authorization network default group tacacs+
```

The following example shows how to provide the same authorization, but it also creates address pools called “mci” and “att”:

```
aaa authorization network default group tacacs+
ip address-pool local
ip local-pool mci 172.16.0.1 172.16.0.255
ip local-pool att 172.17.0.1 172.17.0.255
```

These address pools can then be selected by the TACACS daemon. A sample configuration of the daemon follows:

```
user = mci_customer1 {
    login = cleartext "some password"
    service = ppp protocol = ip {
        addr-pool=mci
    }
}

user = att_customer1 {
    login = cleartext "some other password"
    service = ppp protocol = ip {
        addr-pool=att
    }
}
```

RADIUS Authorization Example

The following example shows how to configure the router to authorize using RADIUS:

```
aaa new-model
aaa authorization exec default group radius if-authenticated
aaa authorization network default group radius
radius-server host ip
radius-server key
```

The lines in this sample RADIUS authorization configuration are defined as follows:

- The **aaa authorization exec default group radius if-authenticated** command configures the network access server to contact the RADIUS server to determine if users are permitted to start an EXEC shell when they log in. If an error occurs when the network access server contacts the RADIUS server, the fallback method is to permit the CLI to start, provided the user has been properly authenticated.

The RADIUS information returned may be used to specify an autocommand or a connection access list be applied to this connection.

- The **aaa authorization network default group radius** command configures network authorization via RADIUS. This can be used to govern address assignment, the application of access lists, and various other per-user quantities.



Note

Because no fallback method is specified in this example, authorization will fail if, for any reason, there is no response from the RADIUS server.

Reverse Telnet Authorization Examples

The following examples show how to cause the network access server to request authorization information from a TACACS+ security server before allowing a user to establish a reverse Telnet session:

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization reverse-access default group tacacs+
!
tacacs-server host 172.31.255.0
tacacs-server timeout 90
tacacs-server key goaway
```

The lines in this sample TACACS+ reverse Telnet authorization configuration are defined as follows:

- The **aaa new-model** command enables AAA.
- The **aaa authentication login default group tacacs+** command specifies TACACS+ as the default method for user authentication during login.
- The **aaa authorization reverse-access default group tacacs+** command specifies TACACS+ as the method for user authorization when trying to establish a reverse Telnet session.
- The **tacacs-server host** command identifies the TACACS+ server.
- The **tacacs-server timeout** command sets the interval of time that the network access server waits for the TACACS+ server to reply.
- The **tacacs-server key** command defines the encryption key used for all TACACS+ communications between the network access server and the TACACS+ daemon.

The following example shows how to configure a generic TACACS+ server to grant a user, pat, reverse Telnet access to port tty2 on the network access server named “maple” and to port tty5 on the network access server named “oak”:

```
user = pat
  login = cleartext lab
  service = raccess {
    port#1 = maple/tty2
    port#2 = oak/tty5
```



Note

In this example, “maple” and “oak” are the configured host names of network access servers, not DNS names or alias.

The following example shows how to configure the TACACS+ server (CiscoSecure) to grant a user named pat reverse Telnet access:

```
user = pat
profile_id = 90
profile_cycle = 1
member = Tacacs_Users
service=shell {
  default cmd=permit
}
service=raccess {
  allow "c2511e0" "tty1" ".*"
  refuse ".*" ".*" ".*"
  password = clear "goaway"
```



Note

CiscoSecure only supports reverse Telnet using the command line interface in versions 2.1(x) through version 2.2(1).

An empty “service=raccess { }” clause permits a user to have unconditional access to network access server ports for reverse Telnet. If no “service=raccess” clause exists, the user is denied access to any port for reverse Telnet.

For more information about configuring TACACS+, refer to the chapter “Configuring TACACS+.” For more information about configuring CiscoSecure, refer to the *CiscoSecure Access Control Server User Guide*, version 2.1(2) or greater.

The following example shows how to cause the network access server to request authorization from a RADIUS security server before allowing a user to establish a reverse Telnet session:

```
aaa new-model
```

```
aaa authentication login default group radius
aaa authorization reverse-access default group radius
!
radius-server host 172.31.255.0
radius-server key go away
auth-port 1645 acct-port 1646
```

The lines in this sample RADIUS reverse Telnet authorization configuration are defined as follows:

- The **aaa new-model** command enables AAA.
- The **aaa authentication login default group radius** command specifies RADIUS as the default method for user authentication during login.
- The **aaa authorization reverse-access default group radius** command specifies RADIUS as the method for user authorization when trying to establish a reverse Telnet session.
- The **radius-server host** command identifies the RADIUS server.
- The **radius-server key** command defines the encryption key used for all RADIUS communications between the network access server and the RADIUS daemon.

The following example shows how to send a request to the RADIUS server to grant a user named “pat” reverse Telnet access at port tty2 on the network access server named “maple”:

```
Username = "pat"
Password = "goaway"
User-Service-Type = Shell-User
cisco-avpair = "raccess:port#1=maple/tty2"
```

The syntax "raccess:port=any/any" permits a user to have unconditional access to network access server ports for reverse Telnet. If no "raccess:port={nasname}/{tty number}" clause exists in the user profile, the user is denied access to reverse Telnet on all ports.

For more information about configuring RADIUS, refer to the chapter “Configuring RADIUS.”

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Configuring Accounting

The AAA accounting feature allows the services that users are accessing and the amount of network resources that users are consuming to be tracked. When AAA accounting is enabled, the network access server reports user activity to the TACACS+ or RADIUS security server (depending on which security method is implemented) in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, and auditing.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Configuring Accounting” section on page 28](#).

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Configuring Accounting, page 2](#)
- [Restrictions for Configuring Accounting, page 2](#)
- [Information About Configuring Accounting, page 2](#)
- [How to Configure AAA Accounting, page 16](#)
- [Accounting Attribute-Value Pairs, page 23](#)
- [Configuration Examples for AAA Accounting, page 23](#)
- [Feature Information for Configuring Accounting, page 28](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008 Cisco Systems, Inc. All rights reserved.

Prerequisites for Configuring Accounting

The following tasks must be performed before configuring accounting using named method lists:

- Enable AAA on the network access server. For more information about enabling AAA on the Cisco router or access server, see “AAA Overview” in the *Cisco IOS Security Configuration Guide*.
- Define the characteristics of the RADIUS or TACACS+ security server if RADIUS or TACACS+ authorization is issued. For more information about configuring the Cisco network access server to communicate with the RADIUS security server, see “Configuring RADIUS” in the *Cisco IOS Security Configuration Guide*. For more information about configuring the Cisco network access server to communicate with the TACACS+ security server, see “Configuring TACACS+” in the *Cisco IOS Security Configuration Guide*.

Restrictions for Configuring Accounting

The AAA Accounting feature has the following restrictions:

- Accounting information can be sent simultaneously to a maximum of four AAA servers.
- SSG Restriction—For SSG systems, the **aaa accounting network broadcast** command broadcasts only **start-stop** accounting records. If interim accounting records are configured using the **ssg accounting interval** command, the interim accounting records are sent only to the configured default RADIUS server.

Information About Configuring Accounting

The following sections discuss how Accounting feature:

- [Named Method Lists for Accounting, page 2](#)
- [AAA Accounting Types, page 5](#)
- [AAA Accounting Enhancements, page 14](#)

Named Method Lists for Accounting

Like authentication and authorization method lists, method lists for accounting define the way accounting is performed and the sequence in which these methods are performed.

Named accounting method lists allow particular security protocol to be designated and used on specific lines or interfaces for accounting services. The only exception is the default method list (which, by coincidence, is named “default”). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

A method list is simply a named list describing the accounting methods to be queried (such as RADIUS or TACACS+), in sequence. Method lists allow one or more security protocols to be designated and used for accounting, thus ensuring a backup system for accounting in case the initial method fails. Cisco IOS software uses the first method listed to support accounting; if that method fails to respond, the Cisco IOS software selects the next accounting method listed in the method list. This process continues until there is successful communication with a listed accounting method, or all methods defined are exhausted.

**Note**

The Cisco IOS software attempts accounting with the next listed accounting method only when there is no response from the previous method. If accounting fails at any point in this cycle—meaning that the security server responds by denying the user access—the accounting process stops and no other accounting methods are attempted.

Accounting method lists are specific to the type of accounting being requested. AAA supports six different types of accounting:

- **Network**—Provides information for all PPP, SLIP, or ARAP sessions, including packet and byte counts.
- **EXEC**—Provides information about user EXEC terminal sessions of the network access server.
- **Commands**—Provides information about the EXEC mode commands that a user issues. Command accounting generates accounting records for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- **Connection**—Provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler/disassembler (PAD), and rlogin.
- **System**—Provides information about system-level events.
- **Resource**—Provides “start” and “stop” records for calls that have passed user authentication, and provides “stop” records for calls that fail to authenticate.

**Note**

System accounting does not use named accounting lists; only the default list for system accounting can be defined.

Once again, when a named method list is created, a particular list of accounting methods for the indicated accounting type are defined.

Accounting method lists must be applied to specific lines or interfaces before any of the defined methods are performed. The only exception is the default method list (which is named “default”). If the **aaa accounting** command for a particular accounting type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no accounting takes place.

This section includes the following subsections:

- [Method Lists and Server Groups, page 4](#)
- [AAA Accounting Methods, page 5](#)

Method Lists and Server Groups

A server group is a way to group existing RADIUS or TACACS+ server hosts for use in method lists. [Figure 1](#) shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers, and T1 and T2 are TACACS+ servers. R1 and R2 comprise the group of RADIUS servers. T1 and T2 comprise the group of TACACS+ servers.

Figure 1 *Typical AAA Network Configuration*



In Cisco IOS software, RADIUS and TACACS+ server configurations are global. A subset of the configured server hosts can be specified using server groups. These server groups can be used for a particular service. For example, server groups allow R1 and R2 to be defined as separate server groups (SG1 and SG2), and T1 and T2 as separate server groups (SG3 and SG4). This means either R1 and T1 (SG1 and SG3) can be specified in the method list or R2 and T2 (SG2 and SG4) in the method list, which provides more flexibility in the way that RADIUS and TACACS+ resources are assigned.

Server groups also can include multiple host entries for the same server, as long as each entry has a unique identifier. The combination of an IP address and a UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. In other words, this unique identifier enables RADIUS requests to be sent to different UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry configured acts as failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order in which they are configured.)

For more information about configuring server groups and about configuring server groups based on DNIS numbers, see “Configuring RADIUS” or “Configuring TACACS+” in the *Cisco IOS Security Configuration Guide*.

AAA Accounting Methods

Cisco IOS supports the following two methods for accounting:

- **TACACS+**—The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.
- **RADIUS**—The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.

AAA Accounting Types

AAA supports six different accounting types:

- [Network Accounting](#)
- [Connection Accounting](#)
- [EXEC Accounting](#)
- [System Accounting](#)
- [Command Accounting](#)
- [Resource Accounting](#)

Network Accounting

Network accounting provides information for all PPP, SLIP, or ARAP sessions, including packet and byte counts.

The following example shows the information contained in a RADIUS network accounting record for a PPP user who comes in through an EXEC session:

```
Wed Jun 27 04:44:45 2001
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 5
  User-Name = "username1"
  Client-Port-DNIS = "4327528"
  Caller-ID = "562"
  Acct-Status-Type = Start
  Acct-Authentic = RADIUS
  Service-Type = Exec-User
  Acct-Session-Id = "0000000D"
  Acct-Delay-Time = 0
  User-Id = "username1"
  NAS-Identifier = "172.16.25.15"
```

```
Wed Jun 27 04:45:00 2001
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 5
  User-Name = "username1"
  Client-Port-DNIS = "4327528"
  Caller-ID = "562"
  Acct-Status-Type = Start
  Acct-Authentic = RADIUS
  Service-Type = Framed
  Acct-Session-Id = "0000000E"
  Framed-IP-Address = "10.1.1.2"
```

```

Framed-Protocol = PPP
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:47:46 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 5
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "562"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Framed
Acct-Session-Id = "0000000E"
Framed-IP-Address = "10.1.1.2"
Framed-Protocol = PPP
Acct-Input-Octets = 3075
Acct-Output-Octets = 167
Acct-Input-Packets = 39
Acct-Output-Packets = 9
Acct-Session-Time = 171
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:48:45 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 5
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "408"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = "0000000D"
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

```

The following example shows the information contained in a TACACS+ network accounting record for a PPP user who first started an EXEC session:

```

Wed Jun 27 04:00:35 2001 172.16.25.15 username1 tty4 562/4327528
starttask_id=28 service=shell
Wed Jun 27 04:00:46 2001 172.16.25.15 username1 tty4 562/4327528 starttask_id=30
addr=10.1.1.1 service=ppp
Wed Jun 27 04:00:49 2001 172.16.25.15 username1 tty4 408/4327528 update
task_id=30 addr=10.1.1.1 service=ppp protocol=ip addr=10.1.1.1
Wed Jun 27 04:01:31 2001 172.16.25.15 username1 tty4 562/4327528
stoptask_id=30 addr=10.1.1.1 service=ppp protocol=ip addr=10.1.1.1
bytes_in=2844 bytes_out=1682 paks_in=36 paks_out=24 elapsed_time=51
Wed Jun 27 04:01:32 2001 172.16.25.15 username1 tty4 562/4327528
stoptask_id=28 service=shell elapsed_time=57

```

**Note**

The precise format of accounting packets records may vary depending on the security server daemon.

The following example shows the information contained in a RADIUS network accounting record for a PPP user who comes in through autoselect:

```

Wed Jun 27 04:30:52 2001

```

```

NAS-IP-Address = "172.16.25.15"
NAS-Port = 3
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "562"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Framed
Acct-Session-Id = "0000000B"
Framed-Protocol = PPP
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:36:49 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 3
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "562"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Framed
Acct-Session-Id = "0000000B"
Framed-Protocol = PPP
Framed-IP-Address = "10.1.1.1"
Acct-Input-Octets = 8630
Acct-Output-Octets = 5722
Acct-Input-Packets = 94
Acct-Output-Packets = 64
Acct-Session-Time = 357
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

```

The following example shows the information contained in a TACACS+ network accounting record for a PPP user who comes in through autoselect:

```

Wed Jun 27 04:02:19 2001 172.16.25.15 username1 Async5 562/4327528
starttask_id=35 service=ppp
Wed Jun 27 04:02:25 2001 172.16.25.15 username1 Async5 562/4327528 update
task_id=35 service=ppp protocol=ip addr=10.1.1.2
Wed Jun 27 04:05:03 2001 172.16.25.15 username1 Async5 562/4327528
stoptask_id=35 service=ppp protocol=ip addr=10.1.1.2 bytes_in=3366
bytes_out=2149 paks_in=42 paks_out=28 elapsed_time=164

```

Connection Accounting

Connection accounting provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler/disassembler (PAD), and rlogin.

The following example shows the information contained in a RADIUS connection accounting record for an outbound Telnet connection:

```

Wed Jun 27 04:28:00 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 2
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "5622329477"
Acct-Status-Type = Start

```

```

Acct-Authentic = RADIUS
Service-Type = Login
Acct-Session-Id = "00000008"
Login-Service = Telnet
Login-IP-Host = "10.68.202.158"
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

```

```

Wed Jun 27 04:28:39 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 2
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "5622329477"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Login
Acct-Session-Id = "00000008"
Login-Service = Telnet
Login-IP-Host = "10.68.202.158"
Acct-Input-Octets = 10774
Acct-Output-Octets = 112
Acct-Input-Packets = 91
Acct-Output-Packets = 99
Acct-Session-Time = 39
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

```

The following example shows the information contained in a TACACS+ connection accounting record for an outbound Telnet connection:

```

Wed Jun 27 03:47:43 2001      172.16.25.15      username1      tty3      5622329430/4327528
start      task_id=10      service=connection      protocol=telnet      addr=10.68.202.158
cmd=telnet      username1-sun
Wed Jun 27 03:48:38 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop      task_id=10      service=connection      protocol=telnet      addr=10.68.202.158
cmd=telnet      username1-sun      bytes_in=4467      bytes_out=96      paks_in=61      paks_out=72
elapsed_time=55

```

The following example shows the information contained in a RADIUS connection accounting record for an outbound rlogin connection:

```

Wed Jun 27 04:29:48 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 2
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "5622329477"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Login
Acct-Session-Id = "0000000A"
Login-Service = Rlogin
Login-IP-Host = "10.68.202.158"
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:30:09 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 2
User-Name = "username1"

```

```

Client-Port-DNIS = "4327528"
Caller-ID = "5622329477"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Login
Acct-Session-Id = "0000000A"
Login-Service = Rlogin
Login-IP-Host = "10.68.202.158"
Acct-Input-Octets = 18686
Acct-Output-Octets = 86
Acct-Input-Packets = 90
Acct-Output-Packets = 68
Acct-Session-Time = 22
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

```

The following example shows the information contained in a TACACS+ connection accounting record for an outbound rlogin connection:

```

Wed Jun 27 03:48:46 2001      172.16.25.15      username1      tty3      5622329430/4327528
start      task_id=12      service=connection      protocol=rlogin      addr=10.68.202.158
cmd=rlogin username1-sun /user username1
Wed Jun 27 03:51:37 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop      task_id=12      service=connection      protocol=rlogin      addr=10.68.202.158
cmd=rlogin username1-sun /user username1      bytes_in=659926      bytes_out=138      paks_in=2378
paks_
out=1251      elapsed_time=171

```

The following example shows the information contained in a TACACS+ connection accounting record for an outbound LAT connection:

```

Wed Jun 27 03:53:06 2001      172.16.25.15      username1      tty3      5622329430/4327528
start      task_id=18      service=connection      protocol=lat      addr=VAX      cmd=lat
VAX
Wed Jun 27 03:54:15 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop      task_id=18      service=connection      protocol=lat      addr=VAX      cmd=lat
VAX      bytes_in=0      bytes_out=0      paks_in=0      paks_out=0      elapsed_time=6

```

EXEC Accounting

EXEC accounting provides information about user EXEC terminal sessions (user shells) on the network access server, including username, date, start and stop times, the access server IP address, and (for dial-in users) the telephone number the call originated from.

The following example shows the information contained in a RADIUS EXEC accounting record for a dial-in user:

```

Wed Jun 27 04:26:23 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 1
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "5622329483"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = "00000006"
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

```

```

Wed Jun 27 04:27:25 2001

```

```

NAS-IP-Address = "172.16.25.15"
NAS-Port = 1
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "5622329483"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = "00000006"
Acct-Session-Time = 62
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

```

The following example shows the information contained in a TACACS+ EXEC accounting record for a dial-in user:

```

Wed Jun 27 03:46:21 2001      172.16.25.15      username1      tty3      5622329430/4327528
start      task_id=2      service=shell
Wed Jun 27 04:08:55 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop      task_id=2      service=shell      elapsed_time=1354

```

The following example shows the information contained in a RADIUS EXEC accounting record for a Telnet user:

```

Wed Jun 27 04:48:32 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 26
User-Name = "username1"
Caller-ID = "10.68.202.158"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = "00000010"
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:48:46 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 26
User-Name = "username1"
Caller-ID = "10.68.202.158"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = "00000010"
Acct-Session-Time = 14
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

```

The following example shows the information contained in a TACACS+ EXEC accounting record for a Telnet user:

```

Wed Jun 27 04:06:53 2001      172.16.25.15      username1      tty26      10.68.202.158
starttask_id=41      service=shell
Wed Jun 27 04:07:02 2001      172.16.25.15      username1      tty26      10.68.202.158
stoptask_id=41      service=shell      elapsed_time=9

```


System Accounting

System accounting provides information about all system-level events (for example, when the system reboots or when accounting is turned on or off).

The following accounting record shows a typical TACACS+ system accounting record server indicating that AAA accounting has been turned off:

```
Wed Jun 27 03:55:32 2001      172.16.25.15   unknown unknown unknown start   task_id=25
service=system event=sys_acct reason=reconfigure
```



Note

The precise format of accounting packets records may vary depending on the TACACS+ daemon.

The following accounting record shows a TACACS+ system accounting record indicating that AAA accounting has been turned on:

```
Wed Jun 27 03:55:22 2001      172.16.25.15   unknown unknown unknown stop    task_id=23
service=system event=sys_acct reason=reconfigure
```

Additional tasks for measuring system resources are covered in the Cisco IOS software configuration guides. For example, IP accounting tasks are described in the “Configuring IP Services” feature module in the *Cisco IOS IP Configuration Guide*.

Command Accounting

Command accounting provides information about the EXEC shell commands for a specified privilege level that are being executed on a network access server. Each command accounting record includes a list of the commands executed for that privilege level, as well as the date and time each command was executed, and the user who executed it.

The following example shows the information contained in a TACACS+ command accounting record for privilege level 1:

```
Wed Jun 27 03:46:47 2001      172.16.25.15   username1 tty3   5622329430/4327528
stop task_id=3 service=shell priv-lvl=1 cmd=show version <cr>
Wed Jun 27 03:46:58 2001      172.16.25.15   username1 tty3   5622329430/4327528
stop task_id=4 service=shell priv-lvl=1 cmd=show interfaces Ethernet 0
<cr>
Wed Jun 27 03:47:03 2001      172.16.25.15   username1 tty3   5622329430/4327528
stop task_id=5 service=shell priv-lvl=1 cmd=show ip route <cr>
```

The following example shows the information contained in a TACACS+ command accounting record for privilege level 15:

```
Wed Jun 27 03:47:17 2001      172.16.25.15   username1 tty3   5622329430/4327528
stop task_id=6 service=shell priv-lvl=15 cmd=configure terminal <cr>
Wed Jun 27 03:47:21 2001      172.16.25.15   username1 tty3   5622329430/4327528
stop task_id=7 service=shell priv-lvl=15 cmd=interface Serial 0 <cr>
Wed Jun 27 03:47:29 2001      172.16.25.15   username1 tty3   5622329430/4327528
stop task_id=8 service=shell priv-lvl=15 cmd=ip address 10.1.1.1
255.255.255.0 <cr>
```



Note

The Cisco Systems implementation of RADIUS does not support command accounting.

Resource Accounting

The Cisco implementation of AAA accounting provides “start” and “stop” record support for calls that have passed user authentication. The additional feature of generating “stop” records for calls that fail to authenticate as part of user authentication is also supported. Such records are necessary for users employing accounting records to manage and monitor their networks.

This section includes the following subsections:

- [AAA Resource Failure Stop Accounting, page 12](#)
- [AAA Resource Accounting for Start-Stop Records, page 14](#)

AAA Resource Failure Stop Accounting

Before AAA resource failure stop accounting, there was no method of providing accounting records for calls that failed to reach the user authentication stage of a call setup sequence. Such records are necessary for users employing accounting records to manage and monitor their networks and their wholesale customers.

This functionality generates a “stop” accounting record for any calls that do not reach user authentication; “stop” records are generated from the moment of call setup. All calls that pass user authentication behave as they did before; that is, no additional accounting records are seen.

**Note**

For Cisco IOS Release 12.2, this function is supported only on the Cisco AS5300 and Cisco AS5800.

[Figure 2](#) illustrates a call setup sequence with normal call flow (no disconnect) and without AAA resource failure stop accounting enabled.

Figure 2 Modem Dial-In Call Setup Sequence With Normal Flow and Without Resource Failure Stop Accounting Enabled



[Figure 3](#) illustrates a call setup sequence with normal call flow (no disconnect) and with AAA resource failure stop accounting enabled.

Figure 3 *Modem Dial-In Call Setup Sequence With Normal Flow and With Resource Failure Stop Accounting Enabled*



Figure 4 illustrates a call setup sequence with call disconnect occurring before user authentication and with AAA resource failure stop accounting enabled.

Figure 4 *Modem Dial-In Call Setup Sequence With Call Disconnect Occurring Before User Authentication and With Resource Failure Stop Accounting Enabled*



Figure 11 illustrates a call setup sequence with call disconnect occurring before user authentication and without AAA resource failure stop accounting enabled.

Figure 5 *Modem Dial-In Call Setup Sequence With Call Disconnect Occurring Before User Authentication and Without Resource Failure Stop Accounting Enabled*



AAA Resource Accounting for Start-Stop Records

AAA resource accounting for start-stop records supports the ability to send a “start” record at each call setup, followed by a corresponding “stop” record at the call disconnect. This functionality can be used to manage and monitor wholesale customers from one source of data reporting, such as accounting records.

With this feature, a call setup and call disconnect “start-stop” accounting record tracks the progress of the resource connection to the device. A separate user authentication “start-stop” accounting record tracks the user management progress. These two sets of accounting records are interlinked by using a unique session ID for the call.

**Note**

For Cisco IOS Release 12.2, this function is supported only on the Cisco AS5300 and Cisco AS5800.

Figure 6 illustrates a call setup sequence with AAA resource start-stop accounting enabled.

Figure 6 *Modem Dial-In Call Setup Sequence With Resource Start-Stop Accounting Enabled*



AAA Accounting Enhancements

The section includes the following enhancements:

- [AAA Broadcast Accounting, page 14](#)
- [AAA Session MIB, page 15](#)

AAA Broadcast Accounting

AAA broadcast accounting allows accounting information to be sent to multiple AAA servers at the same time; that is, accounting information can be broadcast to one or more AAA servers simultaneously. This functionality allows service providers to send accounting information to their own private AAA servers and to the AAA servers of their end customers. It also provides redundant billing information for voice applications.

Broadcasting is allowed among groups of RADIUS or TACACS+ servers, and each server group can define its backup servers for failover independently of other groups.

Thus, service providers and their end customers can use different protocols (RADIUS or TACACS+) for the accounting server. Service providers and their end customers can also specify their backup servers independently. As for voice applications, redundant accounting information can be managed independently through a separate group with its own failover sequence.

AAA Session MIB

The AAA session MIB feature allows customers to monitor and terminate their authenticated client connections using Simple Network Management Protocol (SNMP). The data of the client is presented so that it correlates directly to the AAA accounting information reported by either the RADIUS or the TACACS+ server. AAA session MIB provides the following information:

- Statistics for each AAA function (when used in conjunction with the **show radius statistics** command)
- Status of servers providing AAA functions
- Identities of external AAA servers
- Real-time information (such as idle times), providing additional criteria for use by SNMP networks for assessing whether or not to terminate an active call



Note

This command is supported only on Cisco AS5300 and Cisco AS5800 universal access server platforms.

[Table 1](#) shows the SNMP user-end data objects that can be used to monitor and terminate authenticated client connections with the AAA session MIB feature.

Table 1 *SNMP End-User Data Objects*

SessionId	The session identification used by the AAA accounting protocol (same value as reported by RADIUS attribute 44 (Acct-Session-ID)).
UserId	The user login ID or zero-length string if a login is unavailable.
IpAddr	The IP address of the session or 0.0.0.0 if an IP address is not applicable or unavailable.
IdleTime	The elapsed time in seconds that the session has been idle.
Disconnect	The session termination object used to disconnect the given client.
CallId	The entry index corresponding to this accounting session that the Call Tracker record stored.

[Table 2](#) describes the AAA summary information provided by the AAA session MIB feature using SNMP on a per-system basis.

Table 2 *SNMP AAA Session Summary*

ActiveTableEntries	Number of sessions currently active.
ActiveTableHighWaterMark	Maximum number of sessions present at once since last system reinstallation.
TotalSessions	Total number of sessions since last system reinstallation.
DisconnectedSessions	Total number of sessions that have been disconnected using since last system reinstallation.

How to Configure AAA Accounting

This section describes the following configuration tasks involved in configuring AAA Accounting:

- [Configuring AAA Accounting Using Named Method Lists](#)
- [Suppressing Generation of Accounting Records for Null Username Sessions](#)
- [Generating Interim Accounting Records](#)
- [Generating Accounting Records for Failed Login or Session](#)
- [Specifying Accounting NETWORK-Stop Records Before EXEC-Stop Records](#)
- [Configuring AAA Resource Failure Stop Accounting](#)
- [Configuring AAA Resource Accounting for Start-Stop Records](#)
- [Configuring AAA Broadcast Accounting](#)
- [Configuring AAA Resource Failure Stop Accounting](#)
- [Configuring AAA Session MIB](#)
- [Establishing a Session with a Router if the AAA Server is Unreachable](#)
- [Monitoring Accounting](#)
- [Troubleshooting Accounting](#)

Configuring AAA Accounting Using Named Method Lists

To configure AAA accounting using named method lists, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# aaa accounting { system network exec connection commands <i>level</i> } { default <i>list-name</i> } { start-stop stop-only none } [<i>method1</i> [<i>method2</i> ...]]	Creates an accounting method list and enables accounting. The argument <i>list-name</i> is a character string used to name the created list.
Step 2	Router(config)# line [aux console tty vty] <i>line-number</i> [<i>ending-line-number</i>] or Router(config)# interface <i>interface-type</i> <i>interface-number</i>	Enters the line configuration mode for the lines to which the accounting method list is applied. or Enters the interface configuration mode for the interfaces to which the accounting method list is applied.
Step 3	Router(config-line)# accounting { arap commands <i>level</i> connection exec } { default <i>list-name</i> } or Router(config-if)# ppp accounting { default <i>list-name</i> }	Applies the accounting method list to a line or set of lines. or Applies the accounting method list to an interface or set of interfaces.



Note

System accounting does not use named method lists. For system accounting, define only the default method list.

This section includes the following sections:

- [Accounting Types, page 17](#)
- [Accounting Record Types, page 17](#)
- [Accounting Methods, page 17](#)

Accounting Types

Named accounting method lists are specific to the indicated type of accounting.

- **network**—To create a method list to enable authorization for all network-related service requests (including SLIP, PPP, PPP NCPs, and ARA protocols), use the **network** keyword. For example, to create a method list that provides accounting information for ARAP (network) sessions, use the **arap** keyword.
- **exec**—To create a method list that provides accounting records about user EXEC terminal sessions on the network access server, including username, date, start and stop times, use the **exec** keyword.
- **commands**—To create a method list that provides accounting information about specific, individual EXEC commands associated with a specific privilege level, use the **commands** keyword.
- **connection**—To create a method list that provides accounting information about all outbound connections made from the network access server, use the **connection** keyword.
- **resource**—Creates a method list to provide accounting records for calls that have passed user authentication or calls that failed to be authenticated.



Note

System accounting does not support named method lists.

Accounting Record Types

For minimal accounting, use the **stop-only** keyword, which instructs the specified method (RADIUS or TACACS+) to send a stop record accounting notice at the end of the requested user process. For more accounting information, use the **start-stop** keyword to send a start accounting notice at the beginning of the requested event and a stop accounting notice at the end of the event. To stop all accounting activities on this line or interface, use the **none** keyword.

Accounting Methods

[Table 3](#) lists the supported accounting methods.

Table 3 *AAA Accounting Methods*

Keyword	Description
group radius	Uses the list of all RADIUS servers for accounting.
group tacacs+	Uses the list of all TACACS+ servers for accounting.
group group-name	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group <i>group-name</i> .

The method argument refers to the actual method the authentication algorithm tries. Additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all other methods return an error, specify additional methods in the command. For example, to create a method list named `acct_tac1` that specifies RADIUS as the backup method of authentication in the event that TACACS+ authentication returns an error, enter the following command:

```
aaa accounting network acct_tac1 stop-only group tacacs+ group radius
```

To create a default list that is used when a named list is *not* specified in the **aaa accounting** command, use the **default** keyword followed by the methods that are wanted to be used in default situations. The default method list is automatically applied to all interfaces.

For example, to specify RADIUS as the default method for user authentication during login, enter the following command:

```
aaa accounting network default stop-only group radius
```

AAA accounting supports the following methods:

- **group tacacs**—To have the network access server send accounting information to a TACACS+ security server, use the **group tacacs+ method** keyword. For more specific information about configuring TACACS+ for accounting services, see “Configuring TACACS+” in the *Cisco IOS Security Configuration Guide*.
- **group radius**—To have the network access server send accounting information to a RADIUS security server, use the **group radius method** keyword. For more specific information about configuring RADIUS for accounting services, see “Configuring RADIUS” in the *Cisco IOS Security Configuration Guide*.



Note

Accounting method lists for SLIP follow whatever is configured for PPP on the relevant interface. If no lists are defined and applied to a particular interface (or no PPP settings are configured), the default setting for accounting applies.

- **group group-name**—To specify a subset of RADIUS or TACACS+ servers to use as the accounting method, use the **aaa accounting** command with the **group group-name method**. To specify and define the group name and the members of the group, use the **aaa group server** command. For example, use the **aaa group server** command to first define the members of **group loginrad**:

```
aaa group server radius loginrad
server 172.16.2.3
server 172.16.2.17
server 172.16.2.32
```

This command specifies RADIUS servers 172.16.2.3, 172.16.2.17, and 172.16.2.32 as members of the group *loginrad*.

To specify **group loginrad** as the method of network accounting when no other method list has been defined, enter the following command:

```
aaa accounting network default start-stop group loginrad
```

Before a group name can be used as the accounting method, communication with the RADIUS or TACACS+ security server must be enabled. For more information about establishing communication with a RADIUS server, see “Configuring RADIUS” in the *Cisco IOS Security Configuration Guide*. For more information about establishing communication with a TACACS+ server, see “Configuring TACACS+” in the *Cisco IOS Security Configuration Guide*.

Suppressing Generation of Accounting Records for Null Username Sessions

When AAA accounting is activated, the Cisco IOS software issues accounting records for all users on the system, including users whose username string, because of protocol translation, is NULL. An example of this is users who come in on lines where the **aaa authentication login method-list none** command is applied. To prevent accounting records from being generated for sessions that do not have usernames associated with them, use the following command in global configuration mode:

Command	Purpose
Router(config)# aaa accounting suppress null-username	Prevents accounting records from being generated for users whose username string is NULL.

Generating Interim Accounting Records

To enable periodic interim accounting records to be sent to the accounting server, use the following command in global configuration mode:

Command	Purpose
Router(config)# aaa accounting update {[newinfo] [periodic] number}	Enables periodic interim accounting records to be sent to the accounting server.

When the **aaa accounting update** command is activated, the Cisco IOS software issues interim accounting records for all users on the system. If the keyword **newinfo** is used, interim accounting records are sent to the accounting server every time there is new accounting information to report. An example of this would be when IPCP completes IP address negotiation with the remote peer. The interim accounting record includes the negotiated IP address used by the remote peer.

When used with the keyword **periodic**, interim accounting records are sent periodically as defined by the argument number. The interim accounting record contains all of the accounting information recorded for that user up to the time the interim accounting record is sent.



Caution

Using the **aaa accounting update periodic** command can cause heavy congestion when many users are logged in to the network.

Generating Accounting Records for Failed Login or Session

When AAA accounting is activated, the Cisco IOS software does not generate accounting records for system users who fail login authentication, or who succeed in login authentication but fail PPP negotiation for some reason.

To specify that accounting stop records be generated for users who fail to authenticate at login or during session negotiation, use the following command in global configuration mode:

Command	Purpose
Router(config)# aaa accounting send stop-record authentication failure	Generates “stop” records for users who fail to authenticate at login or during session negotiation using PPP.

Specifying Accounting NETWORK-Stop Records Before EXEC-Stop Records

For PPP users who start EXEC terminal sessions, it can be specified that NETWORK records be generated before EXEC-stop records. In some cases, such as billing customers for specific services, it can be desirable to keep network start and stop records together, essentially “nesting” them within the framework of the EXEC start and stop messages. For example, a user dialing in using PPP can create the following records: EXEC-start, NETWORK-start, EXEC-stop, NETWORK-stop. By nesting the accounting records, NETWORK-stop records follow NETWORK-start messages: EXEC-start, NETWORK-start, NETWORK-stop, EXEC-stop.

To nest accounting records for user sessions, use the following command in global configuration mode:

Command	Purpose
Router(config)# aaa accounting nested	Nests network accounting records.

Configuring AAA Resource Failure Stop Accounting

To enable resource failure stop accounting, use the following command in global configuration:

Command	Purpose
Router(config)# aaa accounting resource <i>method-list stop-failure group server-group</i>	<p>Generates a “stop” record for any calls that do not reach user authentication.</p> <p>Note Before configuring this feature, the tasks described in the section “Prerequisites for Configuring Accounting” section on page 2” must be performed, and SNMP must be enabled on the network access server. For more information about enabling SNMP on a Cisco router or access server, see “Configuring SNMP Support” of the <i>Cisco IOS Configuration Fundamentals Configuration Guide</i>.</p>

Configuring AAA Resource Accounting for Start-Stop Records

To enable full resource accounting for start-stop records, use the following command in global configuration mode:

Command	Purpose
Router(config)# aaa accounting resource <i>method-list start-stop group server-group</i>	Supports the ability to send a “start” record at each call setup, followed with a corresponding “stop” record at the call disconnect. Note Before configuring this feature, the tasks described in the section ““ Prerequisites for Configuring Accounting ” section on page 2” must be performed, and SNMP must be enabled on the network access server. For more information about enabling SNMP on a Cisco router or access server, see “Configuring SNMP Support” of the <i>Cisco IOS Configuration Fundamentals Configuration Guide</i> .

Configuring AAA Broadcast Accounting

To configure AAA broadcast accounting, use the **aaa accounting** command in global configuration mode. This command has been modified to allow the **broadcast** keyword.

Command	Purpose
Router(config)# aaa accounting { system network exec connection commands level } { default <i>list-name</i> } { start-stop stop-only none } [broadcast] <i>method1</i> [<i>method2...</i>]	Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.

Configuring Per-DNIS AAA Broadcast Accounting

To configure AAA broadcast accounting per Dialed Number Identification Service (DNIS), use the **aaa dnis map accounting network** command in global configuration mode. This command has been modified to allow the **broadcast** keyword and multiple server groups.

Command	Purpose
Router(config)# aaa dnis map <i>dnis-number</i> accounting network [start-stop stop-only none] [broadcast] <i>method1</i> [<i>method2...</i>]	Allows per-DNIS accounting configuration. This command has precedence over the global aaa accounting command. Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.

Configuring AAA Session MIB

The following tasks must be performed before configuring the AAA session MIB feature:

- Configure SNMP. For information on SNMP, see “Configuring SNMP Support” in the *Cisco IOS Configuration Fundamentals Configuration Guide*.
- Configure AAA.
- Define the RADIUS or TACACS+ server characteristics.



Note

Overusing SNMP can affect the overall system performance; therefore, normal network management performance must be considered when this feature is used.

To configure AAA session MIB, use the following command in global configuration mode

	Command	Purpose
Step 1	Router(config)# aaa session-mib disconnect	Monitors and terminates authenticated client connections using SNMP. To terminate the call, the disconnect keyword must be used.

Establishing a Session with a Router if the AAA Server is Unreachable

To establish a console or telnet session with a router if the AAA server is unreachable, use the following command in Global Configuration mode:

Command	Purpose
Router(config)# no aaa accounting system guarantee-first	The aaa accounting system guarantee-first command guarantees system accounting as the first record, which is the default condition. In some situations, users may be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than three minutes. To resolve this problem, the no aaa accounting system guarantee-first command can be used.



Note

Entering the **no aaa accounting system guarantee-first** command is not the only condition by which the console or telnet session can be started. For example, if the Privileged EXEC session is being authenticated by TACACS and the TACACS server is not reachable, then the session cannot start.

Monitoring Accounting

No specific **show** command exists for either RADIUS or TACACS+ accounting. To obtain accounting records displaying information about users currently logged in, use the following command in privileged EXEC mode:

Command	Purpose
Router# show accounting	Allows display of the active accountable events on the network and helps collect information in the event of a data loss on the accounting server.

Troubleshooting Accounting

To troubleshoot accounting information, use the following command in privileged EXEC mode:

Command	Purpose
Router# debug aaa accounting	Displays information on accountable events as they occur.

Accounting Attribute-Value Pairs

The network access server monitors the accounting functions defined in either TACACS+ attribute-value (AV) pairs or RADIUS attributes, depending on which security method is implemented. For a list of supported RADIUS accounting attributes, see the appendix “RADIUS Attributes.” For a list of supported TACACS+ accounting AV pairs, see the appendix “TACACS+ Attribute-Value Pairs.”

Configuration Examples for AAA Accounting

This section contains the following examples:

- [Configuring Named Method List: Example](#)
- [Configuring AAA Resource Accounting: Example](#)
- [Configuring AAA Broadcast Accounting: Example](#)
- [Configuring Per-DNIS AAA Broadcast Accounting: Example](#)
- [AAA Session MIB: Example](#)

Configuring Named Method List: Example

The following example shows how to configure a Cisco AS5200 (enabled for AAA and communication with a RADIUS security server) in order for AAA services to be provided by the RADIUS server. If the RADIUS server fails to respond, then the local database is queried for authentication and authorization information, and accounting services are handled by a TACACS+ server.

```
aaa new-model
aaa authentication login admins local
aaa authentication ppp dialins group radius local
aaa authorization network blue1 group radius local
aaa accounting network red1 start-stop group radius group tacacs+

username root password ALongPassword

tacacs-server host 172.31.255.0
tacacs-server key goaway

radius-server host 172.16.2.7
radius-server key myRaDiUSpassWoRd

interface group-async 1
 group-range 1 16
 encapsulation ppp
 ppp authentication chap dialins
 ppp authorization blue1
 ppp accounting red1

line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem dialin
```

The lines in this sample RADIUS AAA configuration are defined as follows:

- The **aaa new-model** command enables AAA network security services.
- The **aaa authentication login admins local** command defines a method list, “admins”, for login authentication.
- The **aaa authentication ppp dialins group radius local** command defines the authentication method list “dialins”, which specifies that first RADIUS authentication and then (if the RADIUS server does not respond) local authentication is used on serial lines using PPP.
- The **aaa authorization network blue1 group radius local** command defines the network authorization method list named “blue1”, which specifies that RADIUS authorization is used on serial lines using PPP. If the RADIUS server fails to respond, then local network authorization is performed.
- The **aaa accounting network red1 start-stop group radius group tacacs+** command defines the network accounting method list named red1, which specifies that RADIUS accounting services (in this case, start and stop records for specific events) are used on serial lines using PPP. If the RADIUS server fails to respond, accounting services are handled by a TACACS+ server.
- The **username** command defines the username and password to be used for the PPP Password Authentication Protocol (PAP) caller identification.
- The **tacacs-server host** command defines the name of the TACACS+ server host.
- The **tacacs-server key** command defines the shared secret text string between the network access server and the TACACS+ server host.

- The **radius-server host** command defines the name of the RADIUS server host.
- The **radius-server key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **interface group-async** command selects and defines an asynchronous interface group.
- The **group-range** command defines the member asynchronous interfaces in the interface group.
- The **encapsulation ppp** command sets PPP as the encapsulation method used on the specified interfaces.
- The **ppp authentication chap dialins** command selects Challenge Handshake Authentication Protocol (CHAP) as the method of PPP authentication and applies the “dialins” method list to the specified interfaces.
- The **ppp authorization blue1** command applies the blue1 network authorization method list to the specified interfaces.
- The **ppp accounting red1** command applies the red1 network accounting method list to the specified interfaces.
- The **line** command switches the configuration mode from global configuration to line configuration and identifies the specific lines being configured.
- The **autoselect ppp** command configures the Cisco IOS software to allow a PPP session to start up automatically on these selected lines.
- The **autoselect during-login** command is used to display the username and password prompt without pressing the Return key. After the user logs in, the autoselect function (in this case, PPP) begins.
- The **login authentication admins** command applies the admins method list for login authentication.
- The **modem dialin** command configures modems attached to the selected lines to only accept incoming calls.

The **show accounting** command yields the following output for the preceding configuration:

```
Active Accounted actions on tty1, User username2 Priv 1
Task ID 5, Network Accounting record, 00:00:52 Elapsed
task_id=5 service=ppp protocol=ip address=10.0.0.98
```

Table 4 describes the fields contained in the preceding output.

Table 4 *show accounting Field Descriptions*

Field	Description
Active Accounted actions on	Terminal line or interface name user with which the user logged in.
User	User's ID.
Priv	User's privilege level.
Task ID	Unique identifier for each accounting session.
Accounting Record	Type of accounting session.
Elapsed	Length of time (hh:mm:ss) for this session type.
attribute=value	AV pairs associated with this accounting session.

Configuring AAA Resource Accounting: Example

The following example shows how to configure the resource failure stop accounting and resource accounting for start-stop records functions:

```
!Enable AAA on your network access server.
aaa new-model
!Enable authentication at login and list the AOL string name to use for login
authentication.
aaa authentication login AOL group radius local
!Enable authentication for ppp and list the default method to use for PPP authentication.
aaa authentication ppp default group radius local
!Enable authorization for all exec sessions and list the AOL string name to use for
authorization.
aaa authorization exec AOL group radius if-authenticated
!Enable authorization for all network-related service requests and list the default method
to use for all network-related authorizations.
aaa authorization network default group radius if-authenticated
!Enable accounting for all exec sessions and list the default method to use for all
start-stop accounting services.
aaa accounting exec default start-stop group radius
!Enable accounting for all network-related service requests and list the default method to
use for all start-stop accounting services.
aaa accounting network default start-stop group radius
!Enable failure stop accounting.
aaa accounting resource default stop-failure group radius
!Enable resource accounting for start-stop records.
aaa accounting resource default start-stop group radius
```

Configuring AAA Broadcast Accounting: Example

The following example shows how to turn on broadcast accounting using the global **aaa accounting** command:

```
aaa group server radius isp
server 10.0.0.1
server 10.0.0.2

aaa group server tacacs+ isp_customer
server 172.0.0.1

aaa accounting network default start-stop broadcast group isp group isp_customer

radius-server host 10.0.0.1
radius-server host 10.0.0.2
radius-server key key1
tacacs-server host 172.0.0.1 key key2
```

The **broadcast** keyword causes “start” and “stop” accounting records for network connections to be sent simultaneously to server 10.0.0.1 in the group isp and to server 172.0.0.1 in the group isp_customer. If server 10.0.0.1 is unavailable, failover to server 10.0.0.2 occurs. If server 172.0.0.1 is unavailable, no failover occurs because backup servers are not configured for the group isp_customer.

Configuring Per-DNIS AAA Broadcast Accounting: Example

The following example shows how to turn on per DNIS broadcast accounting using the global **aaa dnis map accounting network** command:

```
aaa group server radius isp
  server 10.0.0.1
  server 10.0.0.2

aaa group server tacacs+ isp_customer
  server 172.0.0.1

aaa dnis map enable
aaa dnis map 7777 accounting network start-stop broadcast group isp group isp_customer

radius-server host 10.0.0.1
radius-server host 10.0.0.2
radius-server key key_1
tacacs-server host 172.0.0.1 key key_2
```

The **broadcast** keyword causes “start” and “stop” accounting records for network connection calls having DNIS number 7777 to be sent simultaneously to server 10.0.0.1 in the group **isp** and to server 172.0.0.1 in the group **isp_customer**. If server 10.0.0.1 is unavailable, failover to server 10.0.0.2 occurs. If server 172.0.0.1 is unavailable, no failover occurs because backup servers are not configured for the group **isp_customer**.

AAA Session MIB: Example

The following example shows how to set up the AAA session MIB feature to disconnect authenticated client connections for PPP users:

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
aaa session-mib disconnect
```

Feature Information for Configuring Accounting

Table 5 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Releases 12.2(1) or 12.0(3)S or a later release appear in the table.

Not all commands may be available in the Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 5 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 5 Feature Information for Configuring Accounting

Feature Name	Releases	Feature Information
—	Cisco IOS	For information about feature support in Cisco IOS software, use Cisco Feature Navigator.
AAA Broadcast Accounting	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
AAA Session MIB	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
Connection Accounting	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0804R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.



Security Server Protocols



RADIUS



Configuring RADIUS

Feature History

Release	Modification
Cisco IOS	For information about feature support in Cisco IOS software, use Cisco Feature Navigator.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

This chapter describes the Remote Authentication Dial-In User Service (RADIUS) security system, defines its operation, and identifies appropriate and inappropriate network environments for using RADIUS technology. The “[RADIUS Configuration Task List](#)” section describes how to configure RADIUS with the authentication, authorization, and accounting (AAA) command set.

For a complete description of the RADIUS commands used in this chapter, refer to the chapter “RADIUS Commands” in the *Cisco IOS Security Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the “Identifying Supported Platforms” section in the “Using Cisco IOS Software” chapter.

In This Chapter

This chapter includes the following sections:

- [About RADIUS](#)
- [RADIUS Operation](#)
- [RADIUS Configuration Task List](#)
- [Monitoring and Maintaining RADIUS](#)
- [RADIUS Attributes](#)
- [RADIUS Configuration Examples](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

About RADIUS

RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

RADIUS is a fully open protocol, distributed in source code format, that can be modified to work with any security system currently available on the market.

Cisco supports RADIUS under its AAA security paradigm. RADIUS can be used with other AAA security protocols, such as TACACS+, Kerberos, and local username lookup. RADIUS is supported on all Cisco platforms, but some RADIUS-supported features run only on specified platforms.

RADIUS has been implemented in a variety of network environments that require high levels of security while maintaining network access for remote users.

Use RADIUS in the following network environments that require access security:

- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors' access servers, dial-in users are authenticated through a RADIUS server that has been customized to work with the Kerberos security system.
- Turnkey network security environments in which applications support the RADIUS protocol, such as in an access environment that uses a "smart card" access control system. In one case, RADIUS has been used with Enigma's security cards to validate users and grant access to network resources.
- Networks already using RADIUS. You can add a Cisco router with RADIUS to the network. This might be the first step when you make a transition to a Terminal Access Controller Access Control System Plus (TACACS+) server.
- Networks in which a user must only access a single service. Using RADIUS, you can control user access to a single host, to a single utility such as Telnet, or to a single protocol such as Point-to-Point Protocol (PPP). For example, when a user logs in, RADIUS identifies this user as having authorization to run PPP using IP address 10.2.3.4 and the defined access list is started.
- Networks that require resource accounting. You can use RADIUS accounting independent of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session. An Internet service provider (ISP) might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.
- Networks that wish to support preauthentication. Using the RADIUS server in your network, you can configure AAA preauthentication and set up the preauthentication profiles. Preauthentication enables service providers to better manage ports using their existing RADIUS solutions, and to efficiently manage the use of shared resources to offer differing service-level agreements.

RADIUS is not suitable in the following network security situations:

- Multiprotocol access environments. RADIUS does not support the following protocols:
 - AppleTalk Remote Access (ARA)
 - NetBIOS Frame Control Protocol (NBFCP)
 - NetWare Asynchronous Services Interface (NASI)
 - X.25 PAD connections

- Router-to-router situations. RADIUS does not provide two-way authentication. RADIUS can be used to authenticate from one router to a non-Cisco router if the non-Cisco router requires RADIUS authentication.
- Networks using a variety of services. RADIUS generally binds a user to one service model.

RADIUS Operation

When a user attempts to log in and authenticate to an access server using RADIUS, the following steps occur:

1. The user is prompted for and enters a username and password.
2. The username and encrypted password are sent over the network to the RADIUS server.

3. The user receives one of the following responses from the RADIUS server:
 - a. **ACCEPT**—The user is authenticated.
 - b. **REJECT**—The user is not authenticated and is prompted to reenter the username and password, or access is denied.
 - c. **CHALLENGE**—A challenge is issued by the RADIUS server. The challenge collects additional data from the user.
 - d. **CHANGE PASSWORD**—A request is issued by the RADIUS server, asking the user to select a new password.

The **ACCEPT** or **REJECT** response is bundled with additional data that is used for **EXEC** or network authorization. You must first complete RADIUS authentication before using RADIUS authorization. The additional data included with the **ACCEPT** or **REJECT** packets consists of the following:

- Services that the user can access, including Telnet, rlogin, or local-area transport (LAT) connections, and PPP, Serial Line Internet Protocol (SLIP), or **EXEC** services.
- Connection parameters, including the host or client IP address, access list, and user timeouts.

RADIUS Configuration Task List

To configure RADIUS on your Cisco router or access server, you must perform the following tasks:

- Use the **aaa new-model** global configuration command to enable AAA. AAA must be configured if you plan to use RADIUS. For more information about using the **aaa new-model** command, refer to the “AAA Overview” chapter.
- Use the **aaa authentication** global configuration command to define method lists for RADIUS authentication. For more information about using the **aaa authentication** command, refer to the “Configuring Authentication” chapter.
- Use **line** and **interface** commands to enable the defined method lists to be used. For more information, refer to the “Configuring Authentication” chapter.

The following configuration tasks are optional:

- You may use the **aaa group server** command to group selected RADIUS hosts for specific services. For more information about using the **aaa group server** command, refer to the “[Configuring AAA Server Groups](#)” section in this chapter.
- You may use the **aaa dnis map** command to select RADIUS server groups based on DNIS number. To use this command, you must define RADIUS server groups using the **aaa group server** command. For more information about using the **aaa dnis map** command, refer to the section “[Configuring AAA Server Group Selection Based on DNIS](#)” in this chapter.
- You may use the **aaa authorization** global command to authorize specific user functions. For more information about using the **aaa authorization** command, refer to the chapter “Configuring Authorization.”
- You may use the **aaa accounting** command to enable accounting for RADIUS connections. For more information about using the **aaa accounting** command, refer to the chapter “Configuring Accounting.”
- You may use the **dialer aaa** interface configuration command to create remote site profiles that contain outgoing call attributes on the AAA server. For more information about using the **dialer aaa** command, refer to the section “[Configuring Suffix and Password in RADIUS Access Requests](#)” in this chapter.

This section describes how to set up RADIUS for authentication, authorization, and accounting on your network, and includes the following sections:

- [Configuring Router to RADIUS Server Communication](#) (Required)
- [Configuring Router to Use Vendor-Specific RADIUS Attributes](#) (Optional)
- [Configuring Router for Vendor-Proprietary RADIUS Server Communication](#) (Optional)
- [Configuring Router to Query RADIUS Server for Static Routes and IP Addresses](#) (Optional)
- [Configuring Router to Expand Network Access Server Port Information](#) (Optional)
- [Configuring AAA Server Groups](#) (Optional)
- [Configuring AAA Server Groups with Deadtme](#) (Optional)
- [Configuring AAA DNIS Authentication](#)
- [Configuring AAA Server Group Selection Based on DNIS](#) (Optional)
- [Configuring AAA Preauthentication](#)
- [Configuring a Guard Timer](#)
- [Specifying RADIUS Authentication](#)
- [Specifying RADIUS Authorization](#) (Optional)
- [Specifying RADIUS Accounting](#) (Optional)
- [Configuring RADIUS Login-IP-Host](#) (Optional)
- [Configuring RADIUS Prompt](#) (Optional)
- [Configuring Suffix and Password in RADIUS Access Requests](#) (Optional)

For RADIUS configuration examples using the commands in this chapter, refer to the section “[RADIUS Configuration Examples](#)” at the end of this chapter.

Configuring Router to RADIUS Server Communication

The RADIUS host is normally a multiuser system running RADIUS server software from Cisco (CiscoSecure ACS), Livingston, Merit, Microsoft, or another software provider. Configuring router to RADIUS server communication can have several components:

- Host name or IP address
- Authentication destination port
- Accounting destination port
- Timeout period
- Retransmission value
- Key string

RADIUS security servers are identified on the basis of their host name or IP address, host name and specific UDP port numbers, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. In other words, this unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry configured acts as fail-over backup to the first one. Using this

example, if the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The RADIUS host entries will be tried in the order they are configured.)

A RADIUS server and a Cisco router use a shared secret text string to encrypt passwords and exchange responses. To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the router.

The timeout, retransmission, and encryption key values are configurable globally for all RADIUS servers, on a per-server basis, or in some combination of global and per-server settings. To apply these settings globally to all RADIUS servers communicating with the router, use the three unique global commands: **radius-server timeout**, **radius-server retransmit**, and **radius-server key**. To apply these values on a specific RADIUS server, use the **radius-server host** command.

**Note**

You can configure both global and per-server timeout, retransmission, and key value commands simultaneously on the same Cisco network access server. If both global and per-server functions are configured on a router, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands.

To configure per-server RADIUS server communication, use the following command in global configuration mode:

Command	Purpose
<pre>Router(config)# radius-server host {hostname ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string] [alias {hostname ip address}]</pre>	<p>Specifies the IP address or host name of the remote RADIUS server host and assign authentication and accounting destination port numbers. Use the auth-port <i>port-number</i> option to configure a specific UDP port on this RADIUS server to be used solely for authentication. Use the acct-port <i>port-number</i> option to configure a specific UDP port on this RADIUS server to be used solely for accounting. Use the alias keyword to configure up to eight multiple IP addresses for use when referring to RADIUS servers.</p> <p>To configure the network access server to recognize more than one host entry associated with a single IP address, simply repeat this command as many times as necessary, making sure that each UDP port number is different. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.</p> <p>If no timeout is set, the global value is used; otherwise, enter a value in the range 1 to 1000. If no retransmit value is set, the global value is used; otherwise enter a value in the range 1 to 1000. If no key string is specified, the global value is used.</p> <p>Note The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the radius-server host command syntax because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.</p>

To configure global communication settings between the router and a RADIUS server, use the following **radius-server** commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# radius-server key {0 string 7 string string}	Specifies the shared secret text string used between the router and a RADIUS server. Use the 0 line option to configure an unencrypted shared secret. Use the 7 line option to configure an encrypted shared secret.
Step 2	Router(config)# radius-server retransmit retries	Specifies how many times the router transmits each RADIUS request to the server before giving up (the default is 3).
Step 3	Router(config)# radius-server timeout seconds	Specifies for how many seconds a router waits for a reply to a RADIUS request before retransmitting the request.
Step 4	Router(config)# radius-server deadtime minutes	Specifies for how many minutes a RADIUS server that is not responding to authentication requests is passed over by requests for RADIUS authentication.

Configuring Router to Use Vendor-Specific RADIUS Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option has vendor-type 1, which is named "cisco-avpair." The value is a string of the following format:

```
protocol : attribute sep value *
```

"Protocol" is a value of the Cisco "protocol" attribute for a particular type of authorization; protocols that can be used include IP, IPX, VPDN, VOIP, SHELL, RSVP, SIP, AIRNET, OUTBOUND. "Attribute" and "value" are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification, and "sep" is "=" for mandatory attributes and "*" for optional attributes. This allows the full set of features available for TACACS+ authorization to also be used for RADIUS.

For example, the following AV pair causes Cisco's "multiple named ip address pools" feature to be activated during IP authorization (during PPP's IPCP address assignment):

```
cisco-avpair= "ip:addr-pool=first"
```

If you insert an "*", the AV pair "ip:addr-pool=first" becomes optional. Note that any AV pair can be made optional.

```
cisco-avpair= "ip:addr-pool*first"
```

The following example shows how to cause a user logging in from a network access server to have immediate access to EXEC commands:

```
cisco-avpair= "shell:priv-lvl=15"
```

Other vendors have their own unique vendor-IDs, options, and associated VSAs. For more information about vendor-IDs and VSAs, refer to RFC 2138, Remote Authentication Dial-In User Service (RADIUS).

To configure the network access server to recognize and use VSAs, use the following command in global configuration mode:

Command	Purpose
Router(config)# radius-server vsa send [accounting authentication]	Enables the network access server to recognize and use VSAs as defined by RADIUS IETF attribute 26.

For a complete list of RADIUS attributes or more information about vendor-specific attribute 26, refer to the appendix “RADIUS Attributes.”

Configuring Router for Vendor-Proprietary RADIUS Server Communication

Although an Internet Engineering Task Force (IETF) draft standard for RADIUS specifies a method for communicating vendor-specific information between the network access server and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. Cisco IOS software supports a subset of vendor-specific RADIUS attributes.

As mentioned earlier, to configure RADIUS (whether vendor-specific or IETF draft-compliant), you must specify the host running the RADIUS server daemon and the secret text string it shares with the Cisco device. You specify the RADIUS host and secret text string by using the **radius-server** commands. To identify that the RADIUS server is using a vendor-specific implementation of RADIUS, use the **radius-server host non-standard** command. Vendor-specific attributes will not be supported unless you use the **radius-server host non-standard** command.

To specify a vendor-specific RADIUS server host and a shared secret text string, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# radius-server host {hostname ip-address} non-standard	Specifies the IP address or host name of the remote RADIUS server host and identifies that it is using a vendor-specific implementation of RADIUS.
Step 2	Router(config)# radius-server key {0 string 7 string string}	Specifies the shared secret text string used between the router and the vendor-specific RADIUS server. The router and the RADIUS server use this text string to encrypt passwords and exchange responses.

Configuring Router to Query RADIUS Server for Static Routes and IP Addresses

Some vendor-specific implementations of RADIUS let the user define static routes and IP pool definitions on the RADIUS server instead of on each individual network access server in the network. Each network access server then queries the RADIUS server for static route and IP pool information.

To have the Cisco router or access server query the RADIUS server for static routes and IP pool definitions when the device first starts up, use the following command in global configuration mode:

Command	Purpose
Router(config)# radius-server configure-nas	Tells the Cisco router or access server to query the RADIUS server for the static routes and IP pool definitions used throughout its domain.

**Note**

Because the **radius-server configure-nas** command is performed when the Cisco router starts up, it will not take effect until you issue a **copy system:running config nvram:startup-config** command.

Configuring Router to Expand Network Access Server Port Information

There are some situations when PPP or login authentication occurs on an interface different from the interface on which the call itself comes in. For example, in a V.120 ISDN call, login or PPP authentication occurs on a virtual asynchronous interface “**ttt**” but the call itself occurs on one of the channels of the ISDN interface.

The **radius-server attribute nas-port extended** command configures RADIUS to expand the size of the NAS-Port attribute (RADIUS IETF attribute 5) field to 32 bits. The upper 16 bits of the NAS-Port attribute display the type and number of the controlling interface; the lower 16 bits indicate the interface undergoing authentication.

To display expanded interface information in the NAS-Port attribute field, use the following command in global configuration mode:

Command	Purpose
Router(config)# radius-server attribute nas-port format	Expands the size of the NAS-Port attribute from 16 to 32 bits to display extended interface information.

**Note**

This command replaces the **radius-server extended-portnames** command and the **radius-server attribute nas-port extended** command.

On platforms with multiple interfaces (ports) per slot, the Cisco RADIUS implementation will not provide a unique NAS-Port attribute that permits distinguishing between the interfaces. For example, if a dual PRI interface is in slot 1, calls on both Serial1/0:1 and Serial1/1:1 will appear as NAS-Port = 20101.

Once again, this is because of the 16-bit field size limitation associated with RADIUS IETF NAS-Port attribute. In this case, the solution is to replace the NAS-Port attribute with a vendor-specific attribute (RADIUS IETF attribute 26). Cisco's vendor-ID is 9, and the Cisco-NAS-Port attribute is subtype 2. Vendor-specific attributes (VSAs) can be turned on by entering the **radius-server vsa send** command. The port information in this attribute is provided and configured using the **aaa nas port extended** command.

To replace the NAS-Port attribute with RADIUS IETF attribute 26 and to display extended field information, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# radius-server vsa send [accounting authentication]	Enables the network access server to recognize and use vendor-specific attributes as defined by RADIUS IETF attribute 26.
Step 2	Router(config)# aaa nas port extended	Expands the size of the VSA NAS-Port field from 16 to 32 bits to display extended interface information.

The standard NAS-Port attribute (RADIUS IETF attribute 5) will continue to be sent. If you do not want this information to be sent, you can suppress it by using the **no radius-server attribute nas-port** command. When this command is configured, the standard NAS-Port attribute will no longer be sent.

For a complete list of RADIUS attributes, refer to the appendix “RADIUS Attributes.”

For information about configuring RADIUS port identification for PPP, see the *Cisco IOS Wide-Area Networking Configuration Guide*.

Configuring AAA Server Groups

Configuring the router to use AAA server groups provides a way to group existing server hosts. This allows you to select a subset of the configured server hosts and use them for a particular service. A server group is used in conjunction with a global server-host list. The server group lists the IP addresses of the selected server hosts.

Server groups also can include multiple host entries for the same server, as long as each entry has a unique identifier. The combination of an IP address and a UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. In other words, this unique identifier enables RADIUS requests to be sent to different UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry configured acts as failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The RADIUS host entries will be tried in the order in which they are configured.)

To define a server host with a server group name, enter the following commands in global configuration mode. The listed server must exist in global configuration mode:

	Command	Purpose
Step 1	Router(config)# radius-server host {hostname ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string] [alias {hostname ip address}]	Specifies and defines the IP address of the server host before configuring the AAA server-group. Refer to the section “ Configuring Router to RADIUS Server Communication ” of this chapter for more information on the radius-server host command.

	Command	Purpose
Step 2	Router(config-if)# aaa group server { radius tacacs+ } <i>group-name</i>	Defines the AAA server group with a group name. All members of a group must be the same type; that is, RADIUS or TACACS+. This command puts the router in server group subconfiguration mode.
Step 3	Router(config-sg)# server <i>ip-address</i> [auth-port <i>port-number</i>] [acct-port <i>port-number</i>]	<p>Associates a particular RADIUS server with the defined server group. Each security server is identified by its IP address and UDP port number.</p> <p>Repeat this step for each RADIUS server in the AAA server group.</p> <p>Note Each server in the group must be defined previously using the radius-server host command.</p>

Configuring AAA Server Groups with Deadtime

After you have configured a server host with a server name, you can use the **deadtime** command to configure each server per server group. Configuring deadtime within a server group allows you to direct AAA traffic to separate groups of servers that have different operational characteristics.

Configuring deadtime is no longer limited to a global configuration. A separate timer has been attached to each server host in every server group. Therefore, when a server is found to be unresponsive after numerous retransmissions and timeouts, the server is assumed to be dead. The timers attached to each server host in all server groups are triggered. In essence, the timers are checked and subsequent requests to a server (once it is assumed to be dead) are directed to alternate timers, if configured. When the network access server receives a reply from the server, it checks and stops all configured timers (if running) for that server in all server groups.

If the timer has expired, only the server to which the timer is attached is assumed to be alive. This becomes the only server that can be tried for later AAA requests using the server groups to which the timer belongs.



Note

Since one server has different timers and may have different deadtime values configured in the server groups, the same server may in the future have different states (dead and alive) at the same time.



Note

To change the state of a server, you must start and stop all configured timers in all server groups.

The size of the server group will be slightly increased because of the addition of new timers and the deadtime attribute. The overall impact of the structure depends on the number and size of the server groups and how the servers are shared among server groups in a specific configuration.

To configure deadtime within a server group, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# aaa group server radius <i>group1</i>	Defines a RADIUS type server group.
Step 2	Router(config-sg)# deadtime <i>1</i>	Configures and defines deadtime value in minutes. Note Local server group deadtime will override the global configuration. If omitted from the local server group configuration, the value will be inherited from the master list.
Step 3	Router(config-sg)# exit	Exits server group configuration mode.

Configuring AAA DNIS Authentication

DNIS preauthentication enables preauthentication at call setup based on the number dialed. The DNIS number is sent directly to the security server when a call is received. If authenticated by AAA, the call is accepted.

To configure DNIS authentication, perform the following tasks in global configuration mode:

	Command	Purpose
Step 1	Router# config term	Enters global configuration mode.
Step 2	Router(config)# aaa preauth	Enters AAA preauthentication mode.
Step 3	Router(config-preauth)# group { radius tacacs+ <i>server-group</i> }	(Optional) Selects the security server to use for AAA preauthentication requests. The default is RADIUS.
Step 4	Router(config-preauth)# dnis [password <i>string</i>]	Enables preauthentication using DNIS and optionally specifies a password to use in Access-Request packets.

Configuring AAA Server Group Selection Based on DNIS

Cisco IOS software allows you to assign a Dialed Number Identification Service (DNIS) number to a particular AAA server group so that the server group can process authentication, authorization, and accounting requests for users dialing in to the network using that particular DNIS. Any phone line (a regular home phone or a commercial T1/PRI line) can be associated with several phone numbers. The DNIS number identifies the number that was called to reach you.

For example, suppose you want to share the same phone number with several customers, but you want to know which customer is calling before you pick up the phone. You can customize how you answer the phone because DNIS allows you to know which customer is calling when you answer.

Cisco routers with either ISDN or internal modems can receive the DNIS number. This functionality allows users to assign different RADIUS server groups for different customers (that is, different RADIUS servers for different DNIS numbers). Additionally, using server groups you can specify the same server group for AAA services or a separate server group for each AAA service.

Cisco IOS software provides the flexibility to implement authentication and accounting services in several ways:

- Globally—AAA services are defined using global configuration access list commands and applied in general to all interfaces on a specific network access server.
- Per Interface—AAA services are defined using interface configuration commands and applied specifically to the interface being configured on a specific network access server.
- DNIS mapping—You can use DNIS to specify an AAA server to supply AAA services.

Because each of these AAA configuration methods can be configured simultaneously, Cisco has established an order of precedence to determine which server or groups of servers provide AAA services. The order of precedence is as follows:

- Per DNIS—If you configure the network access server to use DNIS to identify/determine which server group provides AAA services, then this method takes precedence over any additional AAA selection method.
- Per interface—If you configure the network access server per interface to use access lists to determine how a server provides AAA services, this method takes precedence over any global configuration AAA access lists.
- Globally—If you configure the network access server by using global AAA access lists to determine how the security server provides AAA services, this method has the least precedence.



Note

Prior to configuring AAA Server Group Selection Based on DNIS, you must configure the list of RADIUS server hosts and configure the AAA server groups. See the sections [“Configuring Router to RADIUS Server Communication”](#) and [“Configuring AAA Server Groups”](#) of this chapter.

To configure the router to select a particular AAA server group based on the DNIS of the server group, configure DNIS mapping. To map a server group with a group name with DNIS number, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# aaa dnis map enable	Enables DNIS mapping.
Step 2	Router(config)# aaa dnis map <i>dnis-number</i> authentication ppp group <i>server-group-name</i>	Maps a DNIS number to a defined AAA server group; the servers in this server group are being used for authentication.
Step 3	Router(config)# aaa dnis map <i>dnis-number</i> authorization network group <i>server-group-name</i>	Maps a DNIS number to a defined AAA server group; the servers in this server group are being used for authorization.
Step 4	Router(config)# aaa dnis map <i>dnis-number</i> accounting network [none start-stop stop-only] group <i>server-group-name</i>	Maps a DNIS number to a defined AAA server group; the servers in this server group are being used for accounting.

Configuring AAA Preauthentication

Configuring AAA preauthentication with ISDN PRI or channel-associated signalling (CAS) allows service providers to better manage ports using their existing RADIUS solutions and efficiently manage the use of shared resources to offer differing service-level agreements. With ISDN PRI or CAS, information about an incoming call is available to the network access server (NAS) before the call is connected. The available call information includes the following:

- The Dialed Number Identification Service (DNIS) number, also referred to as the called number
- The Calling Line Identification (CLID) number, also referred to as the calling number
- The call type, also referred to as the bearer capability

This feature allows a Cisco NAS to decide—on the basis of the DNIS number, the CLID number, or the call type—whether to connect an incoming call. (With ISDN PRI, it enables user authentication and authorization before a call is answered. With CAS, the call must be answered; however, the call can be dropped if preauthentication fails.)

When an incoming call arrives from the public network switch, but before it is connected, AAA preauthentication enables the NAS to send the DNIS number, CLID number, and call type to a RADIUS server for authorization. If the server authorizes the call, then the NAS accepts the call. If the server does not authorize the call, then the NAS sends a disconnect message to the public network switch to reject the call.

In the event that the RADIUS server application becomes unavailable or is slow to respond, a guard timer can be set in the NAS. When the timer expires, the NAS uses a configurable parameter to accept or reject the incoming call that has no authorization.

This feature supports the use of attribute 44 by the RADIUS server application and the use of RADIUS attributes that are configured in the RADIUS preauthentication profiles to specify preauthentication behavior. They may also be used, for instance, to specify whether subsequent authentication should occur and, if so, what authentication method should be used.

The following restrictions apply to AAA preauthentication with ISDN PRI and CAS:

- Attribute 44 is available for CAS calls only when preauthentication or resource pooling is enabled.
- MMP is not available with ISDN PRI.
- AAA preauthentication is available only on the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.



Note

Prior to configuring AAA preauthentication, you must enable the **aaa new-model** command and make sure the supporting preauthentication application is running on a RADIUS server in your network.

To configure AAA preauthentication, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# aaa preauth	Enters AAA preauthentication configuration mode.
Step 2	Router(config-preauth)# group <i>server-group</i>	Specifies the AAA RADIUS server group to use for preauthentication.
Step 3	Router(config-preauth)# clid [if-avail required] [accept-stop] [password <i>string</i>]	Preauthenticates calls on the basis of the CLID number.

	Command	Purpose
Step 4	Router(config-preauth)# ctype [if-avail required] [accept-stop] [password <i>string</i>]	Preauthenticates calls on the basis of the call type.
Step 5	Router(config-preauth)# dnis [if-avail required] [accept-stop] [password <i>string</i>]	Preauthenticates calls on the basis of the DNIS number.
Step 6	Router(config-preauth)# dnis bypass { <i>dnis-group-name</i> }	Specifies a group of DNIS numbers that will be bypassed for preauthentication.

To configure DNIS preauthentication, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# aaa preauth	Enters AAA preauthentication mode.
Step 2	Router(config-preauth)# group { radius tacacs+ <i>server-group</i> }	(Optional) Selects the security server to use for AAA preauthentication requests. The default is RADIUS.
Step 3	Router(config-preauth)# dnis [password <i>string</i>]	Enables preauthentication using DNIS and optionally specifies a password to use in Access-Request packets.

In addition to configuring preauthentication on your Cisco router, you must set up the preauthentication profiles on the RADIUS server. For information on setting up the preauthentication profiles, see the following sections:

- [Setting Up the RADIUS Profile for DNIS or CLID Preauthentication](#)
- [Setting Up the RADIUS Profile for Call Type Preauthentication](#)
- [Setting Up the RADIUS Profile for Preauthentication Enhancements for Callback](#)
- [Setting Up the RADIUS Profile for a Remote Host Name Used for Large-Scale Dial-Out](#)
- [Setting Up the RADIUS Profile for Modem Management](#)
- [Setting Up the RADIUS Profile for Subsequent Authentication](#)
- [Setting Up the RADIUS Profile for Subsequent Authentication Type](#)
- [Setting Up the RADIUS Profile to Include the Username](#)
- [Setting Up the RADIUS Profile for Two-Way Authentication](#)
- [Setting Up the RADIUS Profile to Support Authorization](#)

Setting Up the RADIUS Profile for DNIS or CLID Preauthentication

To set up the RADIUS preauthentication profile, use the DNIS or CLID number as the username, and use the password defined in the **dnis** or **clid** command as the password.

**Note**

The preauthentication profile must have “outbound” as the service type because the password is predefined on the NAS. Setting up the preauthentication profile in this manner prevents users from trying to log in to the NAS with the username of the DNIS number, CLID number, or call type and an obvious password. The “outbound” service type is also included in the access-request packet sent to the RADIUS server.

Setting Up the RADIUS Profile for Call Type Preauthentication

To set up the RADIUS preauthentication profile, use the call type string as the username, and use the password defined in the **ctype** command as the password. The following table shows the call type strings that may be used in the preauthentication profile:

Call Type String	ISDN Bearer Capabilities
digital	Unrestricted digital, restricted digital.
speech	Speech, 3.1 kHz audio, 7 kHz audio. Note This is the only call type available for CAS.
v.110	Anything with V.110 user information layer.
v.120	Anything with V.120 user information layer.

**Note**

The preauthentication profile must have “outbound” as the service type because the password is predefined on the NAS. Setting up the preauthentication profile in this manner prevents users from trying to log in to the NAS with the username of the DNIS number, CLID number, or call type and an obvious password. The “outbound” service type is also included in the access-request packet sent to the RADIUS server and should be a check-in item if the RADIUS server supports check-in items.

Setting Up the RADIUS Profile for Preauthentication Enhancements for Callback

Callback allows remote network users such as telecommuters to dial in to the NAS without being charged. When callback is required, the NAS hangs up the current call and dials the caller back. When the NAS performs the callback, only information for the outgoing connection is applied. The rest of the attributes from the preauthentication access-accept message are discarded.

**Note**

The destination IP address is not required to be returned from the RADIUS server.

The following example shows a RADIUS profile configuration with a callback number of 555-1111 and the service type set to outbound. The cisco-avpair = “preauth:send-name=<string>” uses the string “andy” and the cisco-avpair = “preauth:send-secret=<string>” uses the password “cisco.”

```
5551111 password = "cisco", Service-Type = Outbound
  Service-Type = Callback-Framed
  Framed-Protocol = PPP,
  Dialback-No = "5551212"
  Class = "ISP12"
  cisco-avpair = "preauth:send-name=andy"
```

```
cisco-avpair = "preauth:send-secret=cisco"
```

Setting Up the RADIUS Profile for a Remote Host Name Used for Large-Scale Dial-Out

The following example adds to the previous example by protecting against accidentally calling a valid telephone number but accessing the wrong router by providing the name of the remote, for use in large-scale dial-out:

```
5551111 password = "cisco", Service-Type = Outbound
    Service-Type = Callback-Framed
    Framed-Protocol = PPP,
    Dialback-No = "5551212"
    Class = "ISP12"
    cisco-avpair = "preauth:send-name=andy"
    cisco-avpair = "preauth:send-secret=cisco"
    cisco-avpair = "preauth:remote-name=Router2"
```

Setting Up the RADIUS Profile for Modem Management

When DNIS, CLID, or call type preauthentication is used, the affirmative response from the RADIUS server may include a modem string for modem management in the NAS through vendor-specific attribute (VSA) 26. The modem management VSA has the following syntax:

```
cisco-avpair = "preauth:modem-service=modem min-speed <x> max-speed <y>
modulation <z> error-correction <a> compression <b>"
```

The modem management string within the VSA may contain the following:

Command	Argument
min-speed	<300 to 56000>, any
max-speed	<300 to 56000>, any
modulation	K56Flex, v22bis, v32bis, v34, v90, any
error-correction	lapm, mnp4
compression	mnp5, v42bis

When the modem management string is received from the RADIUS server in the form of a VSA, the information is passed to the Cisco IOS software and applied on a per-call basis. Modem ISDN channel aggregation (MICA) modems provide a control channel through which messages can be sent during the call setup time. Hence, this modem management feature is supported only with MICA modems and newer technologies. This feature is not supported with Microcom modems.

For more information on modem management, refer to the “Modem Configuration and Management” chapter of the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2.

Setting Up the RADIUS Profile for Subsequent Authentication

If preauthentication passes, you may use vendor-proprietary RADIUS attribute 201 (Require-Auth) in the preauthentication profile to determine whether subsequent authentication is to be performed. If attribute 201, returned in the access-accept message, has a value of 0, then subsequent authentication will not be performed. If attribute 201 has a value of 1, then subsequent authentication will be performed as usual.

Attribute 201 has the following syntax:

```
cisco-avpair = "preauth:auth-required=<n>"
```

where *<n>* has the same value range as attribute 201 (that is, 0 or 1).

If attribute 201 is missing in the preauthentication profile, then a value of 1 is assumed, and subsequent authentication is performed.

**Note**

To perform subsequent authentication, you must set up a regular user profile in addition to a preauthentication profile.

Setting Up the RADIUS Profile for Subsequent Authentication Type

If you have specified subsequent authentication in the preauthentication profile, you must also specify the authentication types to be used for subsequent authentication. To specify the authentication types allowed in subsequent authentication, use the following VSA:

```
cisco-avpair = "preauth:auth-type=<string>"
```

where *<string>* can be one of the following:

String	Description
chap	Requires username and password of CHAP for PPP authentication.
ms-chap	Requires username and password of MS-CHAP for PPP authentication.
pap	Requires username and password of PAP for PPP authentication.

To specify that multiple authentication types are allowed, you can configure more than one instance of this VSA in the preauthentication profile. The sequence of the authentication type VSAs in the preauthentication profile is significant because it specifies the order of authentication types to be used in the PPP negotiation.

This VSA is a per-user attribute and replaces the authentication type list in the **ppp authentication** interface command.

**Note**

You should use this VSA only if subsequent authentication is required because it specifies the authentication type for subsequent authentication.

Setting Up the RADIUS Profile to Include the Username

If only preauthentication is used to authenticate a call, the NAS could be missing a username when it brings up the call. RADIUS may provide a username for the NAS to use through RADIUS attribute 1 (User-Name) or through a VSA returned in the access-accept packet. The VSA for specifying the username has the following syntax:

```
cisco-avpair = "preauth:username=<string>"
```

If no username is specified, the DNIS number, CLID number, or call type is used, depending on the last preauthentication command that has been configured (for example, if **clid** was the last preauthentication command configured, the CLID number will be used as the username).

If subsequent authentication is used to authenticate a call, there might be two usernames: one provided by RADIUS and one provided by the user. In this case, the username provided by the user overrides the one contained in the RADIUS preauthentication profile; the username provided by the user is used for both authentication and accounting.

Setting Up the RADIUS Profile for Two-Way Authentication

In the case of two-way authentication, the calling networking device will need to authenticate the NAS. The Password Authentication Protocol (PAP) username and password or Challenge Handshake Authentication Protocol (CHAP) username and password need not be configured locally on the NAS. Instead, username and password can be included in the access-accept messages for preauthentication.



Note

The **ppp authentication** command must be configured with the **radius** method.

To apply for PAP, do not configure the **ppp pap sent-name password** command on the interface. The vendor-specific attributes (VSAs) “preauth:send-name” and “preauth:send-secret” will be used as the PAP username and PAP password for outbound authentication.

For CHAP, “preauth:send-name” will be used not only for outbound authentication, but also for inbound authentication. For a CHAP inbound case, the NAS will use the name defined in “preauth:send-name” in the challenge packet to the caller networking device. For a CHAP outbound case, both “preauth:send-name” and “preauth:send-secret” will be used in the response packet.

The following example shows a configuration that specifies two-way authentication:

```
5551111 password = "cisco", Service-Type = Outbound
Service-Type = Framed-User
cisco-avpair = "preauth:auth-required=1"
cisco-avpair = "preauth:auth-type=pap"
cisco-avpair = "preauth:send-name=andy"
cisco-avpair = "preauth:send-secret=cisco"
class = "<some class>"
```



Note

Two-way authentication does not work when resource pooling is enabled.

Setting Up the RADIUS Profile to Support Authorization

If only preauthentication is configured, then subsequent authentication will be bypassed. Note that because the username and password are not available, authorization will also be bypassed. However, you may include authorization attributes in the preauthentication profile to apply per-user attributes and avoid having to return subsequently to RADIUS for authorization. To initiate the authorization process, you must also configure the **aaa authorization network** command on the NAS.

You may configure authorization attributes in the preauthentication profile with one exception: the service-type attribute (attribute 6). The service-type attribute must be converted to a VSA in the preauthentication profile. This VSA has the following syntax:

```
cisco-avpair = "preauth:service-type=<n>"
```

where <n> is one of the standard RFC 2138 values for attribute 6. For a list of possible Service-Type values, refer to the appendix RADIUS Attributes.

**Note**

If subsequent authentication is required, the authorization attributes in the preauthentication profile will not be applied.

Configuring a Guard Timer

Because response times for preauthentication and authentication requests can vary, the guard timer allows you to control the handling of calls. The guard timer starts when the DNIS is sent to the RADIUS server. If the NAS does not receive a response from AAA before the guard timer expires, it accepts or rejects the calls on the basis of the configuration of the timer.

To set a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to an authentication or preauthentication request, use one of the following commands in interface configuration mode:

Command	Purpose
Router(config-if)# isdn guard-timer <i>milliseconds</i> [on-expiry { accept reject }]	Sets an ISDN guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request.
Router(control-config)# call guard-timer <i>milliseconds</i> [on-expiry { accept reject }]	Sets a CAS guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request.

Specifying RADIUS Authentication

After you have identified the RADIUS server and defined the RADIUS authentication key, you must define method lists for RADIUS authentication. Because RADIUS authentication is facilitated through AAA, you must enter the **aaa authentication** command, specifying RADIUS as the authentication method. For more information, refer to the chapter “Configuring Authentication.”

Specifying RADIUS Authorization

AAA authorization lets you set parameters that restrict a user’s access to the network. Authorization using RADIUS provides one method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet. Because RADIUS authorization is facilitated through AAA, you must issue the **aaa authorization** command, specifying RADIUS as the authorization method. For more information, refer to the chapter “Configuring Authorization.”

Specifying RADIUS Accounting

The AAA accounting feature enables you to track the services users are accessing as well as the amount of network resources they are consuming. Because RADIUS accounting is facilitated through AAA, you must issue the **aaa accounting** command, specifying RADIUS as the accounting method. For more information, refer to the chapter “Configuring Accounting.”

Configuring RADIUS Login-IP-Host

To enable the network access server to attempt more than one login host when trying to connect a dial in user, you can enter as many as three Login-IP-Host entries in the user's profile on the RADIUS server. The following example shows that three Login-IP-Host instances have been configured for the user *joeuser*, and that TCP-Clear will be used for the connection:

```
joeuser      Password = xyz
             Service-Type = Login,
             Login-Service = TCP-Clear,
             Login-IP-Host = 10.0.0.0,
             Login-IP-Host = 10.2.2.2,
             Login-IP-Host = 10.255.255.255,
             Login-TCP-Port = 23
```

The order in which the hosts are entered is the order in which they are attempted. Use the **ip tcp synwait-time** command to set the number of seconds that the network access server waits before trying to connect to the next host on the list; the default is 30 seconds.

Your RADIUS server might permit more than three Login-IP-Host entries; however, the network access server supports only three hosts in access-accept packets.

Configuring RADIUS Prompt

To control whether user responses to access-challenge packets are echoed to the screen, you can configure the Prompt attribute in the user profile on the RADIUS server. This attribute is included only in access-challenge packets. The following example shows the Prompt attribute set to No-Echo, which prevents the user's responses from echoing:

```
joeuser Password = xyz
Service-Type = Login,
Login-Service = Telnet,
Prompt = No-Echo,
Login-IP-Host = 172.31.255.255
```

To allow user responses to echo, set the attribute to Echo. If the Prompt attribute is not included in the user profile, responses are echoed by default.

This attribute overrides the behavior of the **radius-server challenge-noecho** command configured on the access server. For example, if the access server is configured to suppress echoing, but the individual user profile allows echoing, then the user responses are echoed.

**Note**

To use the Prompt attribute, your RADIUS server must be configured to support access-challenge packets.

Configuring Suffix and Password in RADIUS Access Requests

Large-scale dial-out eliminates the need to configure dialer maps on every NAS for every destination. Instead, you can create remote site profiles that contain outgoing call attributes on the AAA server. The profile is downloaded by the NAS when packet traffic requires a call to be placed to a remote site.

You can configure the username in the access-request message to RADIUS. The default suffix of the username, "-out," is appended to the username. The format for composing the username attribute is IP address plus configured suffix.

To provide username configuration capability for large-scale dial-out, the **dialer aaa** command is implemented with the new **suffix** and **password** keywords.

	Command	Purpose
Step 1	Router(config)# aaa new-model	Enables the AAA access control model.
Step 2	Router(config)# aaa route download min	Enables the download static route feature and sets the amount of time between downloads.
Step 3	Router(config)# aaa authorization configuration default	Downloads static route configuration information from the AAA server using TACACS+ or RADIUS.
Step 4	Router(config)# interface dialer 1	Defines a dialer rotary group.
Step 5	Router(config-if)# dialer aaa	Allows a dialer to access the AAA server for dialing information.
Step 6	Router(config-if)# dialer aaa suffix suffix password password	Allows a dialer to access the AAA server for dialing information and specifies a suffix and nondefault password for authentication.

Monitoring and Maintaining RADIUS

To monitor and maintain RADIUS, use the following commands in privileged EXEC mode:

Command	Purpose
Router# debug radius	Displays information associated with RADIUS.
Router# show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.

RADIUS Attributes

The network access server monitors the RADIUS authorization and accounting functions defined by RADIUS attributes in each user-profile. For a list of supported RADIUS attributes, refer to the appendix “RADIUS Attributes.”

This section includes the following sections:

- [Vendor-Proprietary RADIUS Attributes](#)
- [RADIUS Tunnel Attributes](#)

Vendor-Proprietary RADIUS Attributes

An Internet Engineering Task Force (IETF) draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the network access server and the RADIUS server. Some vendors, nevertheless, have extended the RADIUS attribute set in a unique way. Cisco IOS software supports a subset of vendor-proprietary RADIUS attributes. For a list of supported vendor-proprietary RADIUS attributes, refer to the appendix “RADIUS Attributes.”

RADIUS Tunnel Attributes

RADIUS is a security server authentication, authorization, and accounting (AAA) protocol originally developed by Livingston, Inc. RADIUS uses attribute value (AV) pairs to communicate information between the security server and the network access server. RFC 2138 and RFC 2139 describe the basic functionality of RADIUS and the original set of Internet Engineering Task Force (IETF)-standard AV pairs used to send AAA information. Two draft IETF standards, “RADIUS Attributes for Tunnel Protocol Support” and “RADIUS Accounting Modifications for Tunnel Protocol Support,” extend the IETF-defined set of AV pairs to include attributes specific to virtual private networks (VPNs); these attributes are used to carry the tunneling information between the RADIUS server and the tunnel initiator. RFC 2865 and RFC 2868 extend the IETF-defined set of AV pairs to include attributes specific to compulsory tunneling in VPNs by allowing the user to specify authentication names for the network access server and the RADIUS server.

Cisco routers and access servers now support new RADIUS IETF-standard VPDN tunnel attributes. These new RADIUS IETF-standard attributes are listed in the “RADIUS Attributes” appendix. Refer to the following three configuration examples later in this chapter:

- [RADIUS User Profile with RADIUS Tunneling Attributes Example](#)
- [L2TP Access Concentrator Examples](#)
- [L2TP Network Server Examples](#)

For more information about L2F, L2TP, VPN, or VPDN, refer to the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2.

RADIUS Configuration Examples

The following sections provide RADIUS configuration examples:

- [RADIUS Authentication and Authorization Example](#)
- [RADIUS Authentication, Authorization, and Accounting Example](#)
- [Vendor-Proprietary RADIUS Configuration Example](#)
- [RADIUS Server with Server-Specific Values Example](#)
- [Multiple RADIUS Servers with Global and Server-Specific Values Example](#)
- [Multiple RADIUS Server Entries for the Same Server IP Address Example](#)
- [RADIUS Server Group Examples](#)
- [Multiple RADIUS Server Entries Using AAA Server Groups Example](#)
- [AAA Server Group Selection Based on DNIS Example](#)
- [AAA Preauthentication Examples](#)
- [RADIUS User Profile with RADIUS Tunneling Attributes Example](#)
- [Guard Timer Examples](#)
- [L2TP Access Concentrator Examples](#)
- [L2TP Network Server Examples](#)

RADIUS Authentication and Authorization Example

The following example shows how to configure the router to authenticate and authorize using RADIUS:

```
aaa authentication login use-radius group radius local
aaa authentication ppp user-radius if-needed group radius
aaa authorization exec default group radius
aaa authorization network default group radius
```

The lines in this sample RADIUS authentication and authorization configuration are defined as follows:

- The **aaa authentication login use-radius group radius local** command configures the router to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database. In this example, **use-radius** is the name of the method list, which specifies RADIUS and then local authentication.
- The **aaa authentication ppp user-radius if-needed group radius** command configures the Cisco IOS software to use RADIUS authentication for lines using PPP with CHAP or PAP if the user has not already been authorized. If the EXEC facility has authenticated the user, RADIUS authentication is not performed. In this example, **user-radius** is the name of the method list defining RADIUS as the if-needed authentication method.
- The **aaa authorization exec default group radius** command sets the RADIUS information that is used for EXEC authorization, autocommands, and access lists.
- The **aaa authorization network default group radius** command sets RADIUS for network authorization, address assignment, and access lists.

RADIUS Authentication, Authorization, and Accounting Example

The following example shows a general configuration using RADIUS with the AAA command set:

```
radius-server host 123.45.1.2
radius-server key myRaDiUSpassWoRd
username root password ALongPassword
aaa authentication ppp dialins group radius local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
aaa authentication login admins local
aaa authorization exec default local
line 1 16
  autoselect ppp
  autoselect during-login
  login authentication admins
  modem ri-is-cd
interface group-async 1
  encaps ppp
  ppp authentication pap dialins
```

The lines in this example RADIUS authentication, authorization, and accounting configuration are defined as follows:

- The **radius-server host** command defines the IP address of the RADIUS server host.
- The **radius-server key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **aaa authentication ppp dialins group radius local** command defines the authentication method list “dialins,” which specifies that RADIUS authentication and then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP.

- The **ppp authentication pap dialins** command applies the “dialins” method list to the lines specified.
- The **aaa authorization network default group radius local** command is used to assign an address and other network parameters to the RADIUS user.
- The **aaa accounting network default start-stop group radius** command tracks PPP usage.
- The **aaa authentication login admins local** command defines another method list, “admins,” for login authentication.
- The **login authentication admins** command applies the “admins” method list for login authentication.

Vendor-Proprietary RADIUS Configuration Example

The following example shows a general configuration using vendor-proprietary RADIUS with the AAA command set:

```
radius-server host alcatraz non-standard
radius-server key myRaDiUSpassWoRd
radius-server configure-nas
username root password ALongPassword
aaa authentication ppp dialins group radius local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
aaa authentication login admins local
aaa authorization exec default local
line 1 16
autoselect ppp
autoselect during-login
login authentication admins
modem ri-is-cd
interface group-async 1
encaps ppp
ppp authentication pap dialins
```

The lines in this example RADIUS authentication, authorization, and accounting configuration are defined as follows:

- The **radius-server host non-standard** command defines the name of the RADIUS server host and identifies that this RADIUS host uses a vendor-proprietary version of RADIUS.
- The **radius-server key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **radius-server configure-nas** command defines that the Cisco router or access server will query the RADIUS server for static routes and IP pool definitions when the device first starts up.
- The **aaa authentication ppp dialins group radius local** command defines the authentication method list “dialins,” which specifies that RADIUS authentication, and then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP.
- The **ppp authentication pap dialins** command applies the “dialins” method list to the lines specified.
- The **aaa authorization network default group radius local** command is used to assign an address and other network parameters to the RADIUS user.
- The **aaa accounting network default start-stop group radius** command tracks PPP usage.

- The **aaa authentication login admins local** command defines another method list, “admins,” for login authentication.
- The **login authentication admins** command applies the “admins” method list for login authentication.

RADIUS Server with Server-Specific Values Example

The following example shows how to configure server-specific timeout, retransmit, and key values for the RADIUS server with IP address 172.31.39.46:

```
radius-server host 172.31.39.46 timeout 6 retransmit 5 key rad123
```

Multiple RADIUS Servers with Global and Server-Specific Values Example

The following example shows how to configure two RADIUS servers with specific timeout, retransmit, and key values. In this example, the **aaa new-model** command enables AAA services on the router, while specific AAA commands define the AAA services. The **radius-server retransmit** command changes the global retransmission value to 4 for all RADIUS servers. The **radius-server host** command configures specific timeout, retransmission, and key values for the RADIUS server hosts with IP addresses 172.16.1.1 and 172.29.39.46.

```
! Enable AAA services on the router and define those services.
aaa new-model
aaa authentication login default group radius
aaa authentication login console-login none
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius
enable password tryit1
!
! Change the global retransmission value for all RADIUS servers.
radius-server retransmit 4
!
! Configure per-server specific timeout, retransmission, and key values.
! Change the default auth-port and acct-port values.
radius-server host 172.16.1.1 auth-port 1612 acct-port 1616 timeout 3 retransmit 3 key
radkey
!
! Configure per-server specific timeout and key values. This server uses the global
! retransmission value.
radius-server host 172.29.39.46 timeout 6 key rad123
```

Multiple RADIUS Server Entries for the Same Server IP Address Example

The following example shows how to configure the network access server to recognize several RADIUS host entries with the same IP address. Two different host entries on the same RADIUS server are configured for the same services—authentication and accounting. The second host entry configured acts as fail-over backup to the first one. (The RADIUS host entries will be tried in the order they are configured.)

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group radius
```



```
! The next set of commands configures multiple host entries for the same IP address.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 2000 acct-port 2000
```

RADIUS Server Group Examples

The following example shows how to create server group *radgroup1* with three different RADIUS server members, each using the default authentication port (1645) and accounting port (1646):

```
aaa group server radius radgroup1
server 172.16.1.11
server 172.17.1.21
server 172.18.1.31
```

The following example shows how to create server group *radgroup2* with three RADIUS server members, each with the same IP address but with unique authentication and accounting ports:

```
aaa group server radius radgroup2
server 172.16.1.1 auth-port 1000 acct-port 1001
server 172.16.1.1 auth-port 2000 acct-port 2001
server 172.16.1.1 auth-port 3000 acct-port 3001
```

Multiple RADIUS Server Entries Using AAA Server Groups Example

The following example shows how to configure the network access server to recognize two different RADIUS server groups. One of these groups, *group1*, has two different host entries on the same RADIUS server configured for the same services. The second host entry configured acts as failover backup to the first one. Each group is individually configured for *deadtime*; *deadtime* for group 1 is one minute, and *deadtime* for group 2 is two minutes.



Note

In cases where both global commands and server commands are used, the server command will take precedence over the global command.

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group group1
! The following commands define the group1 RADIUS server group and associate servers
! with it and configures a deadtime of one minute.
aaa group server radius group1
server 1.1.1.1 auth-port 1645 acct-port 1646
server 2.2.2.2 auth-port 2000 acct-port 2001
deadtime 1
! The following commands define the group2 RADIUS server group and associate servers
! with it and configures a deadtime of two minutes.
aaa group server radius group2
server 2.2.2.2 auth-port 2000 acct-port 2001
server 3.3.3.3 auth-port 1645 acct-port 1646
deadtime 2
! The following set of commands configures the RADIUS attributes for each host entry
! associated with one of the defined server groups.
radius-server host 1.1.1.1 auth-port 1645 acct-port 1646
radius-server host 2.2.2.2 auth-port 2000 acct-port 2001
radius-server host 3.3.3.3 auth-port 1645 acct-port 1646
```

AAA Server Group Selection Based on DNIS Example

The following example shows how to select RADIUS server groups based on DNIS to provide specific AAA services:

```
! This command enables AAA.
aaa new-model
!
! The following set of commands configures the RADIUS attributes for each server
! that will be associated with one of the defined server groups.
radius-server host 172.16.0.1 auth-port 1645 acct-port 1646 key cisco1
radius-server host 172.17.0.1 auth-port 1645 acct-port 1646 key cisco2
radius-server host 172.18.0.1 auth-port 1645 acct-port 1646 key cisco3
radius-server host 172.19.0.1 auth-port 1645 acct-port 1646 key cisco4
radius-server host 172.20.0.1 auth-port 1645 acct-port 1646 key cisco5

! The following commands define the sg1 RADIUS server group and associate servers
! with it.
aaa group server radius sg1
  server 172.16.0.1
  server 172.17.0.1
! The following commands define the sg2 RADIUS server group and associate a server
! with it.
aaa group server radius sg2
  server 172.18.0.1
! The following commands define the sg3 RADIUS server group and associate a server
! with it.
aaa group server radius sg3
  server 172.19.0.1
! The following commands define the default-group RADIUS server group and associate
! a server with it.
aaa group server radius default-group
  server 172.20.0.1
!
! The next set of commands configures default-group RADIUS server group parameters.
aaa authentication ppp default group default-group
aaa accounting network default start-stop group default-group
!
```

```
! The next set of commands enables DNIS mapping and maps DNIS numbers to the defined
! RADIUS server groups. In this configuration, all PPP connection requests using
! DNIS 7777 are sent to the sg1 server group. The accounting records for these
! connections (specifically, start-stop records) are handled by the sg2 server group.
! Calls with a DNIS of 8888 use server group sg3 for authentication and server group
! default-group for accounting. Calls with a DNIS of 9999 use server group
! default-group for authentication and server group sg3 for accounting records
! (stop records only). All other calls with DNIS other than the ones defined use the
! server group default-group for both authentication and stop-start accounting records.
aaa dnis map enable
aaa dnis map 7777 authentication ppp group sg1
aaa dnis map 7777 accounting network start-stop group sg2
aaa dnis map 8888 authentication ppp group sg3
aaa dnis map 9999 accounting network stop-only group sg3
```

AAA Preauthentication Examples

The following example shows a simple configuration that specifies that the DNIS number be used for preauthentication:

```
aaa preauth
group radius
dnis required
```

The following example shows a configuration that specifies that both the DNIS number and the CLID number be used for preauthentication. DNIS preauthentication will be performed first, followed by CLID preauthentication.

```
aaa preauth
  group radius
  dnis required
  clid required
```

The following example specifies that preauthentication be performed on all DNIS numbers except the two DNIS numbers specified in the DNIS group called “hawaii”:

```
aaa preauth
group radius
dnis required
dnis bypass hawaii
```

```
dialer dnis group hawaii
  number 12345
  number 12346
```

The following example shows a sample AAA configuration with DNIS preauthentication:

```
aaa new-model
aaa authentication login CONSOLE none
aaa authentication login RADIUS_LIST group radius
aaa authentication login TAC_PLUS group tacacs+ enable
aaa authentication login V.120 none
aaa authentication enable default enable group tacacs+
aaa authentication ppp RADIUS_LIST if-needed group radius
aaa authorization exec RADIUS_LIST group radius if-authenticated
aaa authorization exec V.120 none
aaa authorization network default group radius if-authenticated
aaa authorization network RADIUS_LIST if-authenticated group radius
aaa authorization network V.120 group radius if-authenticated
aaa accounting suppress null-username
aaa accounting exec default start-stop group radius
aaa accounting commands 0 default start-stop group radius
```

```

aaa accounting network default start-stop group radius
aaa accounting connection default start-stop group radius
aaa accounting system default start-stop group radius
aaa preauth
  dn timer 30
aaa nas port extended
!
radius-server configure-nas
radius-server host 10.0.0.0 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.255.255.255 auth-port 1645 acct-port 1646 non-standard
radius-server retransmit 2
radius-server deadtime 1
radius-server attribute nas-port format c
radius-server unique-ident 18
radius-server key MyKey

```

**Note**

To configure preauthentication, you must also set up preauthentication profiles on the RADIUS server.

RADIUS User Profile with RADIUS Tunneling Attributes Example

The following example shows a RADIUS user profile (Merit Daemon format) that includes RADIUS tunneling attributes. This entry supports two tunnels, one for L2F and the other for L2TP. The tag entries with :1 support L2F tunnels, and the tag entries with :2 support L2TP tunnels.

```

cisco.com Password = "cisco", Service-Type = Outbound
  Service-Type = Outbound,
  Tunnel-Type = :1:L2F,
  Tunnel-Medium-Type = :1:IP,
  Tunnel-Client-Endpoint = :1:"10.0.0.2",
  Tunnel-Server-Endpoint = :1:"10.0.0.3",
  Tunnel-Client-Auth-Id = :1:"l2f-cli-auth-id",
  Tunnel-Server-Auth-Id = :1:"l2f-svr-auth-id",
  Tunnel-Assignment-Id = :1:"l2f-assignment-id",
  Cisco-Avpair = "vpdn:nas-password=l2f-cli-pass",
  Cisco-Avpair = "vpdn:gw-password=l2f-svr-pass",
  Tunnel-Preference = :1:1,
  Tunnel-Type = :2:L2TP,
  Tunnel-Medium-Type = :2:IP,
  Tunnel-Client-Endpoint = :2:"10.0.0.2",
  Tunnel-Server-Endpoint = :2:"10.0.0.3",
  Tunnel-Client-Auth-Id = :2:"l2tp-cli-auth-id",
  Tunnel-Server-Auth-Id = :2:"l2tp-svr-auth-id",
  Tunnel-Assignment-Id = :2:"l2tp-assignment-id",
  Cisco-Avpair = "vpdn:l2tp-tunnel-password=l2tp-tnl-pass",
  Tunnel-Preference = :2:2

```

Guard Timer Examples

The following example shows an ISDN guard timer that is set at 8000 milliseconds. A call will be rejected if the RADIUS server has not responded to a preauthentication request when the timer expires.

```

interface serial1/0/0:23
  isdn guard-timer 8000 on-expiry reject

aaa preauth
  group radius
  dn timer 30

```

The following example shows a CAS guard timer that is set at 20,000 milliseconds. A call will be accepted if the RADIUS server has not responded to a preauthentication request when the timer expires.

```
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
 cas-custom 0
 call guard-timer 20000 on-expiry accept

aaa preauth
group radius
dnis required
```

L2TP Access Concentrator Examples

The following example shows a basic L2TP configuration for the L2TP access concentrator (LAC) for the topology shown in [Figure 12](#). The local name is not defined, so the host name used is the local name. Because the L2TP tunnel password is not defined, the username password is used. In this example, VPDN is configured locally on the LAC and does not take advantage of the new RADIUS tunnel attributes.

Figure 12 *Topology for Configuration Examples*



```
! Enable AAA globally.
aaa new-model
! Enable AAA authentication for PPP and list the default method to use for PPP
! authentication.
aaa authentication ppp default local
! Define the username as "DJ."
username DJ password 7 030C5E070A00781B
! Enable VPDN.
vpdn enable
! Define VPDN group number 1.
vpdn-group 1
! Allow the LAC to respond to dialin requests using L2TP from IP address 172.21.9.13
! domain "cisco.com."
request dialin
protocol l2tp
domain cisco.com
initiate-ip to 172.21.9.13
local name nas-1
```

The following example shows how to configure the LAC if RADIUS tunnel attributes are supported. In this example, there is no local VPDN configuration on the LAC; the LAC, instead, is configured to query the remote RADIUS security server.

```
! Enable global AAA securities services.
aaa new-model
```

```

! Enable AAA authentication for PPP and list RADIUS as the default method to use
! for PPP authentication.
aaa authentication ppp default group radius local
! Enable AAA (network) authorization and list RADIUS as the default method to use for
! authorization.
aaa authorization network default group radius
! Define the username as "DJ."
username DJ password 7 030C5E070A00781B
! Enable VPDN.
vpdn enable
! Configure the LAC to interface with the remote RADIUS security server.
radius host 171.69.1.1 auth-port 1645 acct-port 1646
radius-server key cisco

```

L2TP Network Server Examples

The following example shows a basic L2TP configuration with corresponding comments on the L2TP network server (LNS) for the topology shown in [Figure 12](#):

```

! Enable AAA globally.
aaa new-model
! Enable AAA authentication for PPP and list the default method to use for PPP
! authentication.
aaa authentication ppp default local
! Define the username as "partner."
username partner password 7 030C5E070A00781B
! Create virtual-template 1 and assign all values for virtual access interfaces.
interface Virtual-Template1
! Borrow the IP address from interface ethernet 1.
ip unnumbered Ethernet0
! Disable multicast fast switching.
no ip mroute-cache
! Use CHAP to authenticate PPP.
ppp authentication chap
! Enable VPDN.
vpdn enable
! Create vpdn-group number 1.
vpdn-group 1
! Accept all dialin l2tp tunnels from virtual-template 1 from remote peer DJ.
accept dialin l2tp virtual-template 1 remote DJ
protocol any
virtual-template 1
terminate-from hostname nas1
local name hgw1

```

The following example shows how to configure the LNS with a basic L2F and L2TP configuration using RADIUS tunneling attributes:

```

aaa new-model
aaa authentication login default none
aaa authentication login console none
aaa authentication ppp default local group radius
aaa authorization network default group radius if-authenticated
!
username l2f-cli-auth-id password 0 l2f-cli-pass
username l2f-svr-auth-id password 0 l2f-svr-pass
username l2tp-svr-auth-id password 0 l2tp-tnl-pass
!
vpdn enable
vpdn search-order domain
!
vpdn-group 1

```

```
accept-dialin
protocol l2f
virtual-template 1
terminate-from hostname l2f-cli-auth-id
local name l2f-svr-auth-id
!
vpdn-group 2
accept-dialin
protocol l2tp
virtual-template 2
terminate-from hostname l2tp-cli-auth-id
local name l2tp-svr-auth-id
!
interface Ethernet1/0
ip address 10.0.0.3 255.255.255.0
no ip route-cache
no ip mroute-cache
!
interface Virtual-Template1
ip unnumbered Ethernet1/0
ppp authentication pap
!
interface Virtual-Template2
ip unnumbered Ethernet1/0
ppp authentication pap
!
radius-server host 1.1.1.1 auth-port 1645 acct-port 1646
radius-server key <deleted>
!
```



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



AAA Dead-Server Detection

First Published: February 13, 2004

Last Updated: March 4, 2008

The AAA Dead-Server Detection feature allows you to configure the criteria that are to be used to mark a RADIUS server as dead. If no criteria are explicitly configured, the criteria will be computed dynamically on the basis of the number of outstanding transactions. Using this feature will result in less downtime and quicker packet processing.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for AAA Dead-Server Detection](#)” section on page 9.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for AAA Dead-Server Detection, page 2](#)
- [Restrictions for AAA Dead-Server Detection, page 2](#)
- [Information About AAA Dead-Server Detection, page 2](#)
- [How to Configure AAA Dead-Server Detection, page 3](#)
- [Configuration Examples for AAA Dead-Server Detection, page 5](#)
- [Additional References, page 6](#)
- [Command Reference, page 8](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008 Cisco Systems, Inc. All rights reserved.

Prerequisites for AAA Dead-Server Detection

- You must have access to a RADIUS server.
- You should be familiar with configuring a RADIUS server.
- You should be familiar with configuring authentication, authorization, and accounting (AAA).
- Before a server can be marked as dead, you must first configure the **radius-server deadtime** command. If this command is not configured, even if the criteria are met for the server to be marked as dead, the server state will be the “up” state.

Restrictions for AAA Dead-Server Detection

- Original transmissions are not counted in the number of consecutive timeouts that must occur on the router before the server is marked as dead—only the number of retransmissions are counted.

Information About AAA Dead-Server Detection

To configure the AAA Dead-Server Detection feature, you should understand the following concept:

- [Criteria for Marking a RADIUS Server As Dead, page 2](#)

Criteria for Marking a RADIUS Server As Dead

The AAA Dead-Server Detection feature allows you to determine the criteria that are used to mark a RADIUS server as dead. That is, you can configure the minimum amount of time, in seconds, that must elapse from the time that the router last received a valid packet from the RADIUS server to the time the server is marked as dead. If a packet has not been received since the router booted, and there is a timeout, the time criterion will be treated as though it has been met.

In addition, you can configure the number of consecutive timeouts that must occur on the router before the RADIUS server is marked as dead. If the server performs both authentication and accounting, both types of packets are included in the number. Improperly constructed packets are counted as though they are timeouts. Only retransmissions are counted, not the initial transmission. (Each timeout causes one retransmission to be sent.)



Note

Both the time criterion and the tries criterion must be met for the server to be marked as dead.

The RADIUS dead-server detection configuration will result in the prompt detection of RADIUS servers that have stopped responding. This configuration will also result in the avoidance of servers being improperly marked as dead when they are “swamped” (responding slowly) and the avoidance of the state of servers being rapidly changed from dead to live to dead again. This prompt detection of nonresponding RADIUS servers and the avoidance of swamped and dead-to-live-to-dead-again servers will result in less deadtime and quicker packet processing.

How to Configure AAA Dead-Server Detection

This section contains the following procedures:

- [Configuring AAA Dead-Server Detection, page 3](#) (required)
- [Verifying AAA Dead-Server Detection, page 4](#) (optional)

Configuring AAA Dead-Server Detection

To configure AAA Dead-Server Detection, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server deadtime** *minutes*
5. **radius-server dead-criteria** [**time** *seconds*] [**tries** *number-of-tries*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Router (config)# aaa new-model	Enables the AAA access control model.
Step 4	radius-server deadtime <i>minutes</i> Example: Router (config)# radius-server deadtime 5	Improves RADIUS response times when some servers might be unavailable and causes the unavailable servers to be skipped immediately.
Step 5	radius-server dead-criteria [<i>time seconds</i>] [<i>tries number-of-tries</i>] Example: Router (config)# radius-server dead-criteria time 5 tries 4	Forces one or both of the criteria—used to mark a RADIUS server as dead—to be the indicated constant.

Troubleshooting Tips

After you have configured AAA Dead-Server Detection, you should verify your configuration using the **show running-config** command. This verification is especially important if you have used the **no** form of the **radius-server dead-criteria** command. The output of the **show running-config** command must show the same values in the “Dead Criteria Details” field that you configured using the **radius-server dead-criteria** command.

Verifying AAA Dead-Server Detection

To verify your AAA Dead-Server Detection configuration, perform the following steps. The **show** and **debug** commands may be used in any order.

SUMMARY STEPS

1. **enable**
2. **debug aaa dead-criteria transactions**
3. **show aaa dead-criteria**
4. **show aaa servers**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	debug aaa dead-criteria transactions Example: Router# debug aaa dead-criteria transactions	Displays AAA dead-criteria transaction values.
Step 3	show aaa dead-criteria Example: Router# show aaa dead-criteria	Displays dead-criteria information for a AAA server.
Step 4	show aaa servers [private public] Example: Router# show aaa server private	Displays the status and number of packets that are sent to and received from all public and private authentication, authorization, and accounting (AAA) RADIUS servers. <ul style="list-style-type: none"> The private keyword optionally displays the AAA servers only. The public keyword optionally displays the AAA servers only.

Configuration Examples for AAA Dead-Server Detection

This section provides the following configuration examples:

- [Configuring AAA Dead-Server Detection: Example, page 5](#)
- [debug aaa dead-criteria transactions Command: Example, page 6](#)
- [show aaa dead-criteria Command: Example, page 6](#)

Configuring AAA Dead-Server Detection: Example

The following example shows that the router will be considered dead after 5 seconds and four tries:

```
Router (config)# aaa new-model
Router (config)# radius-server deadtime 5
Router (config)# radius-server dead-criteria time 5 tries 4
```

debug aaa dead-criteria transactions Command: Example

The following output example shows dead-criteria transaction information for a particular server group:

```
Router# debug aaa dead-criteria transactions
```

```
AAA Transaction debugs debugging is on
```

```
*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Computed Retransmit Tries: 22, Current Max Tries: 22
*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Computed Dead Detect Interval: 25s, Current Max
Interval: 25s
*Nov 14 23:44:17.403: AAA/SG/TRANSAC: Estimated Outstanding Transactions: 6, Current Max
Transactions: 6
```

show aaa dead-criteria Command: Example

The following output example shows that dead-server-detection information has been requested for a RADIUS server at the IP address 172.19.192.80:

```
Router# show aaa dead-criteria radius 172.19.192.80 radius
```

```
RADIUS Server Dead Criteria:
=====
Server Details:
  Address : 172.19.192.80
  Auth Port : 1645
  Acct Port : 1646
Server Group : radius
Dead Criteria Details:
  Configured Retransmits : 62
  Configured Timeout : 27
  Estimated Outstanding Transactions: 5
  Dead Detect Time : 25s
  Computed Retransmit Tries: 22
  Statistics Gathered Since Last Successful Transaction
=====
Max Computed Outstanding Transactions: 5
Max Computed Dead Detect Time: 25s
Max Computed Retransmits : 22
```

Additional References

The following sections provide references related to the AAA Dead-Server Detection feature.

Related Documents

Related Topic	Document Title
Configuring RADIUS	“ Configuring RADIUS ” chapter of <i>Cisco IOS Security Configuration Guide</i>
Configuring AAA	“ Authentication, Authorization, and Accounting (AAA) ” section of <i>Cisco IOS Security Configuration Guide</i>
Security commands	<i>Cisco IOS Security Commands</i> , Release 12.3 T

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug aaa dead-criteria transactions**
- **radius-server dead-criteria**
- **show aaa dead-criteria**
- **show aaa servers**

Feature Information for AAA Dead-Server Detection

Table 15 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Releases 12.2(1) or 12.0(3)S or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 15 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 15 Feature Information for AAA Dead-Server Detection

Feature Name	Releases	Feature Information
AAA Dead-Server Detection	12.3(6)	This feature was introduced.
	12.3(7)T	This feature was integrated into Cisco IOS Release 12.3(7)T.

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.



AAA-SERVER-MIB Set Operation

The AAA-SERVER-MIB Set Operation feature allows you to extend and expand your ability to configure authentication, authorization, and accounting (AAA) servers using the CISCO-AAA-SERVER-MIB. Using this feature, you can do the following:

- Create and add new AAA servers.
- Modify the “KEY” under the CISCO-AAA-SERVER-MIB.
- Delete the AAA server configuration.

History for the AAA-SERVER-MIB Set Operation Feature

Release	Modification
12.4(4)T	This feature was introduced.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for AAA-SERVER-MIB Set Operation, page 2](#)
- [Restrictions for AAA-SERVER-MIB Set Operation, page 2](#)
- [Information About AAA-SERVER-MIB Set Operation, page 2](#)
- [How to Configure AAA-SERVER-MIB Set Operation, page 3](#)
- [Configuration Examples for AAA-SERVER-MIB Set Operation, page 3](#)
- [Additional References, page 6](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for AAA-SERVER-MIB Set Operation

AAA must have been enabled on the router, that is, the **aaa new-model** command must have been configured. If this configuration has not been accomplished, the set operation fails.

Restrictions for AAA-SERVER-MIB Set Operation

Currently, the CISCO SNMP set operation is supported only for the RADIUS protocol. Therefore, only RADIUS servers in global configuration mode can be added, modified, or deleted.

Information About AAA-SERVER-MIB Set Operation

Before using the AAA-SERVER-MIB Set Operation feature, you should understand the following concepts:

- [CISCO-AAA-SERVER-MIB, page 2](#)
- [CISCO-AAA-SERVER-MIB Set Operation, page 2](#)

CISCO-AAA-SERVER-MIB

The CISCO-AAA-SERVER-MIB provides that statistics reflect both the state of the AAA server operation with the server itself and of AAA communications with external servers. The CISCO-AAA-SERVER-MIB provides the following information:

- Statistics for each AAA operation
- Status of servers that are providing AAA functions
- Identities of external AAA servers

CISCO-AAA-SERVER-MIB Set Operation

Before Cisco IOS Release 12.4(4)T, the CISCO-AAA-SERVER-MIB supported only the “get” operation. Effective with this release, the CISCO-AAA-SERVER-MIB supports the set operation. With the set operation, you can do the following:

- Create or add a new AAA server.
- Modify the KEY under the CISCO-AAA-SERVER-MIB. This “secret key” is used for secure connectivity to the AAA server, which is present with the network access server (NAS) and the AAA server.
- Delete the AAA server configuration.

How to Configure AAA-SERVER-MIB Set Operation

No special configuration is required for this feature. The Simple Network Management Protocol (SNMP) framework can be used to manage MIBs. See the section “[Additional References](#)” for a reference to configuring SNMP.

SNMP values can be verified by performing the following steps.

SUMMARY STEPS

1. **enable**
2. **show running-config | include radius-server host**
3. **show aaa servers**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	show running-config include radius-server host Example: Router# show running-config include radius-server host	Displays all the RADIUS servers that are configured in the global configuration mode.
Step 3	show aaa servers Example: Router# show aaa servers	Displays information about the number of requests sent to and received from authentication, authorization, and accounting (AAA) servers.

Configuration Examples for AAA-SERVER-MIB Set Operation

This section includes the following example:

- [RADIUS Server Configuration and Server Statistics: Example, page 4](#)

RADIUS Server Configuration and Server Statistics: Example

The following output example shows the RADIUS server configuration and server statistics before and after the set operation.

Before the Set Operation

```
Router# show running-config | include radius-server host
```

```
! The following line is for server 1.
radius-server host 172.19.192.238 auth-port 2095 acct-port 2096 key cisco2
! The following line is for server 2.
radius-server host 172.19.192.238 auth-port 1645 acct-port 1646
```

Server Statistics

```
Router# show aaa servers
```

```
RADIUS: id 2, priority 1, host 172.19.192.238, auth-port 2095, acct-port 2096
State: current UP, duration 25s, previous duration 0s
  Dead: total time 0s, count 7
Authen: request 8, timeouts 8
  Response: unexpected 0, server error 0, incorrect 0, time 0ms
  Transaction: success 0, failure 2
Author: request 0, timeouts 0
  Response: unexpected 0, server error 0, incorrect 0, time 0ms
  Transaction: success 0, failure 0
Account: request 0, timeouts 0
  Response: unexpected 0, server error 0, incorrect 0, time 0ms
  Transaction: success 0, failure 0
Elapsed time since counters last cleared: 5m

RADIUS: id 3, priority 2, host 172.19.192.238, auth-port 1645, acct-port 1646
State: current UP, duration 5s, previous duration 0s
  Dead: total time 0s, count 2
Authen: request 8, timeouts 8
  Response: unexpected 0, server error 0, incorrect 0, time 0ms
  Transaction: success 0, failure 4
Author: request 0, timeouts 0
  Response: unexpected 0, server error 0, incorrect 0, time 0ms
  Transaction: success 0, failure 0
Account: request 0, timeouts 0
  Response: unexpected 0, server error 0, incorrect 0, time 0ms
  Transaction: success 0, failure 0
Elapsed time since counters last cleared: 3m
```

SNMP Get Operation to Check the Configuration and Statistics of the RADIUS Servers

```
aaa-server5:/users/smetri> getmany 10.0.1.42 casConfigTable
casAddress.2.2 = 172.19.192.238
casAddress.2.3 = 172.19.192.238
casAuthenPort.2.2 = 2095
casAuthenPort.2.3 = 1645
casAcctPort.2.2 = 2096
casAcctPort.2.3 = 1646
casKey.2.2 =
casKey.2.3 =
! The following line shows priority for server 1.
casPriority.2.2 = 1
! The following line shows priority for server 2.
casPriority.2.3 = 2
casConfigRowStatus.2.2 = active(1)
casConfigRowStatus.2.3 = active(1)
aaa-server5:/users/smetri>
```

SNMP Set Operation

The key of the existing RADIUS server is being changed. The index "1" is being used. That index acts as a wildcard for addition, deletion, or modification of any entries.

Change the key for server 1:=>

```
aaa-server5:/users/smetri> setany -v2c 10.0.1.42 public casAddress.2.1 -a 172.19.192.238
casAuthenPort.2.1 -i 2095 casAcctPort.2.1 -i 2096 casKey.2.1 -o king
casAddress.2.1 = 172.19.192.238
casAuthenPort.2.1 = 2095
casAcctPort.2.1 = 2096
casKey.2.1 = king
aaa-server5:/users/smetri>
```

After the Set Operation

After the above SNMP set operation, the configurations on the router change. The following output shows the output after the set operation.

Router# **show running-config | include radius-server host**

```
radius-server host 172.19.192.238 auth-port 1645 acct-port 1646
! The following line shows a change in the key value to "king."
radius-server host 172.19.192.238 auth-port 2095 acct-port 2096 key king
```

Router# **show aaa servers**

```
RADIUS: id 3, priority 1, host 172.19.192.238, auth-port 1645, acct-port 1646
State: current UP, duration 189s, previous duration 0s
  Dead: total time 0s, count 2
Authen: request 8, timeouts 8
  Response: unexpected 0, server error 0, incorrect 0, time 0ms
  Transaction: success 0, failure 4
Author: request 0, timeouts 0
  Response: unexpected 0, server error 0, incorrect 0, time 0ms
  Transaction: success 0, failure 0
Account: request 0, timeouts 0
  Response: unexpected 0, server error 0, incorrect 0, time 0ms
  Transaction: success 0, failure 0
Elapsed time since counters last cleared: 6m

! The following line shows a new server with new statistics.
RADIUS: id 4, priority 2, host 172.19.192.238, auth-port 2095, acct-port 2096
State: current UP, duration 209s, previous duration 0s
  Dead: total time 0s, count 7
Authen: request 0, timeouts 0
  Response: unexpected 0, server error 0, incorrect 0, time 0ms
  Transaction: success 0, failure 0
Author: request 0, timeouts 0
  Response: unexpected 0, server error 0, incorrect 0, time 0ms
  Transaction: success 0, failure 0
Account: request 0, timeouts 0
  Response: unexpected 0, server error 0, incorrect 0, time 0ms
```

Additional References

The following sections provide references related to the AAA-SERVER-MIB Set Operation feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands, including show commands	Cisco IOS Master Commands List
Configuring SNMP	The chapter “ Configuring SNMP Support ” in the <i>Cisco IOS Network Management Configuration Guide</i>

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2007 Cisco Systems, Inc. All rights reserved.



ACL Default Direction

First Published: October 15, 2001

Last Updated: February 23, 2007

The ACL Default Direction feature allows you to change the filter direction (where filter direction is not specified) to inbound packets only; that is, you can configure your server to filter packets that are coming toward the network.

History for the ACL Default Direction Feature

Release	Modification
12.2(4)T	This feature was introduced.
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB3	This feature was integrated into Cisco IOS Release 12.2(31)SB3.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for ACL Default Direction, page 2](#)
- [Information About ACL Default Direction, page 2](#)
- [How to Configure ACL Default Direction, page 2](#)
- [Configuration Examples for ACL Default Direction, page 4](#)
- [Additional References, page 5](#)
- [Command Reference, page 7](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for ACL Default Direction

Before you can change the default direction of filters from RADIUS, you must perform the following tasks:

- Configure your network access server (NAS) for authentication, authorization, and accounting (AAA) and to accept incoming calls.

For more information, refer to the AAA chapters of the [Cisco IOS Security Configuration Guide](#), Release 12.4 and the [Cisco IOS Dial Technologies Configuration Guide](#), Release 12.4.

- Create a filter on your NAS.

For more information, refer to the section “[Configuring IP Services](#)” section of the chapter IP Addressing and Services of the [Cisco IOS IP Addressing Services Configuration Guide](#), Release 12.4.

- Add a filter definition for a RADIUS user; for example, Filter-Id = “myfilter”.

Information About ACL Default Direction

Before changing the default direction of filters for your access control lists (ACLs) from RADIUS, you should understand the following concepts:

- [The radius-server attribute 11 direction default Command, page 2](#)
- [Benefits of ACL Default Direction, page 2](#)

The radius-server attribute 11 direction default Command

The **radius-server attribute 11 direction default** command allows you to change the default direction of filters for your ACLs via RADIUS. (RADIUS attribute 11 (Filter-Id) indicates the name of the filter list for the user.) Enabling this command allows you to change the filter direction to inbound—which stops traffic from entering a router, and reduces resource consumption—rather than keeping the outbound default direction, where filtering occurs only as the traffic is about to leave the network.

Benefits of ACL Default Direction

The ACL Default Direction feature allows you to change the default direction, which is outbound, of filters for your ACLs to inbound via the **radius-server attribute 11 direction default** command.

How to Configure ACL Default Direction

This section contains the following procedures:

- [Configuring the ACL Default Direction from RADIUS via Attribute 11 \(Filter-Id\), page 3](#) (required)
- [Verifying the ACL Default Direction from RADIUS via Attribute 11 \(Filter-Id\), page 3](#) (optional)

Configuring the ACL Default Direction from RADIUS via Attribute 11 (Filter-Id)

To configure the default direction of filters from RADIUS via attribute 11, perform the following steps.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `radius-server attribute 11 direction default [inbound | outbound]`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# <code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>radius-server attribute 11 direction default [inbound outbound]</code> Example: Router(config)# <code>radius-server attribute 11 direction default inbound</code>	Specifies the default direction of filters from RADIUS to inbound or outbound.

Verifying the ACL Default Direction from RADIUS via Attribute 11 (Filter-Id)

To verify the default direction of filters from RADIUS and to verify that RADIUS attribute 11 is being sent in access accept requests, perform the following steps.

SUMMARY STEPS

1. `enable`
2. `more system:running-config`
3. `debug radius`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	more system:running-config Example: Router# more system:running-config	Displays the contents of the current running configuration file.
Step 3	debug radius Example: Router# debug radius	Displays information associated with RADIUS. The output of this command shows whether attribute 11 is being sent in access accept requests.

Configuration Examples for ACL Default Direction

This section provides the following configuration examples:

- [Default Direction of Filters via RADIUS Attribute 11 \(Filter-Id\): Example, page 4](#)
- [RADIUS User Profile with Filter-Id: Example, page 4](#)

Default Direction of Filters via RADIUS Attribute 11 (Filter-Id): Example

The following example shows how to configure RADIUS attribute 11 to change the default direction of filters. In this example, the filtering is applied to inbound packets only.

radius-server attribute 11 direction default inbound

RADIUS User Profile with Filter-Id: Example

The following is an example of a RADIUS user profile (Merit Daemon format) that includes RADIUS attribute 11 (Filter-Id):

```
client Password = "password1"
    Service-Type = Framed,
    Framed-Protocol = PPP,
    Filter-Id = "myfilter.out"
```

The RADIUS user profile shown in this example produces the following reply from the NAS:

```
RADIUS: Send to unknown id 79 10.51.13.4:1645, Access-Request, len 85
RADIUS: authenticator 84 D3 B5 7D C2 5B 70 AD - 1E 5C 56 E8 3A 91 D0 6E
RADIUS: User-Name          [1]  8  "client"
RADIUS: CHAP-Password      [3]  19  *
RADIUS: NAS-Port           [5]  6  20030
RADIUS: NAS-Port-Type      [61] 6  ISDN                      [2]
RADIUS: Called-Station-Id  [30] 6  "4321"
RADIUS: Calling-Station-Id [31] 6  "1234"
RADIUS: Service-Type       [6]  6  Framed                      [2]
```

```

RADIUS: NAS-IP-Address      [4]   6   10.1.73.74

RADIUS: Received from id 79 10.51.13.4:1645, Access-Accept, len 46
RADIUS: authenticator 9C 6C 66 E2 F1 42 D6 4B - C1 7D D4 5E 9D 09 BB A1
RADIUS: Service-Type        [6]   6   Framed                      [2]
RADIUS: Framed-Protocol     [7]   6   PPP                        [1]
RADIUS: Filter-Id           [11]  14
RADIUS: 6D 79 66 69 6C 74 65 72 2E 6F 75 74      [myfilter.out]

```

Additional References

The following sections provide references related to the ACL Default Direction feature.

Related Documents

Related Topic	Document Title
Cisco IOS Dial Technologies configuration	<i>Cisco IOS Dial Technologies Configuration Guide</i> , Release 12.4
Cisco IOS security configuration	<i>Cisco IOS Security Configuration Guide</i> , Release 12.4
Cisco IOS security commands	<ul style="list-style-type: none"> • <i>Cisco IOS Security Command Reference</i>, Release 12.4T • <i>Cisco IOS Security Command Reference</i>, Release 12.2SB • <i>Cisco IOS Security Command Reference</i>, Release 12.2 SR
Configuring IP services	“Configuring IP Services” section of the chapter “IP Addressing and Services” of the <i>Cisco IOS IP Addressing Services Configuration Guide</i> , Release 12.4.

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

RFCs

RFC	Title
RFC 2865	<i>Remote Authentication Dial-In User Service (RADIUS)</i>

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **radius-server attribute 11 direction default**

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0708R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Attribute Screening for Access Requests

First Published: November 19, 2003

Last Updated: December 17, 2007

The Attribute Screening for Access Requests feature allows you to configure your network access server (NAS) to filter attributes in outbound Access Requests to the RADIUS server for purposes of authentication or authorization.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Attribute Screening for Access Requests](#)” section on [page 9](#).

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Attribute Screening for Access Requests, page 2](#)
- [Restrictions for Attribute Screening for Access Requests, page 2](#)
- [Information About Attribute Screening for Access Requests, page 2](#)
- [How to Configure Attribute Screening for Access Requests, page 2](#)
- [Configuration Examples for Attribute Filtering for Access Requests, page 6](#)
- [Additional References, page 7](#)
- [Command Reference, page 8](#)
- [Feature Information for Attribute Screening for Access Requests, page 9](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2003–2004, 2006–2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for Attribute Screening for Access Requests

- You must be familiar with configuring attribute lists.

Restrictions for Attribute Screening for Access Requests

- Attributes 1 (Username), 2 (User-Password), and 3 (Chap-Password) cannot be filtered.

Information About Attribute Screening for Access Requests

To configure the Attribute Screening for Access Requests feature, you should understand the following concept:

- [Configuring an NAS to Filter Attributes in Outbound Access Requests, page 2](#)

Configuring an NAS to Filter Attributes in Outbound Access Requests

The Attribute Screening for Access Requests feature allows you to configure your NAS to filter attributes in outbound Access Requests to the RADIUS server for purposes of authentication or authorization. The filters can be configured on the NAS, or they can be downloaded via downloadable vendor-specific attributes (VSAs) from the authentication, authorization, and accounting (AAA) server.

The following are some examples of the downloadable VSAs:

```
Cisco:Cisco-Avpair="ppp-authen-type=chap"  
Cisco:Cisco-Avpair="ppp-authen-list=group 1"  
Cisco:Cisco-Avpair="ppp-author-list=group 1"  
Cisco:Cisco-Avpair="vpdn:tunnel-id=B53"  
Cisco:Cisco-Avpair="vpdn:ip-addresses=10.0.58.35"
```

**Note**

You must be aware of which attributes you want to filter. Filtering certain key attributes can result in authentication failure (for example, attribute 60 should not be filtered).

How to Configure Attribute Screening for Access Requests

This section contains the following procedures:

- [Configuring Attribute Screening for Access Requests, page 3](#)
- [Configuring a Router to Support Downloadable Filters, page 4](#)
- [Monitoring and Maintaining Attribute Filtering for Access Requests, page 5](#)

Configuring Attribute Screening for Access Requests

To configure the attribute screening for access requests, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute list** *listname*
4. **attribute** *value1* [*value2* [*value3...*]]
5. **aaa group server radius** *group-name*
6. **authorization** [**request** | **reply**] [**accept** | **reject**] *listname*
or
accounting [**request** | **reply**] [**accept** | **reject**] *listname*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	radius-server attribute list <i>listname</i> Example: Router (config)# radius-server attribute list attrlist	Defines an attribute list.
Step 4	attribute <i>value1</i> [<i>value2</i> [<i>value3...</i>]] Example: Router (config)# attribute 6-10, 12	Adds attributes to an accept or reject list.
Step 5	aaa group server radius <i>group-name</i> Example: Router (config)# aaa group server radius rad1	Applies the attribute list to the AAA server group and enters server-group configuration mode.

	Command or Action	Purpose
Step 6	<p>authorization [request reply] [accept reject] <i>listname</i></p> <p>or</p> <p>accounting [request reply] [accept reject] <i>listname</i></p> <p>Example: Router (config-sg-radius)# authorization request accept attrlist</p> <p>or</p> <p>Example: Router (config-sg-radius)# accounting request accept attrlist</p>	<p>Filters attributes in outbound Access Requests to the RADIUS server for purposes of authentication or authorization.</p> <ul style="list-style-type: none"> The request keyword defines filters for outgoing authorization Access Requests. The reply keyword defines filters for incoming authorization Accept and Reject packets and for outgoing accounting requests.

Configuring a Router to Support Downloadable Filters

To configure your router to support downloadable filters, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authorization template**
4. **aaa authorization network default group radius**
5. **radius-server attribute list** *list-name*
6. **attribute** *value1* [*value2* [*value3...*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>aaa authorization template</p> <p>Example: Router (config)# aaa authorization template</p>	<p>Enables usage of a local or remote customer template on the basis of Virtual Private Network (VPN) routing and forwarding (VRF).</p>

	Command or Action	Purpose
Step 4	aaa authorization network default group radius Example: Router (config)# aaa authorization network default group radius	Sets parameters that restrict user access to a network.
Step 5	radius-server attribute list list-name Example: Router (config)# radius-server attribute list attlist	Defines an accept or reject list name.
Step 6	attribute value1 [value2 [value3...]] Example: Router (config)# attribute 10-14, 24	Adds attributes to an accept or reject list.

Troubleshooting Tips

If attribute filtering is not working, ensure that the attribute list is properly defined.

Monitoring and Maintaining Attribute Filtering for Access Requests

To monitor and maintain attribute filtering, you can use the **debug radius** command.

SUMMARY STEPS

1. **enable**
2. **debug radius**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	debug radius Example: Router# debug radius	Displays information associated with RADIUS, including filtering information.

Configuration Examples for Attribute Filtering for Access Requests

This section provides the following configuration examples:

- [Attribute Filtering for Access Requests: Example, page 6](#)
- [Attribute Filtering User Profile: Example, page 6](#)
- [debug radius Command: Example, page 7](#)

Attribute Filtering for Access Requests: Example

The following example shows that the attributes 30-31 that are defined in “all-attr” will be rejected in all outbound Access Request messages:

```
aaa group server radius ras
 server 172.19.192.238 auth-port 1745 acct-port 1746
 authorization request reject all-attr
!
.
.
.
radius-server attribute list all-attr
 attribute 30-31
!
.
.
.
```

Attribute Filtering User Profile: Example

The following is a sample user profile after attribute filtering has been configured for Access Requests:

```
cisco.com Password = "cisco"
Service-Type = Framed,
Framed-Protocol = PPP,
Cisco:Cisco-Avpair = :1:"rad-serv=172.19.192.87 key rad123",
Cisco:Cisco-Avpair = :1:"rad-serv-filter=authorization request reject range1",
Cisco:Cisco-Avpair = :1:"rad-serv-filter=accounting request reject range1",
Cisco:Cisco-Avpair = "ppp-authen-type=chap"
Cisco:Cisco-Avpair = "ppp-authen-list=group 1",
Cisco:Cisco-Avpair = "ppp-author-list=group 1",
Cisco:Cisco-Avpair = "ppp-acct-list=start-stop group 1",
Cisco:Cisco-Avpair = "vpdn:tunnel-id=B53",
Cisco:Cisco-Avpair = "vpdn:tunnel-type=l2tp",
Cisco:Cisco-Avpair = "vpdn:ip-addresses=10.0.58.35",
Cisco:Cisco-Avpair = "vpdn:l2tp-tunnel-password=cisco"

user2@cisco.com
Service-Type = Outbound,
Cisco:Cisco-Avpair = "vpdn:tunnel-id=B53",
Cisco:Cisco-Avpair = "vpdn:tunnel-type=l2tp",
Cisco:Cisco-Avpair = "vpdn:ip-addresses=10.0.58.35",
Cisco:Cisco-Avpair = "vpdn:l2tp-tunnel-password=cisco"
```


When a session for user2@cisco.com “comes up” at the Layer 2 Tunneling Protocol (L2TP) Network Server (LNS)—as is shown above—because the **aaa authorization template** command has been configured, a RADIUS request is sent to the server for Cisco.com. The server then sends an Access Accept message if authentication is successful, along with the VSAs that are configured as part of the Cisco.com profile. If filters are configured as part of the Cisco.com profile, these filters will be parsed and applied to the RADIUS requests for user2@cisco.com.

In the above profile example, filter range1 has been applied to the authorization and accounting requests.

debug radius Command: Example

If the attribute you are trying to filter is rejected, you will see an **debug radius** output statement similar to the following:

```
RADIUS: attribute 31 rejected
```

If you try to filter an attribute that cannot be filtered, you will see an output statement similar to the following:

```
RADIUS: attribute 1 cannot be rejected
```

Additional References

The following sections provide references related to Attribute Filtering for Access Requests.

Related Documents

Related Topic	Document Title
Configuring RADIUS	“Configuring RADIUS” chapter of the <i>Cisco IOS Security Configuration Guide</i>
Security commands	Cisco IOS Security Command Reference
RADIUS attribute lists	RADIUS Attribute Screening

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **authorization (server-group)**

Feature Information for Attribute Screening for Access Requests

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Attribute Screening for Access Requests

Feature Name	Releases	Feature Information
Attribute Screening for Access Requests	12.3(3)B 12.3(7)T 12.2(28)SB 12.2(33)SRC Cisco IOS XE Release 2.1	<p>The Attribute Screening for Access Requests feature allows a network access server (NAS) to be configured to filter attributes in outbound Access Requests to the RADIUS server for purposes of authentication or authorization.</p> <p>In 12.3(3)B, this feature was introduced.</p> <p>This feature was integrated into Cisco IOS Release 12.3(7)T</p> <p>This feature was integrated into Cisco IOS Release 12.2(28)SB.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRC.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>The following commands were introduced or modified by this feature: authorization (server-group).</p>

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2003–2004, 2006–2007 Cisco Systems, Inc. All rights reserved.



Enable Multilink PPP via RADIUS for Preauthentication User

Feature History

Release	Modification
12.2(11)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

This feature module describes the Enable Multilink PPP via RADIUS for Preauthentication User feature in Cisco IOS Release 12.2(11)T. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 3](#)
- [Supported Standards, MIBs, and RFCs, page 4](#)
- [Prerequisites, page 4](#)
- [Configuration Tasks, page 4](#)
- [Configuration Examples, page 5](#)
- [Command Reference, page 6](#)
- [Glossary, page 7](#)

Feature Overview

The Enable Multilink PPP via RADIUS for Preauthentication User feature allows you to selectively enable and disable Multilink PPP (MLP) negotiation for different users via RADIUS vendor-specific attribute (VSA) preauth:ppp-multilink=1.



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

You can enable MLP by configuring the **ppp multilink** command on an interface, but then this command enables MLP negotiation for all connections and users on that interface; that is, you cannot selectively enable or disable MLP negotiation for specific connections and users on an interface.

**Note**

To enable this feature, the **ppp multilink** command should not be configured on the interface; this command will disable MLP by default. If the **ppp multilink** command is already configured on the interface, the attribute “preauth:ppp-multilink=1” will not override this command.

How MLP via RADIUS Works

Because MLP parameters are negotiated at the time of link control protocol (LCP) negotiation, RADIUS VSA `preauth:ppp-multilink=1` should only be a part of preauthentication user authorization. You should add this VSA to the preauthentication profile of the user to enable MLP. Thus, MLP will be enabled only for preauthentication users whose profiles contain this VSA; MLP will be disabled for all other users. If the MLP VSA is received during PPP user authorization (as opposed to preauthentication user authorization), it will be too late to negotiate MLP, and MLP will not be enabled.

When this VSA is received during preauthentication user authorization, MLP negotiation for the user is enabled. MLP is enabled when the VSA value is 1. All attribute values other than 1 are ignored.

Roles of the L2TP Access Server and L2TP Network Server

With this feature, you do not need to configure MLP on the interface of the L2TP access server (LAC); during preauthentication user authorization, the LAC will selectively choose to enable MLP for preauthentication users who receive `preauth:ppp-multilink=1`. On the L2TP network server (LNS), you can control the maximum number of links allowed in the multilink bundle by sending RADIUS VSA `multilink:max-links=n` during PPP user authorization.

New Vendor-Specific Attributes

This feature introduces the following new VSAs:

- Cisco-AVpair = `preauth:ppp-multilink=1`
Turns on MLP on the interface and is applied to the preauthentication profile.
- Cisco-AVpair = `multilink:max-links=n`
Restricts the maximum number of links that a user can have in a multilink bundle and is used with the `service=ppp` attribute. The range of “n” is from 1 to 255.
- Cisco-AVpair = `multilink:min-links=1`
Sets the minimum number of links for MLP. The range of “n” is from 0 to 255.
- Cisco-AVpair = `multilink:load-threshold=n`
Sets the load threshold for the caller for which additional links are added or deleted from the multilink bundle. If the load exceeds the specified value, links are added; if the load drops below the specified value, links are deleted. This attribute is used with the `service=ppp` attribute. The range of “n” is from 1 to 255.

**Note**

RADIUS VSAs multilink:max-links, multilink:min-links, and multilink:load-threshold serve the same purpose as TACACS+ per-user attributes, max-links, min-links, and load-threshold respectively.

Benefits

Selective Multilink PPP Configuration

MLP negotiation can be selectively enabled and disabled for different users by applying RADIUS VSA preauth:ppp-multilink=1 to the preauthentication profile.

Related Documents

- “RADIUS Attributes” appendix in the *Cisco IOS Security Configuration Guide*, Release 12.2
- “TACACS+ Attribute-Value Pairs” appendix in the *Cisco IOS Security Configuration Guide*, Release 12.2
- “Configuring RADIUS” chapter in the *Cisco IOS Security Configuration Guide*, Release 12.2
- “PPP Configuration” chapter in the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2
- *Cisco IOS Dial Technologies Command Reference*, Release 12.2

Supported Platforms

- Cisco AS5300 series
- Cisco AS5350 series
- Cisco AS5400 series
- Cisco AS5800 series
- Cisco AS5850 series

Determining Platform Support Through Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Feature Navigator. Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

Before enabling MLP via RADIUS VSA preauth:ppp-multilink=1, you should perform the following tasks:

- Enable the network access server (NAS) to recognize and use VSAs as defined by RADIUS IETF attribute 26 by using the **radius-server vsa send** command.

For more information about using VSAs, refer to the section “Configuring Router to Use Vendor-Specific RADIUS Attributes” of the chapter “Configuring RADIUS” in the *Cisco IOS Security Configuration Guide*, Release 12.2.

- Enable preauthentication.

For information about configuring preauthentication, refer to the section “Configuring AAA Preauthentication” of the chapter “Configuring RADIUS” in the *Cisco IOS Security Configuration Guide*, Release 12.2.

Configuration Tasks

None

Verifying MLP Negotiation via RADIUS in Preauthentication

To display bundle information for the MLP bundles, use the **show ppp multilink** EXEC command.

```
Router# show ppp multilink
```

```
Virtual-Access1, bundle name is mlpuser
Bundle up for 00:00:15
Dialer interface is Serial0:23
0 lost fragments, 0 reordered, 0 unassigned
0 discarded, 0 lost received, 1/255 load
0x0 received sequence, 0x0 sent sequence
Member links: 1 (max 7, min 1)
Serial0:22, since 00:00:15, no frags rcvd
```


Table 15 describes the significant fields shown when MLP is enabled.

Table 15 *show ppp multilink Field Descriptions*

Field	Description
Virtual-Access1	Multilink bundle virtual interface.
Bundle	Configured name of the multilink bundle.
Dialer Interface is Serial0:23	Name of the interface that dials the calls.
1/255 load	Load on the link in the range 1/255 to 255/255. (255/255 is a 100% load.)
Member links: 1	Number of child interfaces.

Configuration Examples

This section provides dialin VPDN configurations using Cisco VSA ppp-multilink examples:

- [LAC for MLP Configuration Example](#)
- [LAC RADIUS Profile for Preauthentication Example](#)
- [LNS for MLP Configuration Example](#)
- [LNS RADIUS Profile Example](#)

LAC for MLP Configuration Example

The following example is a sample configuration that can be used to configure a LAC for MLP via RADIUS:

```
! Enable preauthentication
aaa preauth
  group radius
  dnis required

!Enable VPDN
vpdn enable
!
vpdn-group 1
  request-dialin
  protocol l2tp
  dnis 56118
  initiate-to ip 10.0.1.22
  local name lac-router

! Don't need to configure multilink on the interface
! Multilink will be enabled by "ppp-multilink" attribute
interface Serial0:23
  ip address 15.0.1.7 255.0.0.0
  encapsulation ppp
  dialer-group 1
  isdn switch-type primary-5ess
  isdn calling-number 56118
  peer default ip address pool pool1
  no cdp enable
  ppp authentication chap
```

LAC RADIUS Profile for Preauthentication Example

The following example shows a LAC RADIUS profile for a preauthentication user who has applied the `preauth:ppp-multilink=1` VSA:

```
56118 Password = "cisco"
      Service-Type = Outbound,
      Framed-Protocol = PPP,
      Framed-MTU = 1500,
      Cisco-Avpair = "preauth:auth-required=1",
      Cisco-Avpair = "preauth:auth-type=chap",
      Cisco-Avpair = "preauth:username=dnis:56118",
      Cisco-Avpair = "preauth:ppp-multilink=1"
```

LNS for MLP Configuration Example

The following example is a sample configuration that can be used to configure a LNS to limit the number of links in a MLP bundle:

```
! Enable VPDN
vpdn enable
!
vpdn-group 1
 accept-dialin
 protocol any
 virtual-template 1
 terminate-from hostname lac-router
 local name lns-router
!
! Configure multilink on interface
interface Virtual-Template 1
 ip unnumbered Ethernet 0/0
 ppp authentication chap
 ppp multilink
```

LNS RADIUS Profile Example

The following example shows a LNS RADIUS profile for specifying the maximum number of links in a multilink bundle. The following multilink VSAs should be specified during PPP user authorization.

```
mascot password = "cisco"
      Service-Type = Framed,
      Framed-Protocol = PPP,
      Cisco-Avpair = "multilink:max-links=7"
      Cisco-Avpair = "multilink:min-links=1"
      Cisco-Avpair = "multilink:load-threshold=128"
```

Command Reference

This feature uses no new or modified commands. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

Glossary

AAA—authentication, authorization, and accounting. Suite of network security services that provide the primary framework through which access control can be set up on your Cisco router or access server.

attribute—RADIUS Internet Engineering Task Force (IETF) attributes are the original set of 255 standard attributes that are used to communicate AAA information between a client and a server. Because IETF attributes are standard, the attribute data is predefined and well known; thus all clients and servers that exchange AAA information via IETF attributes must agree on attribute data such as the exact meaning of the attributes and the general bounds of the values for each attribute.

L2F—Layer 2 Forwarding. Protocol that supports the creation of secure virtual private dial-up networks over the Internet.

L2TP—Layer 2 Tunnel Protocol. A Layer 2 tunneling protocol that enables an ISP or other access service to create a virtual tunnel to link customer remote sites or remote users with corporate home networks. In particular, a network access server (NAS) at the ISP point of presence (POP) exchanges PPP messages with the remote users and communicates by L2F or L2TP requests and responses with the customer tunnel server to set up tunnels.

LAC—L2TP access concentrator. A network access server (NAS) to which the client directly connects and through which PPP frames are tunneled to the L2TP network server (LNS). The LAC need only implement the media over which L2TP is to operate to pass traffic to one or more LNSs. The LAC may tunnel any protocol carried within PPP. The LAC initiates incoming calls and receives outgoing calls. A LAC is analogous to an L2F network access server.

LNS—L2TP network server. A termination point for L2TP tunnels, and an access point where PPP frames are processed and passed to higher-layer protocols. An LNS can operate on any platform that terminates PPP. The LNS handles the server side of the L2TP protocol. L2TP relies only on the single medium over which L2TP tunnels arrive. The LNS initiates outgoing calls and receives incoming calls. An LNS is analogous to a home gateway in L2F technology.

MLP—Multilink PPP. MLP allows packets to be fragmented and the fragments to be sent at the same time over multiple point-to-point links to the same remote address. The multiple links come up in response to a defined dialer load threshold. The load can be calculated on inbound traffic, outbound traffic, or on either, as needed for the traffic between the specific sites. MLP provides bandwidth on demand and reduces transmission latency across WAN links.

MLP is designed to work over synchronous and asynchronous serial and BRI and PRI types of single or multiple interfaces that have been configured to support both dial-on-demand rotary groups and PPP encapsulation.

RADIUS—Remote Authentication Dial-In User Service. RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

VSA—Vendor-Specific Attribute. VSAs derived from one IETF attribute—vendor-specific (attribute 26). Attribute 26 allows a vendor to create and implement an additional 255 attributes. That is, a vendor can create an attribute that does not match the data of any IETF attribute and encapsulate it behind attribute 26: essentially, Vendor-Specific = “protocol:attribute=value.”

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0708R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Enhanced Test Command

First Published: August 9, 2001

Last Updated: December 17, 2007

The Enhanced Test Command feature allows a named user profile to be created with calling line ID (CLID) or dialed number identification service (DNIS) attribute values. The CLID or DNIS attribute values can be associated with the RADIUS record that is sent with the user profile so that the RADIUS server can access CLID or DNIS attribute information for all incoming calls.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Enhanced Test Command”](#) section on page 6.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Restrictions for the Enhanced Test Command, page 2](#)
- [How to Configure the Enhanced Test Command, page 2](#)
- [Configuration Example for Enhanced Test Command, page 3](#)
- [Additional References, page 4](#)
- [Command Reference, page 5](#)
- [Feature Information for Enhanced Test Command, page 6](#)
- [Glossary, page 7](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2001, 2006–2007 Cisco Systems, Inc. All rights reserved.

Restrictions for the Enhanced Test Command

The **test aaa group** command does not work with TACACS+.

How to Configure the Enhanced Test Command

The following sections describe how to configure the Enhanced Test Command feature:

- [Configuring a User Profile and Associating it with the RADIUS Record](#)
- [Verifying the Enhanced Test Command Configuration](#)

Configuring a User Profile and Associating it with the RADIUS Record

This section describes how to create a named user profile with CLID or DNIS attribute values and associate it with the RADIUS record.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa user profile** *profile-name*
4. **aaa attribute** {dnis | clid} *attribute-value*
5. **exit**
6. **test aaa group** {group-name | radius} *username password new-code* [profile *profile-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa user profile <i>profile-name</i> Example: Router(config)# aaa user profile profilename1	Creates a user profile.
Step 4	aaa attribute {dnis clid} Example: Router# configure terminal	Adds DNIS or CLID attribute values to the user profile and enters AAA-user configuration mode.

	Command or Action	Purpose
Step 5	exit	Exit Global Configuration mode.
Step 6	Router# test aaa group {group-name radius } username password new-code [profile profile-name] Example: Router# test aaa group radius secret new-code profile profilename1	Associates a DNIS or CLID named user profile with the record sent to the RADIUS server. Note The <i>profile-name</i> must match the <i>profile-name</i> specified in the aaa user profile command.

Verifying the Enhanced Test Command Configuration

To verify the Enhanced Test Command configuration, use the following commands in privileged EXEC mode:

Command	Purpose
Router# debug radius	Displays information associated with RADIUS.
Router# more system:running-config	Displays the contents of the current running configuration file. (Note that the more system:running-config command has replaced the show running-config command.)

Configuration Example for Enhanced Test Command

This section provides the following configuration example:

- [User Profile Associated With a test aaa group command Example](#)

User Profile Associated With a test aaa group command Example

The following example shows how to configure the dnis = dnisvalue user profile “prfl1” and associate it with a **test aaa group** command. In this example, the **debug radius** command has been enabled and the output follows the configuration.

```

aaa user profile prfl1
  aaa attribute dnis
  aaa attribute dnis dnisvalue
  no aaa attribute clid
! Attribute not found.
  aaa attribute clid clidvalue
  no aaa attribute clid
exit
!
! Associate the dnis user profile with the test aaa group command.
test aaa group radius user1 pass new-code profile prfl1
!
!
! debug radius output, which shows that the dnis value has been passed to the radius
! server.
```

```

*Dec 31 16:35:48: RADIUS: Sending packet for Unique id = 0
*Dec 31 16:35:48: RADIUS: Initial Transmit unknown id 8 172.22.71.21:1645,
Access-Request, len 68
*Dec 31 16:35:48: RADIUS: code=Access-Request id=08 len=0068
    authenticator=1E CA 13 F2 E2 81 57 4C - 02 EA AF 9D 30 D9 97 90
    T=User-Password[2]                                L=12 V=*
    T=User-Name[1]                                     L=07 V="test"
    T=Called-Station-Id[30]                             L=0B V="dnisvalue"
    T=Service-Type[6]                                L=06 V=Login [1]
    T=NAS-IP-Address[4]                              L=06 V=10.0.1.81
*Dec 31 16:35:48: RADIUS: Received from id 8 172.22.71.21:1645, Access-Accept, len 38
*Dec 31 16:35:48: RADIUS: code=Access-Accept id=08 len=0038

```

Additional References

The following sections provide references related to Enhanced Test Command.

Related Documents

Related Topic	Document Title
Security Commands	Cisco IOS Security Command Reference

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **aaa attribute**
- **aaa user profile**
- **test aaa group**

Feature Information for Enhanced Test Command

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Enhanced Test Command

Feature Name	Releases	Feature Information
Enhanced Test Command	12.2(4)T 12.2(28)SB 12.2(33)SRC Cisco IOS XE Release 2.1	<p>The Enhanced Test Command feature allows a named user profile to be created with calling line ID (CLID) or Dialed Number Identification Service (DNIS) attribute values. The CLID or DNIS attribute values can be associated with the RADIUS record that is sent with the user profile so that the RADIUS server can access CLID or DNIS attribute information for all incoming calls.</p> <p>This feature was introduced in Cisco IOS Release 12.2(4)T.</p> <p>This feature was integrated into Cisco IOS Release 12.2(28)SB.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRC.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>The following commands were introduced or modified by this feature: aaa attribute, aaa user profile, test aaa group</p>

Glossary

attribute—RADIUS Internet Engineering Task Force (IETF) attributes are the original set of 255 standard attributes that are used to communicate AAA information between a client and a server. Because IETF attributes are standard, the attribute data is predefined and well known; thus all clients and servers who exchange AAA information via IETF attributes must agree on attribute data such as the exact meaning of the attributes and the general bounds of the values for each attribute.

CLID—calling line ID. CLID provides the number from which a call originates.

DNIS—dialed number identification service. DNIS provides the number that is dialed.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2001, 2006–2007 Cisco Systems, Inc. All rights reserved.



Framed-Route in RADIUS Accounting

First Published: November 3, 2003

Last Updated: December 17, 2007

The Framed-Route in RADIUS Accounting feature provides for the presence of Framed-Route (RADIUS attribute 22) information in RADIUS Accounting-Request accounting records. The Framed-Route information is returned to the RADIUS server in the Accounting-Request packets. The Framed-Route information can be used to verify that a per-user route or routes have been applied for a particular static IP customer on the network access server (NAS).

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Framed-Route in RADIUS Accounting](#)” section on [page 7](#).

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Framed-Route in RADIUS Accounting, page 2](#)
- [Information About Framed-Route in RADIUS Accounting, page 2](#)
- [How to Monitor Framed-Route in RADIUS Accounting, page 3](#)
- [Additional References, page 5](#)
- [Command Reference, page 6](#)
- [Feature Information for Framed-Route in RADIUS Accounting, page 7](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for Framed-Route in RADIUS Accounting

Be familiar with configuring authentication, authorization, and accounting (AAA), RADIUS servers, and RADIUS attribute screening.

Information About Framed-Route in RADIUS Accounting

This section includes the following concepts:

- [Framed-Route, Attribute 22, page 2](#)
- [Framed-Route in RADIUS Accounting Packets, page 2](#)

Framed-Route, Attribute 22

Framed-Route, attribute 22 as defined in Internet Engineering Task Force (IETF) standard RFC 2865, provides for routing information to be configured for the user on the NAS. The Framed-Route attribute information is usually sent from the RADIUS server to the NAS in Access-Accept packets. The attribute can appear multiple times.

Framed-Route in RADIUS Accounting Packets

The Framed-Route attribute information in RADIUS accounting packets shows per-user routes that have been applied for a particular static IP customer on the NAS. The Framed-Route attribute information is currently sent in Access-Accept packets. Effective with Cisco IOS Release 12.3(4)T, the Framed-Route attribute information is also sent in Accounting-Request packets if it was provided in the Access-Accept packets and was applied successfully. Zero or more instances of the Framed-Route attribute may be present in the Accounting-Request packets.

**Note**

If there is more than one Framed-Route attribute in an Access-Accept packet, there can also be more than one Framed-Route attribute in the Accounting-Request packet.

The Framed-Route information is returned in Stop and Interim accounting records and in Start accounting records when accounting Delay-Start is configured.

No configuration is required to have the Frame-Route attribute information returned in the RADIUS accounting packets.

How to Monitor Framed-Route in RADIUS Accounting

Use the **debug radius** command to monitor whether Framed-Route (attribute 22) information is being sent in RADIUS Accounting-Request packets.

Examples

This section provides the following example:

- [debug radius Command Output: Example, page 3](#)

debug radius Command Output: Example

In the following example, the **debug radius** command is used to verify that Framed-Route (attribute 22) information is being sent in the Accounting-Request packets (see the line 00:06:23: RADIUS: Framed-Route [22] 26 "10.80.0.1 255.255.255.255 10.60.0.1 100").

Router# **debug radius**

```
00:06:23: RADIUS: Send to unknown id 0 10.1.0.2:1645, Access-Request, len 126
00:06:23: RADIUS: authenticator 40 28 A8 BC 76 D4 AA 88 - 5A E9 C5 55 0E 50 84 37
00:06:23: RADIUS: Framed-Protocol [7] 6 PPP [1]
00:06:23: RADIUS: User-Name [1] 14 "nari@trw1001"
00:06:23: RADIUS: CHAP-Password [3] 19 *
00:06:23: RADIUS: NAS-Port [5] 6 1
00:06:23: RADIUS: Vendor, Cisco [26] 33
00:06:23: RADIUS: Cisco AVpair [1] 27 "interface=Virtual-Access1"
00:06:23: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
00:06:23: RADIUS: Service-Type [6] 6 Framed [2]
00:06:23: RADIUS: NAS-IP-Address [4] 6 12.1.0.1
00:06:23: RADIUS: Acct-Session-Id [44] 10 "00000002"
00:06:23: RADIUS: Received from id 0 10.1.0.2:1645, Access-Accept, len 103
00:06:23: RADIUS: authenticator 5D 2D 9F 25 11 15 45 B2 - 54 BB 7F EB CE 79 20 3B
00:06:23: RADIUS: Vendor, Cisco [26] 33
00:06:23: RADIUS: Cisco AVpair [1] 27 "interface=Virtual-Access1"
00:06:23: RADIUS: Service-Type [6] 6 Framed [2]
00:06:23: RADIUS: Framed-Protocol [7] 6 PPP [1]
00:06:23: RADIUS: Framed-IP-Netmask [9] 6 255.255.255.255
00:06:23: RADIUS: Framed-IP-Address [8] 6 10.60.0.1
00:06:23: RADIUS: Framed-Route [22] 26 "10.80.0.1 255.255.255.255 10.60.0.1 100"
<=====
00:06:23: RADIUS: Received from id 2
00:06:24: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up
00:06:25: AAA/AUTHOR: Processing PerUser AV route
00:06:25: Vi1 AAA/PERUSER/ROUTE: route string: IP route 10.80.0.1 255.255.255.255 10.60.0.1 100

00:06:25: RADIUS/ENCODE(00000002): Unsupported AAA attribute timezone
00:06:25: RADIUS(00000002): sending
00:06:25: RADIUS: Send to unknown id 1 10.1.0.2:1646, Accounting-Request, len 278
00:06:25: RADIUS: authenticator E0 CC 99 EB 49 18 B9 78 - 4A 09 60 0F 4E 92 24 C6
00:06:25: RADIUS: Acct-Session-Id [44] 10 "00000002"
00:06:25: RADIUS: Tunnel-Server-Endpoi[67] 12 00:"10.1.1.1"
00:06:25: RADIUS: Tunnel-Client-Endpoi[66] 12 00:"10.1.1.2"
00:06:25: RADIUS: Tunnel-Assignment-Id[82] 15 00:"from_isdn101"
```

```

00:06:25: RADIUS: Tunnel-Type [64] 6 00:L2TP [3]
00:06:25: RADIUS: Acct-Tunnel-Connecti[68] 12 "2056100083"
00:06:25: RADIUS: Tunnel-Client-Auth-I[90] 10 00:"isdn101"
00:06:25: RADIUS: Tunnel-Server-Auth-I[91] 6 00:"lns"
00:06:25: RADIUS: Framed-Protocol [7] 6 PPP [1]
00:06:25: RADIUS: Framed-Route [22] 39 "10.80.0.1 255.255.255.255 10.60.0.1 100"
<=====
00:06:25: RADIUS: Framed-IP-Address [8] 6 10.60.0.1
00:06:25: RADIUS: Vendor, Cisco [26] 35
00:06:25: RADIUS: Cisco AVpair [1] 29 "connect-progress=LAN Ses Up"
00:06:25: RADIUS: Authentic [45] 6 RADIUS [1]
00:06:25: RADIUS: User-Name [1] 14 "username1@example.com"
00:06:25: RADIUS: Acct-Status-Type [40] 6 Start [1]
00:06:25: RADIUS: NAS-Port [5] 6 1
00:06:25: RADIUS: Vendor, Cisco [26] 33
00:06:25: RADIUS: Cisco AVpair [1] 27 "interface=Virtual-Access1"
00:06:25: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
00:06:25: RADIUS: Service-Type [6] 6 Framed [2]
00:06:25: RADIUS: NAS-IP-Address [4] 6 10.1.0.1
00:06:25: RADIUS: Acct-Delay-Time [41] 6 0

```


Additional References

The following sections provide references related to the Framed-Route in RADIUS Accounting feature.

Related Documents

Related Topic	Document Title
RADIUS	<i>Cisco IOS Security Configuration Guide</i> , Release 12.2. Refer to “RADIUS Attributes” in the Appendixes.

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2865	<i>Remote Authentication Dial In User Service (RADIUS)</i>
RFC 3575	<i>IANA Considerations for RADIUS (Remote Authentication Dial In User Service)</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Command Reference

No commands are introduced or modified in the feature in this module. For information about commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

Feature Information for Framed-Route in RADIUS Accounting

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Framed-Route in RADIUS Accounting

Feature Name	Releases	Feature Information
Framed-Route in RADIUS Accounting	12.3(4)T 12.2(28)SB 12.2(33)SRC	<p>The Framed-Route in RADIUS Accounting feature provides for the presence of Framed-Route (RADIUS attribute 22) information in RADIUS Accounting-Request accounting records.</p> <p>This feature was introduced in Cisco IOS Release 12.3(4)T.</p> <p>This feature was integrated into Cisco IOS Release 12.2(28)SB.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRC.</p>

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2003, 2006, 2007 Cisco Systems, Inc. All rights reserved.



Offload Server Accounting Enhancement

First Published: 12.2(4)T

Last Updated: December 31, 2007

The Offload Server Accounting Enhancement feature allows users to maintain authentication and accounting information between their network access servers (NASs) and the offload server.

History for the Offload Server Accounting Enhancement Feature

Release	Modification
12.2(4)T	This feature was introduced.
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This feature was integrated into Cisco IOS Release 12.2(33)SRC.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

For the latest feature information and caveats, see the release notes for your Cisco IOS software release.

Contents

- [Feature Overview, page 2](#)
- [Prerequisites, page 2](#)
- [Configuration Tasks, page 3](#)
- [Configuration Examples, page 4](#)
- [Additional References, page 5](#)
- [Command Reference, page 6](#)
- [Glossary, page 6](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Feature Overview

The Offload Server Accounting Enhancement feature allows users to configure their network access servers (NAS) to synchronize authentication and accounting information—NAS-IP-Address (attribute 4) and Class (attribute 25)—with the offload server.

An offload server interacts with a NAS via Virtual Private Network (VPN) to perform required Point-to-Point Protocol (PPP) negotiation for calls. The NAS performs call preauthentication, whereas the offload server performs user authentication. This feature allows the authentication and accounting data of the NAS to synchronize with the offload server as follows:

- During preauthentication, the NAS generates a unique session-id, adding the Acct-Session-Id (attribute 44) before the existing session-id (NAS-IP-Address), and retrieves a Class attribute. The new session-id is sent in preauthentication requests and resource accounting requests; the Class attribute is sent in resource accounting requests.

**Note**

Unique session-ids are needed when multiple NASs are being processed by one offload server.

- The NAS-IP-Address, the Acct-Session-Id, and the Class attribute are transmitted to the offload server via Layer 2 Forwarding (L2F) options.
- The offload server will include the new, unique session-id in user access requests and user session accounting requests. The Class attribute that was passed from the NAS will be included in the user access request, but a new Class attribute will be received in the user access reply; this new Class attribute should be included in user session accounting requests.

Benefits

The Offload Server Accounting Enhancement feature allows users to maintain authentication and accounting information between their NAS and offload server.

Although NASs can already synchronize information with an offload server, this feature extends the functionality to include a unique session-id, adding the Acct-Session-Id (attribute 44) before the existing session-id (NAS-IP-Address), and Class (attribute 25) information collected by the NASs.

Prerequisites

Before configuring the Offload Server Accounting Enhancement feature, you must perform the following tasks:

- Enable AAA. (For more information, refer to chapter “Configuring Authentication” of the *Cisco IOS Security Configuration Guide*)
- Enable VPN. (For more information, refer to the chapter “Configuring Virtual Private Networks” of the *Cisco IOS Dial Technologies Configuration Guide*)

Configuration Tasks

See the following sections for configuration tasks for the Offload Server Accounting Enhancement feature. Each task in the list is identified as either required or optional.

- [Configuring Unique Session IDs, page 3](#)(required)
- [Configuring Offload Server to Synchronize with NAS Clients, page 3](#)(required)
- [Verifying Offload Server Accounting, page 4](#)(optional)

Configuring Unique Session IDs

To maintain unique session IDs among NASs, use the following global configuration command. When multiple NASs are being processed by one offload server, this feature must be enabled by all NASs and by the offload server to ensure a common and unique session-id.

Command	Purpose
Router(config)# radius-server attribute 44 extend-with-addr	Adds the accounting IP address in front of the existing AAA session ID. Note The unique session-id is different from other NAS session-ids because it adds the Acct-Session-Id (attribute 44) before the existing session-id (NAS-IP-Address).

Configuring Offload Server to Synchronize with NAS Clients

To configure the offload server to synchronize accounting session information with the NAS clients, use the following global configuration command:

Command	Purpose
Router(config)# radius-server attribute 44 sync-with-client	Configures the offload server to synchronize accounting session information with the NAS clients.

Verifying Offload Server Accounting

To verify whether the NAS has synchronized authentication and accounting data with the offload server, use the following commands in privileged EXEC mode:

Command	Purpose
Router# more system:running-config	Displays the contents of the current running configuration file. (Note that the more system:running-config command has replaced the show running-config command.)
Router(config)# debug radius	Displays information associated with RADIUS. The output of this command shows whether attribute 44 is being sent in access requests. The output, however, does not show the entire value for attribute 44. To view the entire value for attribute 44, refer to your RADIUS server log.

Configuration Examples

This section provides the following configuration examples:

- [Unique Session ID Configuration Example, page 4](#)
- [Offload Server Synchronization with NAS Clients Example, page 4](#)

Unique Session ID Configuration Example

The following example shows how to configure unique session IDs among NASs:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 include-in-access-req
radius-server attribute 44 extend-with-addr
```

Offload Server Synchronization with NAS Clients Example

The following example shows how to configure the offload server to synchronize accounting session information with NAS clients:

```
radius-server attribute 44 sync-with-client
```


Additional References

The following sections provide references related to Offload Server Accounting Enhancement.

Related Documents¹

Related Topic	Document Title
Configuring Virtual Private Networks	“Configuring Virtual Private Networks” chapter in the <i>Cisco IOS Dial Technologies Configuration Guide</i>
Security Configuration Guide	<i>Cisco IOS Security Configuration Guide</i>

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

1.

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **radius-server attribute 44 extend-with-addr**
- **radius-server attribute 44 sync-with-client**

Glossary

AAA—authentication, authorization, and accounting. Suite of network security services that provide the primary framework through which access control can be set up on your Cisco router or access server.

Acct-Session-ID (attribute 44)—A unique accounting identifier that makes it easy to match start and stop records in a log file. Acct-Session ID numbers restart at 1 each time the router is power-cycled or the software is reloaded.

Class (attribute 25)—An accounting attribute. Arbitrary value that the network access server includes in all accounting packets for this user if the attribute is supplied by the RADIUS server.

L2F—Layer 2 Forwarding. A Layer 2 tunneling protocol that enables an ISP or other access service to create a virtual tunnel to link customer remote sites or remote users with corporate home networks. In particular, a network access server (NAS) at the ISP point of presence (POP) exchanges PPP messages with the remote users and communicates by L2F or L2TP requests and responses with the customer tunnel server to set up tunnels.

NAS—network access server. A Cisco platform (or collection of platforms, such as an AccessPath system) that interfaces between the packet world (for example, the Internet) and the circuit world (for example, the public switched telephone network).

NAS-IP Address (attribute 4)—Specifies the IP address of the network access server that is requesting authentication. The default value is 0.0.0.0/0.

PPP—Point-to-Point Protocol. Successor to SLIP that provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. Whereas SLIP was designed to work with IP, PPP was designed to work with several network layer protocols, such as IP, IPX, and ARA. PPP also has built-in security mechanisms, such as CHAP and PAP. PPP relies on two protocols: LCP and NCP.

RADIUS—Remote Authentication Dial-In User Service. RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

VPN—A system that permits dial-in networks to exist remotely to home networks, while giving the appearance of being directly connected. VPNs use L2TP and L2F to terminate the Layer 2 and higher parts of the network connection at the LNS instead of the LAC.

**Note**

See [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Per VRF AAA

First Published: June 4, 2001

Last Updated: January 15, 2008

The Per VRF AAA feature allows authentication, authorization, and accounting (AAA) on the basis of Virtual Private Network (VPN) routing and forwarding (VRF) instances. For Cisco IOS Release 12.2(15)T or later releases, you can use a customer template, which may be stored either locally or remotely, and AAA services can be performed on the information that is stored in the customer template. This feature has also been referred to as the Dynamic Per VRF AAA feature

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Per VRF AAA” section on page 30](#).

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Per VRF AAA, page 2](#)
- [Restrictions for Per VRF AAA, page 2](#)
- [Information About Per VRF AAA, page 2](#)
- [How to Configure Per VRF AAA, page 6](#)
- [Configuration Examples for Per VRF AAA, page 18](#)
- [Additional References, page 28](#)
- [Command Reference, page 29](#)
- [Glossary, page 31](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2001-2008 Cisco Systems, Inc. All rights reserved.

Prerequisites for Per VRF AAA

Before configuring the Per VRF AAA feature, you must enable AAA. (For information on completing this task, refer to the AAA chapters of the “[Cisco IOS Security Configuration Guide](#)”, Release 12.4)

Restrictions for Per VRF AAA

- This feature is supported only for RADIUS servers.
- Operational parameters should be defined once per VRF rather than set per server group, because all functionalities must be consistent between the network access server (NAS) and the AAA servers.
- The ability to configure a customer template either locally or remotely is available only for Cisco IOS Release 12.2(15)T and later releases.

Information About Per VRF AAA

When you use the Per VRF AAA feature, AAA services can be based on VRF instances. This feature permits the Provider Edge (PE) or Virtual Home Gateway (VHG) to communicate directly with the customer’s RADIUS server, which is associated with the customer’s Virtual Private Network (VPN), without having to go through a RADIUS proxy. Thus, ISPs can scale their VPN offerings more efficiently because they no longer have to use RADIUS proxies and ISPs can also provide their customers with additional flexibility.

- [How Per VRF AAA Works, page 2](#)
- [Benefits, page 3](#)
- [AAA Accounting Records, page 3](#)
- [New Vendor-Specific Attributes, page 3](#)

How Per VRF AAA Works

To support AAA on a per customer basis, some AAA features must be made VRF aware. That is, ISPs must be able to define operational parameters—such as AAA server groups, method lists, system accounting, and protocol-specific parameters—and bind those parameters to a particular VRF instance. Defining and binding the operational parameters can be accomplished using one or more of the following methods:

- Virtual private dialup network (VPDN) virtual template or dialer interfaces that are configured for a specific customer
- Locally defined customer templates—Per VPN with customer definitions. The customer template is stored locally on the VHG. This method can be used to associate a remote user with a specific VPN based on the domain name or dialed number identification service (DNIS) and provide the VPN-specific configuration for virtual access interface and all operational parameters for the customer AAA server.

- Remotely defined customer templates—Per VPN with customer definitions that are stored on the service provider AAA server in a RADIUS profile. This method is used to associate a remote user with a specific VPN based on the domain name or DNIS and provide the VPN-specific configuration for the virtual access interface and all operational parameters for the AAA server of the customer.

**Note**

The ability to configure locally or remotely defined customer templates is available only with Cisco IOS Release 12.2(15)T and later releases.

Benefits

Configuration Support

ISPs can partition AAA services on a per VRF basis. Thus, ISPs can allow their customers to control some of their own AAA services.

Server Group List Extension

The list of servers in server groups is extended to include the definitions of private servers in addition to references to the hosts in the global configuration, allowing access to both customer servers and global service provider servers simultaneously.

AAA Accounting Records

The Cisco implementation of AAA accounting provides “start” and “stop” record support for calls that have passed user authentication. Start and stop records are necessary for users employing accounting records to manage and monitor their networks.

New Vendor-Specific Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (VSA) attribute 26. Attribute 26 encapsulates VSAs, thereby, allowing vendors to support their own extended attributes otherwise not suitable for general use.

The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. Cisco’s vendor-ID is 9, and the supported option has vendor-type 1, which is named “cisco-avpair.” The value is a string of the following format:

```
protocol : attribute sep value *
```

“Protocol” is a value of the Cisco “protocol” attribute for a particular type of authorization. “Attribute” and “value” are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification, and “sep” is “=” for mandatory attributes and “*” for optional attributes. This format allows the full set of features available for TACACS+ authorization to be used also for RADIUS.

[Table 1](#) summarizes the VSAs that are now supported with Per VRF AAA.

Table 1 VSAs supported with Per VRF AAA

VSA Name	Value Type	Description
Note Each VSA must have the prefix “template:” before the VSA name, unless a different prefix is explicitly stated.		
account-delay	string	This VSA must be “on.” The functionality of this VSA is equal to the aaa accounting delay-start command for the customer template.
account-send-stop	string	This VSA must be “on.” The functionality of this VSA is equal to the aaa accounting send stop-record authentication command with the failure keyword.
account-send-success-remote	string	This VSA must be “on.” The functionality of this VSA is equal to the aaa accounting send stop-record authentication command with the success keyword.
attr-44	string	This VSA must be “access-req.” The functionality of this VSA is equal to the radius-server attribute 44 include-in-access-req command.
ip-addr	string	This VSA specifies the IP address, followed by the mask that the router uses to indicate its own IP address and mask in negotiation with the client; for example, ip-addr=1.2.3.4 255.255.255.255
ip-unnumbered	string	This VSA specifies the name of an interface on the router. The functionality of this VSA is equal to the ip unnumbered command, which specifies an interface name such as “Loopback 0.”
ip-vrf	string	This VSA specifies which VRF will be used for the packets of the end user. This VRF name should match the name that is used on the router via the ip vrf forwarding command.
peer-ip-pool	string	This VSA specifies the name of an IP address pool from which an address will be allocated for the peer. This pool should be configured using the ip local pool command or should be automatically downloadable via RADIUS.
ppp-acct-list	string	<p>This VSA defines the accounting method list that is to be used for PPP sessions.</p> <p>The VSA syntax is as follows: “ppp-acct-list=[start-stop stop-only none] group X [group Y] [broadcast].” It is equal to the aaa accounting network mylist command functionality.</p> <p>The user must specify at least one of the following options: start-stop, stop-only, or none. If either start-stop or stop-only is specified, the user must specify at least one, but not more than four, group arguments. Each group name must consist of integers. The servers in the group should have already been identified in the access-accept via the VSA “rad-serv.” After each group has been specified, the user can specify the broadcast option</p>

VSA Name	Value Type	Description
ppp-authen-list	string	<p>This VSA defines which authentication method list is to be used for PPP sessions and, if more than one method is specified, in what order the methods should be used.</p> <p>The VSA syntax is as follows: “ppp-authen-list=[groupX local local-case none if-needed],” which is equal to the aaa authentication ppp mylist command functionality.</p> <p>The user must specify at least one, but no more than four, authentication methods. If a server group is specified, the group name must be an integer. The servers in the group should have already been identified in the access-accept via the VSA “rad-serv.”</p>
ppp-authen-type	string	<p>This VSA allows the end user to specify at least one of the following authentication types: pap, chap, eap, ms-chap, ms-chap-v2, any, or a combination of the available types that is separated by spaces.</p> <p>The end user will be permitted to log in using only the methods that are specified in this VSA.</p> <p>PPP will attempt these authentication methods in the order presented in the attribute.</p>
ppp-author-list	string	<p>This VSA defines the authorization method list that is to be used for PPP sessions. It indicates which methods will be used and in what order.</p> <p>The VSA syntax is as follows: “ppp-author-list=[groupX] [local] [if-authenticated] [none],” which is equal to the aaa authorization network mylist command functionality.</p> <p>The user must specify at least one, but no more than four, authorization methods. If a server group is specified, the group name must be an integer. The servers in the group should have already been identified in the access-accept via the VSA “rad-serv.”</p>
Note The RADIUS VSAs—rad-serv, rad-server-filter, rad-serv-source-if, and rad-serv-vrf—must have the prefix “aaa:” before the VSA name.		
rad-serv	string	<p>This VSA indicates the IP address, key, timeout, and retransmit number of a server, as well as the group of the server.</p> <p>The VSA syntax is as follows: “rad-serv=a.b.c.d [key SomeKey] [auth-port X] [acct-port Y] [retransmit V] [timeout W].” Other than the IP address, all parameters are optional and can be issued in any order. If the optional parameters are not specified, their default values will be used.</p> <p>The key cannot contain any spaces; for “retransmit V,” “V” can range from 1-100; for “timeout W,” the “W” can range from 1-1000.</p>

VSA Name	Value Type	Description
rad-serv-filter	string	The VSA syntax is as follows: “rad-serv-filter=authorization accounting-request reply-accept reject-filtername.” The filtername must be defined via the radius-server attribute list filtername command.
rad-serv-source-if	string	This VSA specifies the name of the interface that is used for transmitting RADIUS packets. The specified interface must match the interface configured on the router.
rad-serv-vrf	string	This VSA specifies the name of the VRF that is used for transmitting RADIUS packets. The VRF name should match the name that was specified via the ip vrf forwarding command.

How to Configure Per VRF AAA

The following sections contain procedures for possible deployment scenarios for using the Per VRF AAA feature.

- [Configuring Per VRF AAA, page 7](#) (required)
- [Configuring Per VRF AAA Using Local Customer Templates, page 12](#) (optional)
- [Configuring Per VRF AAA Using Remote Customer Templates, page 15](#) (optional)
- [Verifying VRF Routing Configurations, page 17](#) (optional)
- [Troubleshooting Per VRF AAA Configurations, page 18](#) (optional)

Configuring Per VRF AAA

This section contains the following procedures.

- [Configuring AAA, page 7](#)
- [Configuring Server Groups, page 7](#)
- [Configuring Authentication, Authorization, and Accounting for Per VRF AAA, page 8](#)
- [Configuring RADIUS-Specific Commands for Per VRF AAA, page 10](#)
- [Configuring Interface-Specific Commands for Per VRF AAA, page 11](#)

Configuring AAA

To enable AAA you need to complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Router(config)# aaa new-model	Enables AAA globally.

Configuring Server Groups

To configure server groups you need to complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server radius *groupname***

5. **server-private** *ip-address* [**auth-port** *port-number* | **acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Router(config)# aaa new-model	Enables AAA globally.
Step 4	aaa group server radius <i>groupname</i> Example: Router(config)# aaa group server radius v2.44.com	Groups different RADIUS server hosts into distinct lists and distinct methods. Enters server-group configuration mode.
Step 5	server-private <i>ip-address</i> [auth-port <i>port-number</i> acct-port <i>port-number</i>] [non-standard] [timeout <i>seconds</i>] [retransmit <i>retries</i>] [key <i>string</i>] Example: Router(config-sg-radius)# server-private 10.10.130.2 auth-port 1600 key ww	Configures the IP address of the private RADIUS server for the group server. Note If private server parameters are not specified, global configurations will be used. If global configurations are not specified, default values will be used.
Step 6	exit Example: Router(config-sg-radius)# exit	Exits from server-group configuration mode; returns to global configuration mode.

Configuring Authentication, Authorization, and Accounting for Per VRF AAA

To configure authentication, authorization, and accounting for Per VRF AAA, you need to complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**

4. **aaa authentication ppp** {default | list-name} method1 [method2...]
5. **aaa authorization** {network | exec | commands level | reverse-access | configuration} {default | list-name} method1 [method2...]
6. **aaa accounting system default** [vrf vrf-name] {start-stop | stop-only | none} [broadcast] group groupname
7. **aaa accounting delay-start** [vrf vrf-name]
8. **aaa accounting send stop-record authentication** {failure | success {remote-server}} [vrf vrf-name]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Router(config)# aaa new-model	Enables AAA globally.
Step 4	aaa authentication ppp {default list-name} method1 [method2...] Example: Router(config)# aaa authentication ppp method_list_v2.44.com group v2.44.com	Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP.
Step 5	aaa authorization {network exec commands level reverse-access configuration} {default list-name} method1 [method2...] Example: Router(config)# aaa authorization network method_list_v2.44.com group v2.44.com	Sets parameters that restrict user access to a network.
Step 6	aaa accounting system default [vrf vrf-name] {start-stop stop-only none} [broadcast] group groupname Example: Router(config)# aaa accounting system default vrf v2.44.com start-stop group v2.44.com	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS.

	Command or Action	Purpose
Step 7	aaa accounting delay-start [vrf <i>vrf-name</i>] Example: Router(config)# aaa accounting delay-start vrf v2.44.com	Displays generation of the start accounting records until the user IP address is established.
Step 8	aaa accounting send stop-record authentication { failure success { remote-server }} [vrf <i>vrf-name</i>] Example: Router(config)# aaa accounting send stop-record authentication failure vrf v2.44.com	Generates accounting stop records. When using the failure keyword a “stop” record will be sent for calls that are rejected during authentication. When using the success keyword a “stop” record will be sent for calls that meet one of the following criteria: <ul style="list-style-type: none"> • Calls that are authenticated by a remote AAA server when the call is terminated. • Calls that are not authenticated by a remote AAA server and the start record has been sent. • Calls that are successfully established and then terminated with the “stop-only” aaa accounting configuration. Note The success and remote-server keywords are available in Cisco IOS Release 12.4(2)T and later releases.

Configuring RADIUS-Specific Commands for Per VRF AAA

To configure RADIUS-specific commands for Per VRF AAA you need to complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip radius source-interface** *subinterface-name* [**vrf** *vrf-name*]
4. **radius-server attribute 44 include-in-access-req** [**vrf** *vrf-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	ip radius source-interface <i>subinterface-name</i> [vrf vrf-name] Example: Router(config)# ip radius source-interface loopback55	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets and enables the specification on a per-VRF basis.
Step 4	radius-server attribute 44 include-in-access-req [vrf vrf-name] Example: Router(config)# radius-server attribute 44 include-in-access-req vrf v2.44.com	Sends RADIUS attribute 44 in access request packets before user authentication and enables the specification on a per-VRF basis.

Configuring Interface-Specific Commands for Per VRF AAA

To configure interface-specific commands for Per VRF AAA, you need to complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip vrf forwarding** *vrf-name*
5. **ppp authentication** {*protocol1* [*protocol2...*]} *listname*
6. **ppp authorization** *list-name*
7. **ppp accounting default**
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> [<i>name-tag</i>] Example: Router(config)# interface loopback11	Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 4	ip vrf forwarding <i>vrf-name</i> Example: Router(config-if)# ip vrf forwarding v2.44.com	Associates a VRF with an interface.
Step 5	ppp authentication { <i>protocol1</i> [<i>protocol2...</i>]} <i>listname</i> Example: Router(config-if)# ppp authentication chap callin V2_44_com	Enables Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
Step 6	ppp authorization <i>list-name</i> Example: Router(config-if)# ppp authorization V2_44_com	Enables AAA authorization on the selected interface.
Step 7	ppp accounting default Example: Router(config-if)# ppp accounting default	Enables AAA accounting services on the selected interface.
Step 8	exit Example: Router(config)# exit	Exits interface configuration mode.

Configuring Per VRF AAA Using Local Customer Templates

This section contains the following procedures:

- [Configuring AAA, page 12](#)
- [Configuring Server Groups, page 12](#)
- [Configuring Authentication, Authorization, and Accounting for Per VRF AAA, page 12](#)
- [Configuring Authorization for Per VRF AAA with Local Customer Templates, page 13](#)
- [Configuring Local Customer Templates, page 13](#)

Configuring AAA

Perform the tasks as outlined in the “[Configuring Per VRF AAA](#)” section on page 7.

Configuring Server Groups

Perform the tasks as outlined in the “[Configuring Server Groups](#)” section on page 7.

Configuring Authentication, Authorization, and Accounting for Per VRF AAA

Perform the tasks as outlined in the “[Configuring Authentication, Authorization, and Accounting for Per VRF AAA](#)” section on page 8.

Configuring Authorization for Per VRF AAA with Local Customer Templates

To configure authorization for Per VRF AAA with local templates, you need to complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authorization template**
4. **aaa authorization network default local**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa authorization template Example: Router(config)# aaa authorization template	Enables the use of local or remote templates.
Step 4	aaa authorization network default local Example: Router(config)# aaa authorization network default local	Specifies local as the default method for authorization.

Configuring Local Customer Templates


To configure local customer templates, you need to complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn search-order domain**
4. **template name** [default | exit | multilink | no | peer | ppp]
5. **peer default ip address pool** pool-name
6. **ppp authentication** {protocol1 [protocol2...]} [if-needed] [list-name | default] [callin] [one-time]

7. **ppp authorization** [**default** | *list-name*]
8. **aaa accounting** {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname*
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	vpdn search-order domain Example: Router (config)# vpdn search-order domain	Looks up the profiles based on domain.
Step 4	template <i>name</i> [default exit multilink no peer ppp] Example: Router (config)# template v2.44.com	Creates a customer profile template and assigns a unique name that relates to the customer that will be receiving it. Enters template configuration mode.  Note Steps 5, 6, and 7 are optional. Enter multilink , peer , and ppp keywords appropriate to customer application requirements.
Step 5	peer default ip address pool <i>pool-name</i> Example: Router(config-template)# peer default ip address pool v2_44_com_pool	(Optional) Specifies that the customer profile to which this template is attached will use a local IP address pool with the specified name.
Step 6	ppp authentication { <i>protocol1</i> [<i>protocol2</i> ...]} [if-needed] [<i>list-name</i> default] [callin] [one-time] Example: Router(config-template)# ppp authentication chap	(Optional) Sets the PPP link authentication method.
Step 7	ppp authorization [default <i>list-name</i>] Example: Router(config-template)# ppp authorization v2_44_com	(Optional) Sets the PPP link authorization method.

	Command or Action	Purpose
Step 8	aaa accounting { <i>auth-proxy</i> <i>system</i> <i>network</i> <i>exec</i> <i>connection</i> <i>commands level</i> } { <i>default</i> <i>list-name</i> } [<i>vrf vrf-name</i>] { <i>start-stop</i> <i>stop-only</i> <i>none</i> } [<i>broadcast</i>] <i>group groupname</i> Example: Router(config-template)# aaa accounting v2_44_com	(Optional) Enables AAA operational parameters for the specified customer profile.
Step 9	exit Example: Router(config-template)# exit	Exits from template configuration mode; returns to global configuration mode.

Configuring Per VRF AAA Using Remote Customer Templates

This section contains the following procedures:

- [Configuring AAA, page 15](#)
- [Configuring Server Groups, page 15](#)
- [Configuring Authentication for Per VRF AAA with Remote Customer Profiles, page 15](#)
- [Configuring Authorization for Per VRF AAA with Remote Customer Profiles, page 16](#)
- [Configuring the RADIUS Profile on the SP RADIUS Server, page 17](#)

Configuring AAA

Perform the tasks as outlined in the “[Configuring Per VRF AAA](#)” section on page 7.

Configuring Server Groups

Perform the tasks as outlined in the “[Configuring Server Groups](#)” section on page 12.

Configuring Authentication for Per VRF AAA with Remote Customer Profiles

To configure authentication for Per VRF AAA with remote customer profiles, you need to perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authentication ppp** {*default* | *list-name*} *method1* [*method2...*]
4. **aaa authorization** {*network* | *exec* | *commands level* | *reverse-access* | *configuration*} {*default* | *list-name*} [[*method1* [*method2...*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa authentication ppp { default <i>list-name</i> } <i>method1</i> [<i>method2...</i>] Example: Router(config)# ppp authentication ppp default group radius	Specifies one or more authentication, authorization, and accounting (AAA) authentication methods for use on serial interfaces that are running PPP.
Step 4	aaa authorization { network exec commands <i>level</i> reverse-access configuration } { default <i>list-name</i> } [[<i>method1</i> [<i>method2...</i>]] Example: Router(config)# aaa authorization network default group sp	Sets parameters that restrict user access to a network.

Configuring Authorization for Per VRF AAA with Remote Customer Profiles

To configuring authorization for Per VRF AAA with remote customer profiles, you need to perform the following step.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authorization template**
4. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [[*method1* [*method2...*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa authorization template Example: Router(config)# aaa authorization template	Enables use of local or remote templates.
Step 4	aaa authorization {network exec commands level reverse-access configuration} {default list-name} [[method1 [method2...]] Example: Router(config)# aaa authorization network default sp	Specifies the server group that is named as the default method for authorization.

Configuring the RADIUS Profile on the SP RADIUS Server

Configure the RADIUS profile on the SP RADIUS server. See the “[Per VRF AAA Using a Remote RADIUS Customer Template: Example](#)” for an example of how to update the RADIUS profile.

Verifying VRF Routing Configurations

To verify VRF routing configurations, you need to complete the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **show ip route vrf *vrf-name***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	show ip route vrf vrf-name Example: Router(config)# show ip route vrf northvrf	Displays the IP routing table associated with a VRF.

Troubleshooting Per VRF AAA Configurations

To troubleshoot the Per VRF AAA feature, use at least one of the following commands in EXEC mode:

Command	Purpose
Router# debug aaa accounting	Displays information on accountable events as they occur.
Router# debug aaa authentication	Displays information on AAA authentication.
Router# debug aaa authorization	Displays information on AAA authorization.
Router# debug ppp negotiation	Displays information on traffic and exchanges in an internetwork implementing PPP.
Router# debug radius	Displays information associated with RADIUS.
Router# debug vpdn event	Displays Layer 2 Transport Protocol (L2TP) errors and events that are a part of normal tunnel establishment or shutdown for VPNs.
Router# debug vpdn error	Displays debug traces for VPN.

Configuration Examples for Per VRF AAA

This section provides the following configuration examples:

- [Per VRF Configuration: Examples, page 19](#)
- [Customer Template: Examples, page 20](#)
- [AAA Accounting Stop Records: Examples, page 22](#)

Per VRF Configuration: Examples

This section provides the following configuration examples:

- [Per VRF AAA: Example, page 19](#)
- [Per VRF AAA Using a Locally Defined Customer Template: Example, page 19](#)
- [Per VRF AAA Using a Remote RADIUS Customer Template: Example, page 20](#)

Per VRF AAA: Example

The following example shows how to configure the Per VRF AAA feature using a AAA server group with associated private servers:

```
aaa new-model

aaa authentication ppp method_list_v1.55.com group v1.55.com
aaa authorization network method_list_v1.55.com group v1.55.com
aaa accounting network method_list_v1.55.com start-stop group v1.55.com
aaa accounting system default vrf v1.55.com start-stop group v1.55.com
aaa accounting delay-start vrf v1.55.com
aaa accounting send stop-record authentication failure vrf v1.55.com

aaa group server radius v1.55.com
    server-private 10.10.132.4 auth-port 1645 acct-port 1646 key ww
    ip vrf forwarding v1.55.com

ip radius source-interface loopback55
radius-server attribute 44 include-in-access-req vrf v1.55.com
```

Per VRF AAA Using a Locally Defined Customer Template: Example

The following example shows how to configure the Per VRF AAA feature using a locally defined customer template with a AAA server group that has associated private servers:

```
aaa new-model
aaa authentication ppp method_list_v1.55.com group v1.55.com
aaa authorization network method_list_v1.55.com group v1.55.com
aaa authorization network default local
aaa authorization template
aaa accounting network method_list_v1.55.com start-stop group v1.55.com
aaa accounting system default vrf v1.55.com start-stop group v1.55.com

aaa group server radius V1_55_com
    server-private 10.10.132.4 auth-port 1645 acct-port 1646 key ww
    ip vrf forwarding V1.55.com

template V1.55.com
    peer default ip address pool V1_55_com_pool
    ppp authentication chap callin V1_55_com
    ppp authorization V1_55_com
    ppp accounting V1_55_com
    aaa accounting delay-start
    aaa accounting send stop-record authentication failure
    radius-server attribute 44 include-in-access-req
    ip vrf forwarding v1.55.com
    ip radius source-interface Loopback55
```

Per VRF AAA Using a Remote RADIUS Customer Template: Example

The following examples shows how to configure the Per VRF AAA feature using a remotely defined customer template on the SP RADIUS server with a AAA server group that has associated private servers:

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization template
aaa authorization network default group sp

aaa group server radius sp
  server 10.3.3.3

radius-server host 10.3.3.3 auth-port 1645 acct-port 1646 key sp_key
```

The following RADIUS server profile is configured on the SP RADIUS server:

```
cisco-avpair = "aaa:rad-serv#1=10.10.132.4 key ww"
cisco-avpair = "aaa:rad-serv-vrf#1=V1.55.com"
cisco-avpair = "aaa:rad-serv-source-if#1=Loopback 55"
cisco-avpair = "template:ppp-authen-list=group 1"
cisco-avpair = "template:ppp-author-list=group 1"
cisco-avpair = "template:ppp-acct-list= start-stop group 1"
cisco-avpair = "template:account-delay=on"
cisco-avpair = "template:account-send-stop=on"
cisco-avpair = "template:rad-attr44=access-req"
cisco-avpair = "template:peer-ip-pool=V1.55-pool"
cisco-avpair = "template:ip-vrf=V1.55.com"
cisco-avpair = "template:ip-unnumbered=Loopback 55"
framed-protocol = ppp
service-type = framed
```

Customer Template: Examples

This section provides the following configuration examples:

- [Locally Configured Customer Template with RADIUS Attribute Screening and Broadcast Accounting: Example, page 20](#)
- [Remotely Configured Customer Template with RADIUS Attribute Screening and Broadcast Accounting: Example, page 21](#)

Locally Configured Customer Template with RADIUS Attribute Screening and Broadcast Accounting: Example

The following example shows how to create a locally configured template for a single customer, configuring additional features including RADIUS attribute screening and broadcast accounting:

```
aaa authentication ppp default local group radius
aaa authentication ppp V1_55_com group V1_55_com
aaa authorization template
aaa authorization network default local group radius
aaa authorization network V1_55_com group V1_55_com
aaa accounting network V1_55_com start-stop broadcast group V1_55_com group SP_AAA_server

aaa group server radius SP_AAA_server
  server 10.10.100.7 auth-port 1645 acct-port 1646
```



```

aaa group server radius V1_55_com
  server-private 10.10.132.4 auth-port 1645 acct-port 1646
  authorization accept min-author
  accounting accept usage-only
  ip vrf forwarding V1.55.com

ip vrf V1.55.com
  rd 1:55
  route-target export 1:55
  route-target import 1:55

template V1.55.com
  peer default ip address pool V1.55-pool
  ppp authentication chap callin V1_55_com
  ppp authorization V1_55_com
  ppp accounting V1_55_com
  aaa accounting delay-start
  aaa accounting send stop-record authentication failure
  radius-server attribute 44 include-in-access-req

vpdn-group V1.55
  accept-dialin
  protocol l2tp
  virtual-template 13
  terminate-from hostname lac-lb-V1.55
  source-ip 10.10.104.12
  lcp renegotiation always
  l2tp tunnel password 7 060506324F41

interface Virtual-Template13
  ip vrf forwarding V1.55.com
  ip unnumbered Loopback55
  ppp authentication chap callin
  ppp multilink

ip local pool V1.55-pool 10.1.55.10 10.1.55.19 group V1.55-group

ip radius source-interface Loopback0
ip radius source-interface Loopback55 vrf V1.55.com

radius-server attribute list min-author
  attribute 6-7,22,27-28,242
radius-server attribute list usage-only
  attribute 1,40,42-43,46

radius-server host 10.10.100.7 auth-port 1645 acct-port 1646 key ww
radius-server host 10.10.132.4 auth-port 1645 acct-port 1646 key ww

```

Remotely Configured Customer Template with RADIUS Attribute Screening and Broadcast Accounting: Example

The following example shows how to create a remotely configured template for a single customer, configuring additional features including RADIUS attribute screening and broadcast accounting:

```

aaa authentication ppp default local group radius
aaa authorization template
aaa authorization network default local group radius

ip vrf V1.55.com
  rd 1:55

```

```

route-target export 1:55
route-target import 1:55

vpdn-group V1.55
accept-dialin
protocol l2tp
virtual-template 13
terminate-from hostname lac-lb-V1.55
source-ip 10.10.104.12
lcp renegotiation always
l2tp tunnel password 7 060506324F41

interface Virtual-Template13
no ip address
ppp authentication chap callin
ppp multilink

ip local pool V1.55-pool 10.1.55.10 10.1.55.19 group V1.55-group

radius-server attribute list min-author
attribute 6-7,22,27-28,242
radius-server attribute list usage-only
attribute 1,40,42-43,46

```

The customer template is stored as a RADIUS server profile for v1.55.com.

```

cisco-avpair = "aaa:rad-serv#1=10.10.132.4 key ww"
cisco-avpair = "aaa:rad-serv-vrf#1=V1.55.com"
cisco-avpair = "aaa:rad-serv-source-if#1=Loopback 55"
cisco-avpair = "aaa:rad-serv#2=10.10.100.7 key ww"
cisco-avpair = "aaa:rad-serv-source-if#2=Loopback 0"
cisco-avpair = "template:ppp-authen-list=group 1"
cisco-avpair = "template:ppp-author-list=group 1"
cisco-avpair = "template:ppp-acct-list= start-stop group 1 group 2 broadcast"
cisco-avpair = "template:account-delay=on"
cisco-avpair = "template:account-send-stop=on"
cisco-avpair = "template:rad-attr44=access-req"
cisco-avpair = "aaa:rad-serv-filter#1=authorization accept min-author"
cisco-avpair = "aaa:rad-serv-filter#1=accounting accept usage-only"
cisco-avpair = "template:peer-ip-pool=V1.55-pool"
cisco-avpair = "template:ip-vrf=V1.55.com"
cisco-avpair = "template:ip-unnumbered=Loopback 55"
framed-protocol = ppp
service-type = framed

```

AAA Accounting Stop Records: Examples

The following AAA accounting stop record examples show how to configure the **aaa accounting send stop-record authentication** command to control the generation of “stop” records when the **aaa accounting** command is issued with the **start-stop** or **stop-only** keyword.



Note

The **success** and **remote-server** keywords are available in Cisco IOS Release 12.4(2)T and later releases.

This section provides the following configuration examples:

- [AAA Accounting Stop Record and Successful Call: Example, page 23](#)
- [AAA Accounting Stop Record and Rejected Call: Example, page 25](#)

AAA Accounting Stop Record and Successful Call: Example

The following example shows “start” and “stop” records being sent for a successful call when the **aaa accounting send stop-record authentication** command is issued with the **failure** keyword.

```
Router# show running config | include aaa
.
.
.
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting send stop-record authentication failure
aaa accounting network default start-stop group radius
.
.
.
*Jul  7 03:28:31.543: AAA/BIND(00000018): Bind i/f Virtual-Template2
*Jul  7 03:28:31.547: ppp14 AAA/AUTHOR/LCP: Authorization succeeds trivially
*Jul  7 03:28:33.555: AAA/AUTHOR (0x18): Pick method list 'default'
*Jul  7 03:28:33.555: AAA/BIND(00000019): Bind i/f
*Jul  7 03:28:33.555:  Tnl 5192 L2TP: O SCCRQ
*Jul  7 03:28:33.555:  Tnl 5192 L2TP: O SCCRQ, flg TLS, ver 2, len 141, tnl 0,
ns 0, nr 0
      C8 02 00 8D 00 00 00 00 00 00 00 00 80 08 00 00
      00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
      00 06 11 30 80 10 00 00 00 07 4C 41 43 2D 74 75
      6E 6E 65 6C 00 19 00 00 00 08 43 69 73 63 6F 20
      53 79 73 74 65 6D 73 ...
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 0, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse SCCRQ
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 2, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Protocol Ver 256
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 3, len 10, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Framing Cap 0x0
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 4, len 10, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Bearer Cap 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 6, len 8, flag 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Firmware Ver 0x1120
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 7, len 16, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Hostname LNS-tunnel
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 8, len 25, flag 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Vendor Name Cisco Systems, Inc.
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 9, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Assigned Tunnel ID 6897
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 10, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Rx Window Size 20050
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 11, len 22, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Chlng
      81 13 03 F6 A8 E4 1D DD 25 18 25 6E 67 8C 7C 39
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 13, len 22, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Chlng Resp
      4D 52 91 DC 1A 43 B3 31 B4 F5 B8 E1 88 22 4F 41
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: No missing AVPs in SCCRQ
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: I SCCRQ, flg TLS, ver 2, len 157, tnl
5192, ns 0, nr 1
contiguous pak, size 157
```

```

C8 02 00 9D 14 48 00 00 00 00 01 80 08 00 00
00 00 00 02 80 08 00 00 00 02 01 00 80 0A 00 00
00 03 00 00 00 00 80 0A 00 00 00 04 00 00 00 00
00 08 00 00 00 06 11 20 80 10 00 00 00 07 4C 4E
53 2D 74 75 6E 6E 65 6C ...
*Jul 7 03:28:33.571: Tnl 5192 L2TP: I SCCRP from LNS-tunnel
*Jul 7 03:28:33.571: Tnl 5192 L2TP: O SCCCN to LNS-tunnel tnclid 6897
*Jul 7 03:28:33.571: Tnl 5192 L2TP: O SCCCN, flg TLS, ver 2, len 42, tnl
6897, ns 1, nr 1
C8 02 00 2A 1A F1 00 00 00 01 00 01 80 08 00 00
00 00 00 03 80 16 00 00 00 0D 32 24 17 BC 6A 19
B1 79 F3 F9 A9 D4 67 7D 9A DB
*Jul 7 03:28:33.571: uid:14 Tnl/Sn 5192/11 L2TP: O ICRQ to LNS-tunnel 6897/0
*Jul 7 03:28:33.571: uid:14 Tnl/Sn 5192/11 L2TP: O ICRQ, flg TLS, ver 2, len
63, tnl 6897, lsid 11, rsid 0, ns 2, nr 1
C8 02 00 3F 1A F1 00 00 00 02 00 01 80 08 00 00
00 00 00 0A 80 0A 00 00 00 0F C8 14 B4 03 80 08
00 00 00 0E 00 0B 80 0A 00 00 00 12 00 00 00 00
00 0F 00 09 00 64 0F 10 09 02 02 00 1B 00 00
*Jul 7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse AVP 0, len 8, flag
0x8000 (M)
*Jul 7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse ICRP
*Jul 7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse AVP 14, len 8, flag
0x8000 (M)
*Jul 7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Assigned Call ID 5
*Jul 7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: No missing AVPs in ICRP
*Jul 7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: I ICRP, flg TLS, ver 2, len
28, tnl 5192, lsid 11, rsid 0, ns 1, nr 3
contiguous pak, size 28
C8 02 00 1C 14 48 00 0B 00 01 00 03 80 08 00 00
00 00 00 0B 80 08 00 00 00 0E 00 05
*Jul 7 03:28:33.579: uid:14 Tnl/Sn 5192/11 L2TP: O ICCN to LNS-tunnel 6897/5
*Jul 7 03:28:33.579: uid:14 Tnl/Sn 5192/11 L2TP: O ICCN, flg TLS, ver 2, len
167, tnl 6897, lsid 11, rsid 5, ns 3, nr 2
C8 02 00 A7 1A F1 00 05 00 03 00 02 80 08 00 00
00 00 00 0C 80 0A 00 00 00 18 06 1A 80 00 00 0A
00 00 00 26 06 1A 80 00 80 0A 00 00 00 13 00 00
00 01 00 15 00 00 00 1B 01 04 05 D4 03 05 C2 23
05 05 06 0A 0B E2 7A ...
*Jul 7 03:28:33.579: RADIUS/ENCODE(00000018):Orig. component type = PPoE
*Jul 7 03:28:33.579: RADIUS(00000018): Config NAS IP: 10.0.0.0
*Jul 7 03:28:33.579: RADIUS(00000018): sending
*Jul 7 03:28:33.579: RADIUS/ENCODE: Best Local IP-Address 10.0.1.123 for
Radius-Server 172.19.192.238
*Jul 7 03:28:33.579: RADIUS(00000018): Send Accounting-Request to
172.19.192.238:2196 id 1646/23, len 176
*Jul 7 03:28:33.579: RADIUS: authenticator 3C 81 D6 C5 2B 6D 21 8E - 19 FF
43 B5 41 86 A8 A5
*Jul 7 03:28:33.579: RADIUS: Acct-Session-Id [44] 10 "00000023"
*Jul 7 03:28:33.579: RADIUS: Framed-Protocol [7] 6
PPP [1]
*Jul 7 03:28:33.579: RADIUS: Tunnel-Medium-Type [65] 6
00:IPv4 [1]
*Jul 7 03:28:33.583: RADIUS: Tunnel-Client-Endpoi[66] 10 "10.0.0.1"
*Jul 7 03:28:33.583: RADIUS: Tunnel-Server-Endpoi[67] 10 "10.0.0.2"
*Jul 7 03:28:33.583: RADIUS: Tunnel-Assignment-Id[82] 5 "lac"
*Jul 7 03:28:33.583: RADIUS: Tunnel-Type [64] 6
00:L2TP [3]
*Jul 7 03:28:33.583: RADIUS: Acct-Tunnel-Connecti[68] 12 "3356800003"
*Jul 7 03:28:33.583: RADIUS: Tunnel-Client-Auth-I[90] 12 "LAC-tunnel"
*Jul 7 03:28:33.583: RADIUS: Tunnel-Server-Auth-I[91] 12 "LNS-tunnel"
*Jul 7 03:28:33.583: RADIUS: User-Name [1] 16 "user@domain.com"
*Jul 7 03:28:33.583: RADIUS: Acct-Authentic [45] 6
Local [2]

```

```

*Jul  7 03:28:33.583: RADIUS:  Acct-Status-Type      [40]  6
Start                               [1]
*Jul  7 03:28:33.583: RADIUS:  NAS-Port-Type        [61]  6
Virtual                             [5]
*Jul  7 03:28:33.583: RADIUS:  NAS-Port              [5]  6
0
*Jul  7 03:28:33.583: RADIUS:  NAS-Port-Id           [87]  9   "0/0/0/0"
*Jul  7 03:28:33.583: RADIUS:  Service-Type          [6]  6
Framed                             [2]
*Jul  7 03:28:33.583: RADIUS:  NAS-IP-Address         [4]  6
10.0.1.123
*Jul  7 03:28:33.583: RADIUS:  Acct-Delay-Time        [41]  6
0
*Jul  7 03:28:33.683: RADIUS: Received from id 1646/23 172.19.192.238:2196,
Accounting-response, len 20
*Jul  7 03:28:33.683: RADIUS:  authenticator 1C E9 53 42 A2 8A 58 9A - C3 CC
1D 79 9F A4 6F 3A

```

AAA Accounting Stop Record and Rejected Call: Example

The following example shows the “stop” record being sent for a rejected call during authentication when the **aaa accounting send stop-record authentication** command is issued with the **success** keyword.

```

Router# show running config | include aaa
.
.
.
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting send stop-record authentication success remote-server
aaa accounting network default start-stop group radius

Router#

*Jul  7 03:39:40.199: AAA/BIND(00000026): Bind i/f Virtual-Template2
*Jul  7 03:39:40.199: ppp21 AAA/AUTHOR/LCP: Authorization succeeds trivially
*Jul  7 03:39:42.199: RADIUS/ENCODE(00000026):Orig. component type = PPoE
*Jul  7 03:39:42.199: RADIUS:  AAA Unsupported      [156]  7
*Jul  7 03:39:42.199: RADIUS:   30 2F 30 2F
30                               [0/0/0]
*Jul  7 03:39:42.199: RADIUS(00000026): Config NAS IP: 10.0.0.0
*Jul  7 03:39:42.199: RADIUS/ENCODE(00000026): acct_session_id: 55
*Jul  7 03:39:42.199: RADIUS(00000026): sending
*Jul  7 03:39:42.199: RADIUS/ENCODE: Best Local IP-Address 10.0.1.123 for
Radius-Server 172.19.192.238
*Jul  7 03:39:42.199: RADIUS(00000026): Send Access-Request to
172.19.192.238:2195 id 1645/14, len 94
*Jul  7 03:39:42.199: RADIUS:  authenticator A6 D1 6B A4 76 9D 52 CF - 33 5D
16 BE AC 7E 5F A6
*Jul  7 03:39:42.199: RADIUS:  Framed-Protocol        [7]  6
PPP                               [1]
*Jul  7 03:39:42.199: RADIUS:  User-Name              [1]  16   "user@yahoo.com"
*Jul  7 03:39:42.199: RADIUS:  CHAP-Password          [3]  19   *
*Jul  7 03:39:42.199: RADIUS:  NAS-Port-Type          [61]  6
Virtual                             [5]
*Jul  7 03:39:42.199: RADIUS:  NAS-Port              [5]  6
0
*Jul  7 03:39:42.199: RADIUS:  NAS-Port-Id           [87]  9   "0/0/0/0"
*Jul  7 03:39:42.199: RADIUS:  Service-Type          [6]  6
Framed                             [2]

```

```

*Jul 7 03:39:42.199: RADIUS: NAS-IP-Address [4] 6
10.0.1.123
*Jul 7 03:39:42.271: RADIUS: Received from id 1645/14 172.19.192.238:2195,
Access-Accept, len 194
*Jul 7 03:39:42.271: RADIUS: authenticator 30 AD FF 8E 59 0C E4 6C - BA 11
23 63 81 DE 6F D7
*Jul 7 03:39:42.271: RADIUS: Framed-Protocol [7] 6
PPP [1]
*Jul 7 03:39:42.275: RADIUS: Service-Type [6] 6
Framed [2]
*Jul 7 03:39:42.275: RADIUS: Vendor, Cisco [26] 26
*Jul 7 03:39:42.275: RADIUS: Cisco AVpair [1] 20 "vpdn:tunnel-
id=lac"
*Jul 7 03:39:42.275: RADIUS: Vendor, Cisco [26] 29
*Jul 7 03:39:42.275: RADIUS: Cisco AVpair [1] 23 "vpdn:tunnel-
type=l2tp"
*Jul 7 03:39:42.275: RADIUS: Vendor, Cisco [26] 30
*Jul 7 03:39:42.275: RADIUS: Cisco AVpair [1] 24 "vpdn:gw-
password=cisco"
*Jul 7 03:39:42.275: RADIUS: Vendor, Cisco [26] 31
*Jul 7 03:39:42.275: RADIUS: Cisco AVpair [1] 25 "vpdn:nas-
password=cisco"
*Jul 7 03:39:42.275: RADIUS: Vendor, Cisco [26] 34
*Jul 7 03:39:42.275: RADIUS: Cisco AVpair [1] 28 "vpdn:ip-
addresses=12.0.0.2"
*Jul 7 03:39:42.275: RADIUS: Service-Type [6] 6
Framed [2]
*Jul 7 03:39:42.275: RADIUS: Framed-Protocol [7] 6
PPP [1]
*Jul 7 03:39:42.275: RADIUS(00000026): Received from id 1645/14
*Jul 7 03:39:42.275: ppp21 PPP/AAA: Check Attr: Framed-Protocol
*Jul 7 03:39:42.275: ppp21 PPP/AAA: Check Attr: service-type
*Jul 7 03:39:42.275: ppp21 PPP/AAA: Check Attr: tunnel-id
*Jul 7 03:39:42.275: ppp21 PPP/AAA: Check Attr: tunnel-type
*Jul 7 03:39:42.275: ppp21 PPP/AAA: Check Attr: gw-password
*Jul 7 03:39:42.275: ppp21 PPP/AAA: Check Attr: nas-password
*Jul 7 03:39:42.275: ppp21 PPP/AAA: Check Attr: ip-addresses
*Jul 7 03:39:42.275: ppp21 PPP/AAA: Check Attr: service-type
*Jul 7 03:39:42.275: ppp21 PPP/AAA: Check Attr: Framed-Protocol
*Jul 7 03:39:42.279: AAA/BIND(00000027): Bind i/f
*Jul 7 03:39:42.279: Tnl 21407 L2TP: O SCCRQ
*Jul 7 03:39:42.279: Tnl 21407 L2TP: O SCCRQ, flg TLS, ver 2, len 134, tnl
0, ns 0, nr 0
      C8 02 00 86 00 00 00 00 00 00 00 00 80 08 00 00
      00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
      00 06 11 30 80 09 00 00 00 07 6C 61 63 00 19 00
      00 00 08 43 69 73 63 6F 20 53 79 73 74 65 6D 73
      2C 20 49 6E 63 2E 80 ...
*Jul 7 03:39:49.279: Tnl 21407 L2TP: O StopCCN
*Jul 7 03:39:49.279: Tnl 21407 L2TP: O StopCCN, flg TLS, ver 2, len 66, tnl
0, ns 1, nr 0
      C8 02 00 42 00 00 00 00 00 01 00 00 80 08 00 00
      00 00 00 04 80 1E 00 00 00 01 00 02 00 06 54 6F
      6F 20 6D 61 6E 79 20 72 65 74 72 61 6E 73 6D 69
      74 73 00 08 00 09 00 69 00 01 80 08 00 00 00 09
      53 9F
*Jul 7 03:39:49.279: RADIUS/ENCODE(00000026):Orig. component type = PPoE
*Jul 7 03:39:49.279: RADIUS(00000026): Config NAS IP: 10.0.0.0
*Jul 7 03:39:49.279: RADIUS(00000026): sending
*Jul 7 03:39:49.279: RADIUS/ENCODE: Best Local IP-Address 10.0.1.123 for
Radius-Server 172.19.192.238
*Jul 7 03:39:49.279: RADIUS(00000026): Send Accounting-Request to
172.19.192.238:2196 id 1646/32, len 179
*Jul 7 03:39:49.279: RADIUS: authenticator 0A 85 2F F0 65 6F 25 E1 - 97 54

```

```

CC BF EA F7 62 89
*Jul  7 03:39:49.279: RADIUS:  Acct-Session-Id      [44] 10 "00000037"
*Jul  7 03:39:49.279: RADIUS:  Framed-Protocol      [7]  6
PPP                                     [1]
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Medium-Type   [65] 6
00:IPv4                               [1]
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Client-Endpoi [66] 10 "12.0.0.1"
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Server-Endpoi [67] 10 "12.0.0.2"
*Jul  7 03:39:49.283: RADIUS:  Tunnel-Type          [64] 6
00:L2TP                               [3]
*Jul  7 03:39:49.283: RADIUS:  Acct-Tunnel-Connecti [68] 3  "0"
*Jul  7 03:39:49.283: RADIUS:  Tunnel-Client-Auth-I [90] 5  "lac"
*Jul  7 03:39:49.283: RADIUS:  User-Name            [1] 16  "user@domian.com"
*Jul  7 03:39:49.283: RADIUS:  Acct-Authentic       [45] 6
RADIUS                                [1]
*Jul  7 03:39:49.283: RADIUS:  Acct-Session-Time    [46] 6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Input-Octets     [42] 6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Output-Octets    [43] 6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Input-Packets    [47] 6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Output-Packets   [48] 6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Terminate-Cause [49] 6  nas-
error                                [9]
*Jul  7 03:39:49.283: RADIUS:  Acct-Status-Type      [40] 6
Stop                                [2]
*Jul  7 03:39:49.283: RADIUS:  NAS-Port-Type         [61] 6
Virtual                             [5]
*Jul  7 03:39:49.283: RADIUS:  NAS-Port              [5] 6
0
*Jul  7 03:39:49.283: RADIUS:  NAS-Port-Id           [87] 9  "0/0/0/0"
*Jul  7 03:39:49.283: RADIUS:  Service-Type          [6] 6
Framed                             [2]
*Jul  7 03:39:49.283: RADIUS:  NAS-IP-Address        [4] 6
10.0.1.123
*Jul  7 03:39:49.283: RADIUS:  Acct-Delay-Time       [41] 6
0
*Jul  7 03:39:49.335: RADIUS: Received from id 1646/32 172.19.192.238:2196,
Accounting-response, len 20
*Jul  7 03:39:49.335: RADIUS:  authenticator C8 C4 61 AF 4D 9F 78 07 - 94 2B
44 44 17 56 EC 03

```

Additional References

The following sections provide references related to Per VRF AAA.

Related Documents

Related Topic	Document Title
AAA: Configuring Server Groups	Cisco IOS Security Configuration Guide , Release 12.4
Broadcast Accounting	AAA Broadcast Accounting Feature Guide , Release 12.1(1)T
Cisco IOS Security Commands	Cisco IOS Security Command Reference , Release 12.4
Cisco IOS Switching Services Commands	Cisco IOS Switching Services Command Reference , Release 12.2
Configuring Multiprotocol Label Switching	“Configuring Multiprotocol Label Switching” chapter in the Cisco IOS Switching Services Configuration Guide , Release 12.2
Configuring Virtual Templates section	“Virtual Templates, Profiles, and Networks” chapter in the Cisco IOS Dial Technologies Configuration Guide , Release 12.2
RADIUS Attribute Screening	RADIUS Attribute Screening Feature Guide , Release 12.4
RADIUS Debug Enhancements	RADIUS Debug Enhancements Feature Guide , Release 12.4

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or a Cisco IOS master commands list.

- **aaa accounting**
- **aaa accounting delay-start**
- **aaa accounting send stop-record authentication**
- **aaa authorization template**
- **ip radius source-interface**
- **ip vrf forwarding (server-group)**
- **radius-server attribute 44 include-in-access-req**
- **radius-server domain-stripping**
- **server-private (RADIUS)**

Feature Information for Per VRF AAA

Table 2 lists the release history for this feature. Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

This feature has also been referred to as the Dynamic Per VRF AAA feature.

Table 2 Feature Information for Per VRF AAA

Feature Name	Releases	Feature Information
Per VRF AAA	12.2(1)DX 12.2(2)DD 12.2(4)B 12.2(13)T 12.2(15)T 12.4(2)T 12.2(28)SB 12.2(33)SRC	<p>The Per VRF AAA feature allows authentication, authorization, and accounting (AAA) on the basis of Virtual Private Network (VPN) routing and forwarding (VRF) instances. For Cisco IOS Release 12.2(15)T or later releases, you can use a customer template, which may be stored either locally or remotely, and AAA services can be performed on the information that is stored in the customer template.</p> <p>In 12.2(1)DX, this feature was introduced on the Cisco 7200 series and the Cisco 7401ASR.</p> <p>In 12.2(2)DD, the ip vrf forwarding and radius-server domain-stripping commands were added.</p> <p>In 12.2(15)T, the aaa authorization template command was added.</p> <p>In 12.4(2)T, the aaa accounting send stop-record authentication command was updated with additional support for AAA accounting stop records.</p> <p>In 12.2(33)SRC dynamic configuration of AAA was introduced.</p>
Per VRF AAA	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Glossary

AAA—authentication, authorization, and accounting. A framework of security services that provide the method for identifying users (authentication), for remote access control (authorization), and for collecting and sending security server information used for billing, auditing, and reporting (accounting).

L2TP—Layer 2 Tunnel Protocol. A Layer 2 tunneling protocol that enables an ISP or other access service to create a virtual tunnel to link customer remote sites or remote users with corporate home networks. In particular, a network access server (NAS) at the ISP point of presence (POP) exchanges PPP messages with the remote users and communicates by L2F or L2TP requests and responses with the customer tunnel server to set up tunnels.

PE—Provider Edge. Networking devices that are located on the edge of a service provider network.

RADIUS—Remote Authentication Dial-In User Service. RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

SP—service provider.

VHG—Virtual Home Gateway.

VPDN—virtual private dialup network.

VPN—Virtual Private Network. A system that permits dial-in networks to exist remotely to home networks, while giving the appearance of being directly connected. VPNs use L2TP and L2F to terminate the Layer 2 and higher parts of the network connection at the LNS instead of the LAC.

VRF—Virtual Route Forwarding. Initially, a router has only one global default routing/forwarding table. VRFs can be viewed as multiple disjointed routing/forwarding tables, where the routes of a user have no correlation with the routes of another user.

**Note**

See [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2001-2008 Cisco Systems, Inc. All rights reserved.



RFC-2867 RADIUS Tunnel Accounting

The RFC-2867 RADIUS Tunnel Accounting introduces six new RADIUS accounting types that are used with the RADIUS accounting attribute Acct-Status-Type (attribute 40), which indicates whether an accounting request marks the beginning of user service (start) or the end (stop).

This feature also introduces two new virtual private virtual private dialup network (VPDN) commands that help users better troubleshoot VPDN session events.

History for RFC-2867 RADIUS Tunnel Accounting

Release	Modification
12.2(15)B	This feature was introduced on the Cisco 6400 series, Cisco 7200 series, and the Cisco 7400 series routers.
12.3(4)T	This feature was integrated into Cisco IOS Release 12.3(4)T.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions for RFC-2867 RADIUS Tunnel Accounting, page 2](#)
- [Information About RFC-2867 RADIUS Tunnel Accounting, page 2](#)
- [How to Configure RADIUS Tunnel Accounting, page 6](#)
- [Configuration Examples for RADIUS Tunnel Accounting, page 8](#)
- [Additional References, page 11](#)
- [Command Reference, page 12](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Restrictions for RFC-2867 RADIUS Tunnel Accounting

RADIUS tunnel accounting works only with L2TP tunnel support.

Information About RFC-2867 RADIUS Tunnel Accounting

To use RADIUS tunnel attributes and commands, you should understand the following concepts:

- [Benefits of RFC-2867 RADIUS Tunnel Accounting, page 2](#)
- [RADIUS Attributes Support for RADIUS Tunnel Accounting, page 2](#)

Benefits of RFC-2867 RADIUS Tunnel Accounting

Without RADIUS tunnel accounting support, VPDN with network accounting, which allows users to determine tunnel-link status changes, did not report all possible attributes to the accounting record file. Now that all possible attributes can be displayed, users can better verify accounting records with their Internet Service Providers (ISPs).

RADIUS Attributes Support for RADIUS Tunnel Accounting

[Table 1](#) outlines the new RADIUS accounting types that are designed to support the provision of compulsory tunneling in dialup networks; that is, these attribute types allow you to better track tunnel status changes.

**Note**

The accounting types are divided into two separate tunnel types so users can decide if they want tunnel type, tunnel-link type, or both types of accounting.

Table 1 **RADIUS Accounting Types for the Acct-Status-Type Attribute**

Type-Name	Number	Description	Additional Attributes ¹
Tunnel-Start	9	Marks the beginning of a tunnel setup with another node.	<ul style="list-style-type: none"> • User-Name (1)—from client • NAS-IP-Address (4)—from AAA • Acct-Delay-Time (41)—from AAA • Event-Timestamp (55)—from AAA • Tunnel-Type (64)—from client • Tunnel-Medium-Type (65)—from client • Tunnel-Client-Endpoint (66)—from client • Tunnel-Server-Endpoint (67)—from client • Acct-Tunnel-Connection (68)—from client
Tunnel-Stop	10	Marks the end of a tunnel connection to or from another node.	<ul style="list-style-type: none"> • User-Name (1)—from client • NAS-IP-Address (4)—from AAA • Acct-Delay-Time (41)—from AAA • Acct-Input-Octets (42)—from AAA • Acct-Output-Octets (43)—from AAA • Acct-Session-Id (44)—from AAA • Acct-Session-Time (46)—from AAA • Acct-Input-Packets (47)—from AAA • Acct-Output-Packets (48)—from AAA • Acct-Terminate-Cause (49)—from AAA • Acct-Multi-Session-Id (51)—from AAA • Event-Timestamp (55)—from AAA • Tunnel-Type (64)—from client • Tunnel-Medium-Type (65)—from client • Tunnel-Client-Endpoint (66)—from client • Tunnel-Server-Endpoint (67)—from client • Acct-Tunnel-Connection (68)—from client • Acct-Tunnel-Packets-Lost (86)—from client

Table 1 *RADIUS Accounting Types for the Acct-Status-Type Attribute (continued)*

Type-Name	Number	Description	Additional Attributes ¹
Tunnel-Reject	11	Marks the rejection of a tunnel setup with another node.	<ul style="list-style-type: none"> • User-Name (1)—from client • NAS-IP-Address (4)—from AAA • Acct-Delay-Time (41)—from AAA • Acct-Terminate-Cause (49)—from client • Event-Timestamp (55)—from AAA • Tunnel-Type (64)—from client • Tunnel-Medium-Type (65)—from client • Tunnel-Client-Endpoint (66)—from client • Tunnel-Server-Endpoint (67)—from client • Acct-Tunnel-Connection (68)—from client
Tunnel-Link-Start	12	Marks the creation of a tunnel link. Only some tunnel types (Layer 2 Transport Protocol [L2TP]) support the multiple links per tunnel; this value should be included only in accounting packets for tunnel types that support multiple links per tunnel.	<ul style="list-style-type: none"> • User-Name (1)—from client • NAS-IP-Address (4)—from AAA • NAS-Port (5)—from AAA • Acct-Delay-Time (41)—from AAA • Event-Timestamp (55)—from AAA • Tunnel-Type (64)—from client • Tunnel-Medium-Type (65)—from client • Tunnel-Client-Endpoint (66)—from client • Tunnel-Server-Endpoint (67)—from client • Acct-Tunnel-Connection (68)—from client

Table 1 **RADIUS Accounting Types for the Acct-Status-Type Attribute (continued)**

Type-Name	Number	Description	Additional Attributes ¹
Tunnel-Link-Stop	13	Marks the end of a tunnel link. Only some tunnel types (L2TP) support the multiple links per tunnel; this value should be included only in accounting packets for tunnel types that support multiple links per tunnel.	<ul style="list-style-type: none"> • User-Name (1)—from client • NAS-IP-Address (4)—from AAA • NAS-Port (5)—from AAA • Acct-Delay-Time (41)—from AAA • Acct-Input-Octets (42)—from AAA • Acct-Output-Octets (43)—from AAA • Acct-Session-Id (44)—from AAA • Acct-Session-Time (46)—from AAA • Acct-Input-Packets (47)—from AAA • Acct-Output-Packets (48)—from AAA • Acct-Terminate-Cause (49)—from AAA • Acct-Multi-Session-Id (51)—from AAA • Event-Timestamp (55)—from AAA • NAS-Port-Type (61)—from AAA • Tunnel-Type (64)—from client • Tunnel-Medium-Type (65)—from client • Tunnel-Client-Endpoint (66)—from client • Tunnel-Server-Endpoint (67)—from client • Acct-Tunnel-Connection (68)—from client • Acct-Tunnel-Packets-Lost (86)—from client
Tunnel-Link-Reject	14	Marks the rejection of a tunnel setup for a new link in an existing tunnel. Only some tunnel types (L2TP) support the multiple links per tunnel; this value should be included only in accounting packets for tunnel types that support multiple links per tunnel.	<ul style="list-style-type: none"> • User-Name (1)—from client • NAS-IP-Address (4)—from AAA • Acct-Delay-Time (41)—from AAA • Acct-Terminate-Cause (49)—from AAA • Event-Timestamp (55)—from AAA • Tunnel-Type (64)—from client • Tunnel-Medium-Type (65)—from client • Tunnel-Client-Endpoint (66)—from client • Tunnel-Server-Endpoint (67)—from client • Acct-Tunnel-Connection (68)—from client

1. If the specified tunnel type is used, these attributes should also be included in the accounting request packet.

How to Configure RADIUS Tunnel Accounting

This section contains the following procedures

- [Enabling Tunnel Type Accounting Records, page 6](#)
- [Verifying RADIUS Tunnel Accounting, page 8](#)

Enabling Tunnel Type Accounting Records

Use this task to configure your LAC to send tunnel and tunnel-link accounting records to be sent to the RADIUS server.

VPDN Tunnel Events

Two new command line interfaces (CLIs)—vpdn session accounting network (tunnel-link-type records) and vpdn tunnel accounting network (tunnel-type records)—are supported to help identify the following events:

- A VPDN tunnel is brought up or destroyed
- A request to create a VPDN tunnel is rejected
- A user session within a VPDN tunnel is brought up or brought down
- A user session create request is rejected

**Note**

The first two events are tunnel-type accounting records: authentication, authorization, and accounting (AAA) sends Tunnel-Start, Tunnel-Stop, or Tunnel-Reject accounting records to the RADIUS server. The next two events are tunnel-link-type accounting records: AAA sends Tunnel-Link-Start, Tunnel-Link-Stop, or Tunnel-Link-Reject accounting records to the RADIUS server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa accounting network {default | list-name} {start-stop | stop-only | wait-start | none} group groupname**
4. **vpdn enable**
5. **vpdn tunnel accounting network list-name**
6. **vpdn session accounting network list-name**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# aaa accounting network { default <i>list-name</i> } { start-stop stop-only wait-start none } group <i>groupname</i>	Enables network accounting. <ul style="list-style-type: none"> default—If the default network accounting method-list is configured and no additional accounting configurations are enabled on the interface, network accounting is enabled by default. If either the vpdn session accounting network command or the vpdn tunnel accounting network command is linked to the default method-list, all tunnel and tunnel-link accounting records are enabled for those sessions. <i>list-name</i>—The <i>list-name</i> defined in the aaa accounting command must be the same as the <i>list-name</i> defined in the VPDN command; otherwise, accounting will not occur.
Step 4	Router(config)# vpdn enable	Enables virtual private dialup networking on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (if applicable).
Step 5	Router(config)# vpdn tunnel accounting network <i>list-name</i>	Enables Tunnel-Start, Tunnel-Stop, and Tunnel-Reject accounting records. <ul style="list-style-type: none"> <i>list-name</i>—The <i>list-name</i> must match the <i>list-name</i> defined in the aaa accounting command; otherwise, network accounting will not occur.
Step 6	Router(config)# vpdn session accounting network <i>list-name</i>	Enables Tunnel-Link-Start, Tunnel-Link-Stop, and Tunnel-Link-Reject accounting records. <ul style="list-style-type: none"> <i>list-name</i>—The <i>list-name</i> must match the <i>list-name</i> defined in the aaa accounting command; otherwise, network accounting will not occur.

What To Do Next

After you have enabled RADIUS tunnel accounting, you can verify your configuration via the following optional task “[Verifying RADIUS Tunnel Accounting](#).”

Verifying RADIUS Tunnel Accounting

Use either one or both of the following optional steps to verify your RADIUS tunnel accounting configuration.

SUMMARY STEPS

1. `enable`
2. `show accounting`
3. `show vpdn [session | tunnel]`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	Router# <code>show accounting</code>	Displays the active accountable events on the network and helps collect information in the event of a data loss on the accounting server.
Step 3	Router# <code>show vpdn [session] [tunnel]</code>	Displays information about active L2TP tunnel and message identifiers in a VPDN. <ul style="list-style-type: none">• session—Displays a summary of the status of all active tunnels.• tunnel—Displays information about all active L2TP tunnels in summary-style format.

Configuration Examples for RADIUS Tunnel Accounting

This section provides the following configuration examples:

- [Configuring RADIUS Tunnel Accounting on LAC: Example, page 8](#)
- [Configuring RADIUS Tunnel Accounting on LNS: Example, page 10](#)

Configuring RADIUS Tunnel Accounting on LAC: Example

The following example shows how to configure your L2TP access concentrator (LAC) to send tunnel and tunnel-link accounting records to the RADIUS server:

```
aaa new-model
!
!
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting network m1 start-stop group radius
aaa accounting network m2 stop-only group radius
```

```
aaa session-id common
enable secret 5 $1$IDjH$iL7puCja1RMlyOM.JAeuf/
enable password lab
!
username ISP_LAC password 0 tunnelpass
!
!
resource-pool disable
!
!
ip subnet-zero
ip cef
no ip domain-lookup
ip host dirt 171.69.1.129
!
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
vpdn search-order domain dnis
!
vpdn-group 1
 request-dialin
  protocol l2tp
  domain cisco.com
  initiate-to ip 10.1.26.71
  local name ISP_LAC
!
isdn switch-type primary-5ess
!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
controller T1 7/4
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
!
!
interface FastEthernet0/0
 ip address 10.1.27.74 255.255.255.0
 no ip mroute-cache
 duplex half
 speed auto
 no cdp enable
!
interface FastEthernet0/1
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
interface Serial7/4:23
 ip address 60.0.0.2 255.255.255.0
 encapsulation ppp
 dialer string 2000
 dialer-group 1
 isdn switch-type primary-5ess
 ppp authentication chap
!
interface Group-Async0
```

```

no ip address
shutdown
group-range 1/00 3/107
!
ip default-gateway 10.1.27.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.27.254
no ip http server
ip pim bidir-enable
!
!
dialer-list 1 protocol ip permit
no cdp run
!
!
radius-server host 172.19.192.26 auth-port 1645 acct-port 1646 key rad123
radius-server retransmit 3
call rsvp-sync
!

```

Configuring RADIUS Tunnel Accounting on LNS: Example

The following example shows how to configure your L2TP network server (LNS) to send tunnel and tunnel-link accounting records to the RADIUS server:

```

aaa new-model
!
!
aaa accounting network m1 start-stop group radius
aaa accounting network m2 stop-only group radius
aaa session-id common
enable secret 5 $1$ftf.$wE6Q5Yv6hmQiwL9pizPCg1
!
username ENT_LNS password 0 tunnelpass
username user1@cisco.com password 0 lab
username user2@cisco.com password 0 lab
spe 1/0 1/7
  firmware location system:/ucode/mica_port_firmware
spe 2/0 2/9
  firmware location system:/ucode/mica_port_firmware
!
!
resource-pool disable
clock timezone est 2
!
ip subnet-zero
no ip domain-lookup
ip host CALLGEN-SECURITY-V2 64.24.80.28 3.47.0.0
ip host dirt 171.69.1.129
!
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
!
vpdn-group 1
accept-dialin
  protocol l2tp
  virtual-template 1
  terminate-from hostname ISP_LAC
  local name ENT_LNS
!
isdn switch-type primary-5ess

```

```
!  
!  
!  
!  
!  
!  
fax interface-type modem  
mta receive maximum-recipients 0  
!  
interface Loopback0  
  ip address 70.0.0.101 255.255.255.0  
!  
interface Loopback1  
  ip address 80.0.0.101 255.255.255.0  
!  
interface Ethernet0  
  ip address 10.1.26.71 255.255.255.0  
  no ip mroute-cache  
  no cdp enable  
!  
interface Virtual-Template1  
  ip unnumbered Loopback0  
  peer default ip address pool vpdn-pool1  
  ppp authentication chap  
!  
interface Virtual-Template2  
  ip unnumbered Loopback1  
  peer default ip address pool vpdn-pool2  
  ppp authentication chap  
!  
interface FastEthernet0  
  no ip address  
  no ip mroute-cache  
  shutdown  
  duplex auto  
  speed auto  
  no cdp enable  
!  
ip local pool vpdn-pool1 70.0.0.1 70.0.0.100  
ip local pool vpdn-pool2 80.0.0.1 80.0.0.100  
ip default-gateway 10.1.26.254  
ip classless  
ip route 0.0.0.0 0.0.0.0 10.1.26.254  
ip route 90.1.1.2 255.255.255.255 10.1.26.254  
no ip http server  
ip pim bidir-enable  
!  
!  
dialer-list 1 protocol ip permit  
no cdp run  
!  
!  
radius-server host 172.19.192.80 auth-port 1645 acct-port 1646 key rad123  
radius-server retransmit 3  
call rsvp-sync
```

Additional References

The following sections provide references related to RFC-2867 RADIUS Tunnel Accounting.

Related Documents

Related Topic	Document Title
RADIUS attributes	<i>The appendix “RADIUS Attributes” in the Cisco IOS Security Configuration Guide</i>
Vpdn	<i>The chapter “Configuring Virtual Private Networks” in the Cisco IOS Dial Technologies Configuration Guide</i>
Network accounting	<i>The chapter “Configuring Accounting” in the Cisco IOS Security Configuration Guide</i>

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2867	<i>RADIUS Accounting Modifications for Tunnel Protocol Support</i>

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this

module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **aaa accounting**
 - **vpdn session accounting network**
 - **vpdn tunnel accounting network**
-



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



RADIUS Attribute Screening

First Published: May 18, 2001

Last Published: December 17, 2007

The RADIUS Attribute Screening feature allows users to configure a list of “accept” or “reject” RADIUS attributes on the network access server (NAS) for purposes such as authorization or accounting.

If a NAS accepts and processes *all* RADIUS attributes received in an Access-Accept packet, unwanted attributes may be processed, creating a problem for wholesale providers who do not control their customers’ authentication, authorization, and accounting (AAA) servers. For example, there may be attributes that specify services to which the customer has not subscribed, or there may be attributes that may degrade service for other wholesale dial users. The ability to configure the NAS to restrict the use of specific attributes has therefore become a requirement for many users.

The RADIUS Attribute Screening feature should be implemented in one of the following ways:

- To allow the NAS to accept and process all standard RADIUS attributes for a particular purpose, except for those on a configured reject list
- To allow the NAS to reject (filter out) all standard RADIUS attributes for a particular purpose, except for those on a configured accept list

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for RADIUS Attribute Screening” section on page 10](#).

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2001–2002, 2007 Cisco Systems, Inc. All rights reserved.

Contents

- [Prerequisites for RADIUS Attribute Screening, page 2](#)
- [Restrictions for RADIUS Attribute Screening, page 2](#)
- [Information About RADIUS Attribute Screening, page 3](#)
- [How to Screen RADIUS Attributes, page 3](#)
- [Configuration Examples for RADIUS Attribute Screening, page 6](#)
- [Command Reference, page 9](#)
- [Additional References, page 8](#)
- [Feature Information for RADIUS Attribute Screening, page 10](#)
- [Glossary, page 11](#)

Prerequisites for RADIUS Attribute Screening

Before configuring a RADIUS accept or reject list, you must enable AAA.

For more information, refer to the [AAA](#) chapters in the *Cisco IOS Security Configuration Guide*, Release 12.2.

Restrictions for RADIUS Attribute Screening

NAS Requirements

To enable this feature, your NAS should be configured for authorization with RADIUS groups.

Accept or Reject Lists Limitations

The two filters used to configure accept or reject lists are mutually exclusive; therefore, a user can configure only one access list or one reject list for each purpose, per server group.

Vendor-Specific Attributes

This feature does not support vendor-specific attribute (VSA) screening; however, a user can specify attribute 26 (Vendor-Specific) in an accept or reject list, which accepts or rejects all VSAs.

Required Attributes Screening Recommendation

It is recommended that users do not reject the following required attributes:

- For authorization:
 - 6 (Service-Type)
 - 7 (Framed-Protocol)
- For accounting:
 - 4 (NAS-IP-Address)
 - 40 (Acct-Status-Type)
 - 41 (Acct-Delay-Time)
 - 44 (Acct-Session-ID)

If an attribute is required, the rejection is refused, and the attribute is allowed to pass through.



Note

The user does not receive an error at the point of configuring a reject list for required attributes because the list does not specify a purpose—authorization or accounting. The server determines whether an attribute is required when it is known what the attribute is to be used for.

Information About RADIUS Attribute Screening

The RADIUS Attribute Screening feature provides the following benefits:

- Users can configure an accept or reject list consisting of a selection of attributes on the NAS for a specific purpose so unwanted attributes are not accepted and processed.
- Users may wish to configure an accept list that includes only relevant accounting attributes, thereby reducing unnecessary traffic and allowing users to customize their accounting data.

How to Screen RADIUS Attributes

The following sections describe how RADIUS attributes are screened and verified:

- [Configuring RADIUS Attribute Screening](#)
- [Verifying RADIUS Attribute Screening](#)

Configuring RADIUS Attribute Screening

To configure a RADIUS attribute accept or reject list for authorization or accounting, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authentication ppp default group *group-name***

4. **aaa authorization network default group** *group-name*
5. **aaa group server radius** *group-name*
6. **server** *ip-address*
7. **authorization** [**accept** | **reject**] *listname* - or - **accounting** [**accept** | **reject**] *listname*
8. **exit**
9. **radius-server host** {*hostname* | *ip-address*} [**key string**]
10. **radius-server attribute list** *listname*
11. **attribute** *value1* [*value2* [*value3...*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# aaa authentication ppp default group group-name	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
Step 4	Router(config)# aaa authorization network default group group-name	Sets parameters that restrict network access to the user.
Step 5	Router(config)# aaa group server radius group-name	Groups different RADIUS server hosts into distinct lists and distinct methods.
Step 6	Router(config-sg-radius)# server ip-address	Configures the IP address of the RADIUS server for the group server,
Step 7	Router(config-sg-radius)# authorization [accept reject] listname and/or Router(config-sg-radius)# accounting [accept reject] listname	Specifies a filter for the attributes that are returned in an Access-Accept packet from the RADIUS server. and/or Specifies a filter for the attributes that are to be sent to the RADIUS server in an accounting request. Note The accept keyword indicates that all attributes are rejected except for the attributes specified in the <i>listname</i> . The reject keyword indicates that all attributes are accepted except for the attributes specified in the <i>listname</i> and all standard attributes.
Step 8	Router(config-sg-radius)# exit	Exits server-group configuration mode.
Step 9	Router(config)# radius-server host {hostname ip-address} [key string]	Specifies a RADIUS server host.
Step 10	Router(config)# radius-server attribute list listname	Defines the list name given to the set of attributes defined in the attribute command. Note The <i>listname</i> must be the same as the <i>listname</i> defined in Step 5.
Step 11	Router(config-sg-radius)# attribute value1 [value2 [value3...]]	Adds attributes to the configured accept or reject list. Note This command can be used multiple times to add attributes to an accept or reject list.

Verifying RADIUS Attribute Screening

To verify an accept or reject list, use one of the following commands in privileged EXEC mode:

Command	Purpose
Router# debug aaa accounting	Displays information on accountable events as they occur.
Router# debug aaa authentication	Displays information on AAA authentication.
Router# show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.

Configuration Examples for RADIUS Attribute Screening

This section provides the following configuration examples:

- [Authorization Accept: Example](#)
- [Accounting Reject: Example](#)
- [Authorization Reject and Accounting Accept: Example](#)
- [Rejecting Required Attributes: Example](#)

Authorization Accept: Example

The following example shows how to configure an accept list for attribute 6 (Service-Type) and attribute 7 (Framed-Protocol); all other attributes (including VSAs) are rejected for RADIUS authorization.

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
    server 10.1.1.1
    authorization accept min-author
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list min-author
    attribute 6-7
```

Accounting Reject: Example

The following example shows how to configure a reject list for attribute 66 (Tunnel-Client-Endpoint) and attribute 67 (Tunnel-Server-Endpoint); all other attributes (including VSAs) are accepted for RADIUS accounting.

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
    server 10.1.1.1
    accounting reject tnl-x-endpoint
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list tnl-x-endpoint
    attribute 66-67
```


Authorization Reject and Accounting Accept: Example

The following example shows how to configure a reject list for RADIUS authorization and configure an accept list for RADIUS accounting. Although you cannot configure more than one accept or reject list per server group for authorization or accounting, you can configure one list for authorization and one list for accounting per server group.

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
    server 10.1.1.1
    authorization reject bad-author
    accounting accept usage-only
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list usage-only
    attribute 1,40,42-43,46
!
radius-server attribute list bad-author
    attribute 22,27-28,56-59
```

Rejecting Required Attributes: Example

The following example shows debug output for the **debug aaa accounting** command. In this example, required attributes 44, 40, and 41 have been added to the reject list “standard.”

Router# **debug aaa authorization**

```
AAA/ACCT(6): Accounting method=radius-sg (radius)
RADIUS: attribute 44 cannot be rejected
RADIUS: attribute 61 rejected
RADIUS: attribute 31 rejected
RADIUS: attribute 40 cannot be rejected
RADIUS: attribute 41 cannot be rejected
```

Additional References

The following sections provide references related to the RADIUS Attribute Screening feature.

Related Documents

Related Topic	Document Title
IOS security features	Cisco IOS Security Command Reference, Release 12.4T
	Cisco IOS Security Configuration Guide, Release 12.4
RADIUS	Configuring Radius

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this release.	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Command Reference

The following commands are introduced or modified in the feature or features documented in this module.

- [accounting](#) (server-group configuration)
- [authorization](#) (server-group configuration)
- [attribute](#) (server-group configuration)
- [radius-server attribute list](#)

For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

Feature Information for RADIUS Attribute Screening

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for RADIUS Attribute Screening

Feature Name	Releases	Feature Information
RADIUS Attribute Screening	12.2(1)DX 12.2(2)DD 12.2(4)B 12.2(4)T 12.2(13)T 12.2(33)SRC	<p>The RADIUS Attribute Screening feature allows users to configure a list of “accept” or “reject” RADIUS attributes on the network access server (NAS) for purposes such as authorization or accounting.</p> <p>This feature was introduced in 12.2(1)DX.</p> <p>This feature was integrated into Cisco IOS Release 12.2(2)DD.</p> <p>This feature was integrated into Cisco IOS Release 12.2(4)B.</p> <p>This feature was integrated into 12.2(4)T.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRC.</p> <p>Platform support was added for the Cisco 7401 ASR router.</p> <p>The Cisco 7200 series platform applies to the Cisco IOS Releases 12.2(1)DX, 12.2(2)DD, 12.2(4)B, 12.2(4)T, and 12.2(13)T.</p> <p>The Cisco 7401 ASR platform applies to Cisco IOS Release 12.2(13)T only.</p> <p>The following commands were introduced or modified by this feature: accounting (server-group configuration), authorization (server-group configuration), attribute (server-group configuration), radius-server attribute list</p>
RADIUS Attribute Value Screening	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Glossary

AAA—authentication, authorization, and accounting. Suite of network security services that provide the primary framework through which access control can be set up on your Cisco router or access server.

attribute—RADIUS Internet Engineering Task Force (IETF) attributes are the original set of 255 standard attributes that are used to communicate AAA information between a client and a server. Because IETF attributes are standard, the attribute data is predefined and well known; thus all clients and servers who exchange AAA information via IETF attributes must agree on attribute data such as the exact meaning of the attributes and the general bounds of the values for each attribute.

NAS—network access server. A Cisco platform (or collection of platforms, such as an AccessPath system) that interfaces between the packet world (for example, the Internet) and the circuit world (for example, the Public Switched Telephone Network).

RADIUS—Remote Authentication Dial-In User Service. RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

VSA—vendor-specific attribute. VSAs are derived from one IETF attribute—vendor-specific (attribute 26). Attribute 26 allows a vendor to create and implement an additional 255 attributes. That is, a vendor can create an attribute that does not match the data of any IETF attribute and encapsulate it behind attribute 26: essentially, Vendor-Specific = "protocol:attribute=value".

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2001–2002, 2007 Cisco Systems, Inc. All rights reserved.



RADIUS Centralized Filter Management

First Published: November 25, 2002

Last Updated: December 17, 2007

The RADIUS Centralized Filter Management feature introduces a filter-server to simplify ACL configuration and management. This filter-server serves as a centralized RADIUS repository and administration point, which users can centrally manage and configure access control list (ACL) filters.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for RADIUS Centralized Filter Management](#)” section on [page 10](#).

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for RADIUS Centralized Filter Management, page 2](#)
- [Restrictions for RADIUS Centralized Filter Management, page 2](#)
- [Information About RADIUS Centralized Filter Management, page 2](#)
- [How to Configure Centralized Filter Management for RADIUS, page 3](#)
- [Monitoring and Maintaining the Filter Cache, page 6](#)
- [Configuration Examples for RADIUS Centralized Filter Management, page 6](#)
- [Additional References, page 8](#)
- [Command Reference, page 9](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2002, 2006–2007 Cisco Systems, Inc. All rights reserved.

- [Feature Information for RADIUS Centralized Filter Management, page 10](#)

Prerequisites for RADIUS Centralized Filter Management

- You may need to add a dictionary file to your server if it does not support the new RADIUS VSAs. For a sample dictionary and vendors file, see the section “[RADIUS Dictionary and Vendors File: Example](#)” later in this document.
If you need to add a dictionary file, ensure that your RADIUS server is nonstandard and that it can send the newly introduced VSAs.
- You want to set up RADIUS network authentication so a remote user can dial in and get IP connectivity.

Restrictions for RADIUS Centralized Filter Management

Multiple method lists are not supported in this feature; only a single global filter method list can be configured.

Information About RADIUS Centralized Filter Management

Before the RADIUS Centralized Filter Management feature, wholesale providers (who provide premium charges for customer services such as access control lists [ACLs]) were unable to prevent customers from applying exhaustive ACLs, which could impact router performance and other customers. This feature introduces a centralized administration point—a filter server—for ACL management. The filter server acts as a centralized RADIUS repository for ACL configuration.

Whether or not the RADIUS server that is used as the filter server is the same server that is used for access authentication, the network access server (NAS) will initiate a second access request to the filter server. If configured, the NAS will use the filter-ID name as the authentication username and the filter server password for the second access request. The RADIUS server will attempt to authenticate the filter-ID name, returning any required filtering configuration in the access-accept response.

Because downloading ACLs is time consuming, a local cache is maintained on the NAS. If an ACL name exists on the local cache, that configuration will be used without consulting the filter server.



Note

An appropriately configured cache should minimize delays; however, the first dialin user to require a filter will always experience a longer delay because the ACL configuration is retrieved for the first time.

Cache Management

A global filter cache is maintained on the NAS of recently downloaded ACLs; thus, users no longer have to repeatedly request the same ACL configuration information from a potentially overloaded RADIUS server. Users are required to flush the cache when the following criteria have been met:

- After an entry becomes associated with a newly active call, the idle timer that is associated with that entry will be reset, if configured to do so.
- After the idle-time stamp of an entry expires, the entry will be removed.

- After the global cache of entries reaches a specified maximum number, the entry whose idle-timer is closest to the idle time limit will be removed.

A single timer is responsible for managing all cache entries. The timer is started after the first cache entry is created, and it runs periodically until reboot. The period of the timer will correspond to the minimum granularity offered when configuring cache idle timers, which is one expiration per minute. A single timer prevents users from having to manage individual timers per cache entry.

**Note**

The single timer introduces a lack of precision in timer expiration. There is an average error of approximately 50 percent of the timer granularity. Although decreasing the timer granularity will decrease the average error, the decreased timer granularity will negatively impact performance. Because precise timing is not required for cache management, the error delay should be acceptable.

New Vendor-Specific Attribute Support

This feature introduces support for three new vendor-specific attributes (VSAs), which can be divided into the following two categories:

- User profile extensions
 - Filter-Required (50)—Specifies whether the call should be permitted if the specified filter is not found. If present, this attribute will be applied after any authentication, authorization, and accounting (AAA) filter method-list.
- Pseudo-user profile extensions
 - Cache-Refresh (56)—Specifies whether cache entries should be refreshed each time an entry is referenced by a new session. This attribute corresponds to the **cache refresh** command.
 - Cache-Time (57)—Specifies the idle time out, in minutes, for cache entries. This attribute corresponds to the **cache clear age** command.

**Note**

All RADIUS attributes will override any command-line interface (CLI) configurations.

How to Configure Centralized Filter Management for RADIUS

Use the following sections to configure the Centralized Filter Management feature.

- [Configuring the RADIUS ACL Filter Server](#)
- [Configuring the Filter Cache](#)
- [Verifying the Filter Cache](#)

Configuring the RADIUS ACL Filter Server

To enable the RADIUS ACL filter server, use the following command in global configuration mode:

Command	Purpose
Router(config)# aaa authorization cache filterserver default <i>methodlist[methodlist2...]</i>	Enables AAA authorization caches and the downloading of an ACL configuration from a RADIUS filter server. <ul style="list-style-type: none"> default—The default authorization list. <i>methodlist [methodlist2...]</i>—One of the keywords listed on the password command page.

Configuring the Filter Cache

Follow the steps in this section to configure the AAA filter cache.

SUMMARY STEPS

- enable**
- configure terminal**
- aaa cache filter**
- password {0 | 7} password**
- cache disable**
- cache clear age minutes**
- cache refresh**
- cache max number**

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# aaa cache filter	Enables filter cache configuration and enters AAA filter configuration mode.

	Command	Purpose
Step 4	Router(config-aaa-filter)# password {0 7} <i>password</i>	(Optional) Specifies the optional password that is to be used for filter server authentication requests. 0—Specifies that an unencrypted password will follow. 7—Specifies that a hidden password will follow. <i>password</i> —The unencrypted (clear text) password. Note If a password is not specified, the default password (“cisco”) is enabled.
Step 5	Router(config-aaa-filter)# cache disable	(Optional) Disables the cache.
Step 6	Router(config-aaa-filter)# cache clear age <i>minutes</i>	(Optional) Specifies, in minutes, when cache entries expire and the cache is cleared. <i>minutes</i> —Any value between 0 to 4294967295. Note If a time is not specified, the default (1400 minutes [1 day]) is enabled.
Step 7	Router(config-aaa-filter)# cache refresh	(Optional) Refreshes a cache entry when a new session begins. This command is enabled by default. To disable this functionality, use the no cache refresh command.
Step 8	Router(config-aaa-filter)# cache max <i>number</i>	(Optional) Limits the absolute number of entries the cache can maintain for a particular server. <i>number</i> —The maximum number of entries the cache can contain. Any value between 0 to 4294967295. Note If a number is not specified, the default (100 entries) is enabled.

Verifying the Filter Cache

To display the cache status, use the **show aaa cache filterserver** EXEC command. The following is sample output for the **show aaa cache filterserver** command:

```
Router# show aaa cache filterserver
```

```

Filter      Server      Age Expires Refresh Access-Control-Lists
-----
aol         10.2.3.4      0    1440    100 ip in icmp drop
           ip out icmp drop
           ip out forward tcp dstip 1.2.3...
msn         10.3.3.4      N/A   Never    2 ip in tcp drop
msn2        10.4.3.4      N/A   Never    2 ip in tcp drop
vone        10.5.3.4      N/A   Never    0 ip in tcp drop

```



Note

The **show aaa cache filterserver** command shows how many times a particular filter has been referenced or refreshed. This function may be used in administration to determine which filters are actually being used.

Troubleshooting Tips

To help troubleshoot your filter cache configurations, use the privileged EXEC **debug aaa cache filterserver** command. To view sample output for the **debug aaa cache filterserver** command, refer to the section “[Debug Output: Example](#)” later in this document.

Monitoring and Maintaining the Filter Cache

To monitor and maintain filter caches, use at least one of the following EXEC commands:

Command	Purpose
Router# clear aaa cache filterserver acl [<i>filter-name</i>]	Clears the cache status for a particular filter or all filters.
Router# show aaa cache filterserver	Displays the cache status.

Configuration Examples for RADIUS Centralized Filter Management

This section provides the following configuration examples:

- [NAS Configuration: Example, page 6](#)
- [RADIUS Server Configuration: Example, page 7](#)
- [RADIUS Dictionary and Vendors File: Example, page 7](#)
- [Debug Output: Example, page 7](#)

NAS Configuration: Example

The following example shows how to configure the NAS for cache filtering. In this example, the server group “mygroup” is contacted first. If there is no response, the default RADIUS server will then be contacted. If there still is no response, the local filters are contacted. Finally, the call is accepted if the filter cannot be resolved.

```
aaa authorization cache filterserver group mygroup group radius local none
!
aaa group server radius mygroup
 server 10.2.3.4
 server 10.2.3.5
!
radius-server host 10.1.3.4
!
aaa cache filter
 password mycisco
 no cache refresh
 cache max 100
!
```

RADIUS Server Configuration: Example

The following example is a sample RADIUS configuration that is for a remote user “user1” dialing into the NAS:

```
myfilter Password = "cisco"
    Service-Type = Outbound,
    Ascend:Ascend-Call-Filter = "ip in drop srcip 10.0.0.1/32 dstip 10.0.0.10/32
    icmp",
    Ascend:Ascend-Call-Filter = "ip in drop srcip 10.0.0.1/32 dstip 10.0.0.10/32 tcp
    dstport = telnet",
    Ascend:Ascend-Cache-Refresh = Refresh-No,
    Ascend:Ascend-Cache-Time = 15

user1 Password = "cisco"
    Service-Type = Framed,
    Filter-Id = "myfilter",
    Ascend:Ascend-Filter-Required = Filter-Required-Yes,
```

RADIUS Dictionary and Vendors File: Example

The following example is a sample RADIUS dictionary file for the new VSAs. In this example, the dictionary file is for a Merit server.

```
dictionary file:
Ascend.attr Ascend-Filter-Required 50 integer (*, 0, NOENCAPS)
Ascend.attr Ascend-Cache-Refresh 56 integer (*, 0, NOENCAPS)
Ascend.attr Ascend-Cache-Time 57 integer (*, 0, NOENCAPS)

Ascend.value Ascend-Cache-Refresh Refresh-No 0
Ascend.value Ascend-Cache-Refresh Refresh-Yes 1

Ascend.value Ascend-Filter-Required Filter-Required-No 0
Ascend.value Ascend-Filter-Required Filter-Required-Yes 1

vendors file:
50 50
56 56
57 57
```

Debug Output: Example

The following is sample output from the **debug aaa cache filterserver** command:

```
Router# debug aaa cache filterserver

AAA/FLTSV: need "myfilter" (fetch), call 0x612DAC64
AAA/FLTSV: send req, call 0x612DAC50
AAA/FLTSV: method SERVER_GROUP myradius
AAA/FLTSV: recv reply, call 0x612DAC50 (PASS)
AAA/FLTSV: create cache
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: add attr "call-inacl"
AAA/FLTSV: skip attr "filter-cache-refresh"
AAA/FLTSV: skip attr "filter-cache-time"
AAA/CACHE: set "AAA filtserv cache" entry "myfilter" refresh? no
```

```

AAA/CACHE: set "AAA filtserv cache" entry "myfilter" cachetime 15
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: add attr to list "call-inacl" call 0x612DAC64
AAA/FLTSV: PASS call 0x612DAC64
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (0 entries)
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (1 entry)
AAA/CACHE: destroy "AAA filtserv cache" entry "myfilter"
AAA/CACHE: timer "AAA filtserv cache", next in 10 secs (0 entries)

```

Additional References

The following sections provide references related to RADIUS Centralized Filter Management.

Related Documents

Related Topic	Document Title
Configuring Authorization	“ Configuring Authorization ” chapter in the <i>Cisco IOS Security Configuration Guide</i>
Configuring RADIUS	“ Configuring RADIUS ” chapter in the <i>Cisco IOS Security Configuration Guide</i>
Authorization Commands	Cisco IOS Security Command Reference

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **aaa authorization cache filterserver**
- **aaa cache filter**
- **cache clear age**
- **cache disable**
- **cache refresh**
- **clear aaa cache filterserver acl**
- **debug aaa cache filterserver**
- **password**
- **show aaa cache filterserver**

Feature Information for RADIUS Centralized Filter Management

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for RADIUS Centralized Filter Management

Feature Name	Releases	Feature Information
RADIUS Centralized Filter Management	12.2(13)T 12.2(28)SB 12.2(33)SRC Cisco IOS XE Release 2.1	<p>The RADIUS Centralized Filter Management feature introduces a filter-server to simplify ACL configuration and management. This filter-server serves as a centralized RADIUS repository and administration point, which users can centrally manage and configure access control list (ACL) filters.</p> <p>This feature was introduced in Cisco IOS Release 12.2(13)T.</p> <p>This feature was integrated into Cisco IOS Release 12.2(28)SB.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRC.</p> <p>In Cisco IOS Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>The following commands were introduced or modified by this feature: aaa authorization cache filterserver, aaa cache filter, cache clear age, cache disable, cache refresh, clear aaa cache filterserver acl, debug aaa cache filterserver, password, show aaa cache filterserver.</p>

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2005–2007 Cisco Systems, Inc. All rights reserved.



RADIUS Debug Enhancements

Feature History

Release	Modification
12.2(11)T	This feature was introduced on the Cisco 1400 series, Cisco 1600 series, Cisco 1700 series, Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, Cisco 7100, Cisco 7200, Cisco 7500, Cisco AS5300, Cisco AS5800, Cisco Catalyst 5000, Cisco MC3810, and Cisco MGX8850 platforms.

This document describes the Remote Authentication Dial-In User Services (RADIUS) Debug Enhancements feature in Cisco IOS Release 12.2(11)T. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 2](#)
- [Supported Standards, MIBs, and RFCs, page 3](#)
- [Prerequisites, page 4](#)
- [Configuration Tasks, page 4](#)
- [Configuration Examples, page 7](#)
- [Command Reference, page 9](#)
- [Glossary, page 10](#)

Feature Overview

This document details the RADIUS Debug Enhancements feature. RADIUS is a distributed client/server system that provides the following functionality:

- secures networks against unauthorized access
- enables authorization of specific service limits
- provides accounting information so that services can be billed

In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

The **debug radius** command displays information associated with RADIUS. Prior to the RADIUS Debug Enhancements feature, **debug radius** output was available only in an expanded, hexadecimal string format, resulting in displays that were difficult to interpret and analyze. Moreover, attribute value displays were truncated, particularly for vendor-specific attributes (VSAs).

The new feature provides enhanced RADIUS display including the following:

- Packet dump in a more readable, user-friendly ASCII format than before
- Complete display of attribute values without truncation
- Ability to select a brief RADIUS **debug** output display

Benefits

- Provides RADIUS debug display in a user-friendly format
- Supports complete RADIUS debug information
- Provides the default display of packet dump in ASCII format
- Allows a compact debugging output option that is useful for high-traffic, operational environments

Restrictions

Only Internet Engineering Task Force (IETF) attributes and Cisco VSAs used in voice applications are supported. For unsupported attributes, “undebuggable” is displayed.

Related Features and Technologies

- Cisco IOS security
- RADIUS authentication, authorization, and accounting (AAA)
- Cisco Voice over IP (VoIP)

Related Documents

- [Configuration Guide for AAA Billing Features in Cisco Voice-Enabled Routers and Access Servers](#)
- [Cisco IOS Security Configuration Guide](#), Release 12.2, “Configuring RADIUS” chapter
- [RADIUS Vendor-Specific Attributes Voice Implementation Guide](#), Release 12.1
- [Cisco IOS Debug Command Reference](#), Release 12.2

Supported Platforms

- Cisco 1400 series
- Cisco 1600 series
- Cisco 1700 series
- Cisco 2500 series

- Cisco 2600 series
- Cisco 3600 series
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7500 series
- Cisco AS5300
- Cisco AS5800
- Cisco Catalyst 5000
- Cisco MC3810
- Cisco MGX8850

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

- Establish a working IP network. For more information about configuring IP, refer to the part “IP Overview,” and the “Configuring IP Addressing,” and “Configuring IP Services” chapters in the Cisco IOS Release 12.0 *Network Protocols Configuration Guide, Part 1*.
- Configure VoIP. For more information about configuring VoIP, refer to *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2.
- Configure the gateway as a RADIUS client. Refer to the chapter “Configuring the RADIUS Client Gateway” in the *RADIUS Vendor-Specific Attributes Voice Implementation Guide*, Release 12.1.
- Be familiar with IETF RFC 2138.

Configuration Tasks

See the following sections for configuration tasks for the RADIUS Debug Enhancements feature. Each task in the list is identified as either required or optional.

- [Configuring Default Debug ASCII Display](#) (optional)
- [Configuring Debug Display in Brief Format](#) (optional)
- [Configuring Debug Display in Hex Format](#) (optional)
- [Verifying the debug radius Command](#) (optional)

Configuring Default Debug ASCII Display

The complete ASCII format debug display with no truncation is enabled by default; no configuration tasks are required to enable this feature. To reenable the feature if it was disabled by using the **no debug radius** command, use the following command in privileged EXEC mode:

Command	Purpose
Router# debug radius	Enables RADIUS debugging output.

**Note**

Prior to Cisco IOS Release 12.2(11)T, the **debug radius** command enabled truncated debugging output in hexadecimal notation, rather than ASCII. To enable debugging output in hex format, use the **debug radius hex** command.

Configuring Debug Display in Brief Format

Debugging output is available in a compact output that displays only basic information. To enable this display option, use the following command in privileged EXEC mode:

Command	Purpose
Router# debug radius brief	Enables RADIUS debugging output displaying only the client/server interaction and minimum packet information.

Configuring Debug Display in Hex Format

Debugging output is available in hexadecimal notation. To enable this display option, use the following command in privileged EXEC mode:

Command	Purpose
Router# debug radius hex	Enables RADIUS debugging output in hexadecimal notation.

Verifying the debug radius Command

Use the **show debug** command to verify RADIUS output options.

```
5300# show debug
```

```
Radius protocol debugging is on
Radius packet hex dump debugging is on
5300_43#
17:26:52: RADIUS: ustruct sharecount=3
17:26:52: Radius: radius_port_info() success=0 radius_nas_port=1
17:26:52: RADIUS: Initial Transmit ISDN 0:D:23 id 10 10.0.0.0:1824, Accounting-Request,
len 361
17:26:52:      Attribute 4 6 01081D03
17:26:52:      Attribute 26 19 00000009020D4953444E20303A443A3233
17:26:52:      Attribute 61 6 00000000
17:26:52:      Attribute 1 12 34303835323734323036
17:26:52:      Attribute 30 7 3532393831
17:26:52:      Attribute 31 12 34303835323734323036
17:26:52:      Attribute 40 6 00000001
17:26:52:      Attribute 6 6 00000001
17:26:52:      Attribute 26 27 000000092115683332332D67772D69643D353330305F34332E
17:26:52:      Attribute 26 57
000000090133683332332D696E636F6D696E672D636F6E662D69643D3846334133313633204234393830303046
20302033424537314238
17:26:52:      Attribute 26 31
000000091A19683332332D63616C6C2D6F726967696E3D616E73776572
17:26:52:      Attribute 26 32
000000091B1A683332332D63616C6C2D747970653D54656C6570686F6E79
17:26:52:      Attribute 26 56
000000091932683332332D73657475702D74696D653D2A30393A32363A35322E3838302050535420536174204A
616E2031203230303030
17:26:52:      Attribute 26 48
00000009182A683332332D636F6E662D69643D3846334133313633204234393830303046203020334245373142
38
17:26:52:      Attribute 44 10 3030303030303035
17:26:52:      Attribute 41 6 00000000
17:26:52: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to 4085274206
17:26:52: RADIUS: Received from id 10 1.7.157.1:1824, Accounting-response, len 20
17:27:01: RADIUS: ustruct sharecount=3
17:27:01: Radius: radius_port_info() success=0 radius_nas_port=1
```

```

17:27:01: RADIUS: Initial Transmit ISDN 0:D:23 id 11 10.0.0.1:1823, Access-Request, len
173
17:27:01:      Attribute 4 6 01081D03
17:27:01:      Attribute 26 19 00000009020D4953444E20303A443A3233
17:27:01:      Attribute 61 6 00000000
17:27:01:      Attribute 1 8 313233343536
17:27:01:      Attribute 26 48
00000009182A683332332D636F6E662D69643D3846334133313633204234393830303046203020334245373142
38
17:27:01:      Attribute 31 12 34303835323734323036
17:27:01:      Attribute 2 18 C980D8D0E9A061B3D783C61AA6F27214
17:27:01:      Attribute 26 36
00000009011E683332332D6976722D6F75743D7472616E73616374696F6E49443A33
17:27:01: RADIUS: Received from id 11 1.7.157.1:1823, Access-Accept, len 115
17:27:01:      Attribute 6 6 00000001
17:27:01:      Attribute 26 29 000000096517683332332D6372656469742D616D6F756E743D3435
17:27:01:      Attribute 26 27 000000096615683332332D6372656469742D74696D653D3333
17:27:01:      Attribute 26 26 000000096714683332332D72657475726E2D636F64653D30
17:27:01:      Attribute 25 7 6C6F63616C
17:27:01: RADIUS: saved authorization data for user 61AA0698 at 6215087C
17:27:09: %ISDN-6-DISCONNECT: Interface Serial0:22 disconnected from 4085554206 , call
lasted 17 seconds
17:27:09: RADIUS: ustruct sharecount=2
17:27:09: Radius: radius_port_info() success=0 radius_nas_port=1
17:27:09: RADIUS: Sent class "local" at 621508E8 from user 61AA0698
17:27:09: RADIUS: Initial Transmit ISDN 0:D:23 id 12 10.0.0.0:1824, Accounting-Request,
len 776
17:27:09:      Attribute 4 6 01081D03
17:27:09:      Attribute 26 19 00000009020D4953444E20303A443A3233
17:27:09:      Attribute 61 6 00000000
17:27:09:      Attribute 1 8 313233343536
17:27:09:      Attribute 30 7 3532393831
17:27:09:      Attribute 31 12 34303835323734323036
17:27:09:      Attribute 40 6 00000002
17:27:09:      Attribute 25 7 6C6F63616C
17:27:09:      Attribute 45 6 00000001
17:27:09:      Attribute 6 6 00000001
17:27:09:      Attribute 26 27 000000092115683332332D67772D69643D353330305F34332E
17:27:09:      Attribute 26 57
000000090133683332332D696E636F6D696E672D636F6E662D69643D3846334133313633204234393830303046
20302033424537314238
17:27:09:      Attribute 26 31
000000091A19683332332D63616C6C2D6F726967696E3D616E73776572
17:27:09:      Attribute 26 32
000000091B1A683332332D63616C6C2D747970653D54656C6570686F6E79
17:27:09:      Attribute 26 56
000000091932683332332D73657475702D74696D653D2A30393A32363A35322E3838302050535420536174204A
616E20312032303030
17:27:09:      Attribute 26 58
000000091C34683332332D636F6E6E6563742D74696D653D2A30393A32363A35322E3930372050535420536174
204A616E20312032303030
17:27:09:      Attribute 26 61
000000091D37683332332D646973636F6E6E6563742D74696D653D2A30393A32373A31302E3133372050535420
536174204A616E20312032303030
17:27:09:      Attribute 26 32
000000091E1A683332332D646973636F6E6E6563742D63617573653D3130
17:27:09:      Attribute 26 28 000000091F16683332332D766F6963652D7175616C6974793D30
17:27:09:      Attribute 26 48
00000009182A683332332D636F6E662D69643D3846334133313633204234393830303046203020334245373142
38
17:27:09:      Attribute 44 10 3030303030303035
17:27:09:      Attribute 42 6 00000000
17:27:09:      Attribute 43 6 00012CA0
17:27:09:      Attribute 47 6 00000000

```



```

17:27:09:      Attribute 48 6 000001E1
17:27:09:      Attribute 46 6 00000011
17:27:09:      Attribute 26 30 000000090118737562736372696265723D526567756C61724C696E65
17:27:09:      Attribute 26 35
00000009011D683332332D6976722D6F75743D5461726966663A556E6B6E6F776E
17:27:09:      Attribute 26 22 0000000901107072652D62797465732D696E3D30
17:27:09:      Attribute 26 23 0000000901117072652D62797465732D6F75743D30
17:27:09:      Attribute 26 21 00000009010F7072652D70616B732D696E3D30
17:27:09:      Attribute 26 22 0000000901107072652D70616B732D6F75743D30
17:27:09:      Attribute 26 22 0000000901106E61732D72782D73706565643D30
17:27:09:      Attribute 26 22 0000000901106E61732D74782D73706565643D30
17:27:09:      Attribute 41 6 00000000
17:27:09: RADIUS: Received from id 12 10.0.0.0:1824, Accounting-response, len 20

```

Configuration Examples

This section provides the following configuration examples:

- [Default debug radius Command Example](#)
- [Compact Debugging Output Example](#)

Default debug radius Command Example

The following sample output shows the default RADIUS output in ASCII notation, generated by the **debug radius** command:



Note

The following output displays the internal information that is found inside a RADIUS protocol message. For more information about RADIUS protocol messages, see IETF RFC 2138.

```

router# debug radius

Radius protocol debugging is on
Radius packet hex dump debugging is off
router#
00:02:50: RADIUS: ustruct sharecount=3
00:02:50: Radius: radius_port_info() success=0 radius_nas_port=1
00:02:50: RADIUS: Initial Transmit ISDN 0:D:23 id 0 10.0.0.0:1824, Accounting-Request, len
358
00:02:50: RADIUS: NAS-IP-Address [4] 6 10.0.0.1
00:02:50: RADIUS: Vendor, Cisco [26] 19 VT=02 TL=13 ISDN 0:D:23
00:02:50: RADIUS: NAS-Port-Type [61] 6 Async
00:02:50: RADIUS: User-Name [1] 12 "4085274206"
00:02:50: RADIUS: Called-Station-Id [30] 7 "52981"
00:02:50: RADIUS: Calling-Station-Id [31] 12 "4085554206"
00:02:50: RADIUS: Acct-Status-Type [40] 6 Start
00:02:50: RADIUS: Service-Type [6] 6 Login
00:02:50: RADIUS: Vendor, Cisco [26] 27 VT=33 TL=21 h323-gw-id=5300_43.
00:02:50: RADIUS: Vendor, Cisco [26] 55 VT=01 TL=49 h323-incoming-conf-id=8F3A3163
B4980003 0 29BD0
00:02:50: RADIUS: Vendor, Cisco [26] 31 VT=26 TL=25 h323-call-origin=answer
00:02:50: RADIUS: Vendor, Cisco [26] 32 VT=27 TL=26 h323-call-type=Telephony
00:02:50: RADIUS: Vendor, Cisco [26] 57 VT=25 TL=51 h323-setup-time=*16:02:48.681 PST Fri
Dec 31 1999
00:02:50: RADIUS: Vendor, Cisco [26] 46 VT=24 TL=40 h323-conf-id=8F3A3163 B4980003 029BD0
00:02:50: RADIUS: Acct-Session-Id [44] 10 "00000002"
00:02:50: RADIUS: Delay-Time [41] 6 0

```

```

00:02:51: RADIUS: Received from id 0 10.0.0.0:1824, Accounting-response, len 20
00:02:51: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to 4085554206
00:03:01: RADIUS: ustruct sharecount=3
00:03:01: Radius: radius_port_info() success=0 radius_nas_port=1
00:03:01: RADIUS: Initial Transmit ISDN 0:D:23 id 1 1.7.157.1:1823, Access-Request, len
171
00:03:01: RADIUS: NAS-IP-Address [4] 6 10.0.0.1
00:03:01: RADIUS: Vendor, Cisco [26] 19 VT=02 TL=13 ISDN 0:D:23
00:03:01: RADIUS: NAS-Port-Type [61] 6 Async
00:03:01: RADIUS: User-Name [1] 8 "123456"
00:03:01: RADIUS: Vendor, Cisco [26] 46 VT=24 TL=40 h323-conf-id=8F3A3163 B4980003 0 29BD0
00:03:01: RADIUS: Calling-Station-Id [31] 12 "4085274206"
00:03:01: RADIUS: User-Password [2] 18 *
00:03:01: RADIUS: Vendor, Cisco [26] 36 VT=01 TL=30 h323-ivr-out=transactionID:0
00:03:01: RADIUS: Received from id 1 1.7.157.1:1823, Access-Accept, len 115
00:03:01: RADIUS: Service-Type [6] 6 Login
00:03:01: RADIUS: Vendor, Cisco [26] 29 VT=101 TL=23 h323-credit-amount=45
00:03:01: RADIUS: Vendor, Cisco [26] 27 VT=102 TL=21 h323-credit-time=33
00:03:01: RADIUS: Vendor, Cisco [26] 26 VT=103 TL=20 h323-return-code=0
00:03:01: RADIUS: Class [25] 7 6C6F63616C
00:03:01: RADIUS: saved authorization data for user 62321E14 at 6233D258
00:03:13: %ISDN-6-DISCONNECT: Interface Serial0:22 disconnected from 4085274206, call
lasted 22 seconds
00:03:13: RADIUS: ustruct sharecount=2
00:03:13: Radius: radius_port_info() success=0 radius_nas_port=1
00:03:13: RADIUS: Sent class "local" at 6233D2C4 from user 62321E14
00:03:13: RADIUS: Initial Transmit ISDN 0:D:23 id 2 10.0.0.0:1824, Accounting-Request, len
775
00:03:13: RADIUS: NAS-IP-Address [4] 6 10.0.0.1
00:03:13: RADIUS: Vendor, Cisco [26] 19 VT=02 TL=13 ISDN 0:D:23
00:03:13: RADIUS: NAS-Port-Type [61] 6 Async
00:03:13: RADIUS: User-Name [1] 8 "123456"
00:03:13: RADIUS: Called-Station-Id [30] 7 "52981"
00:03:13: RADIUS: Calling-Station-Id [31] 12 "4085554206"
00:03:13: RADIUS: Acct-Status-Type [40] 6 Stop
00:03:13: RADIUS: Class [25] 7 6C6F63616C
00:03:13: RADIUS: Undebuggable [45] 6 00000001
00:03:13: RADIUS: Service-Type [6] 6 Login
00:03:13: RADIUS: Vendor, Cisco [26] 27 VT=33 TL=21 h323-gw-id=5300_43.
00:03:13: RADIUS: Vendor, Cisco [26] 55 VT=01 TL=49 h323-incoming-conf-id=8F3A3163
B4980003 0 29BD0
00:03:13: RADIUS: Vendor, Cisco [26] 31 VT=26 TL=25 h323-call-origin=answer
00:03:13: RADIUS: Vendor, Cisco [26] 32 VT=27 TL=26 h323-call-type=Telephony
00:03:13: RADIUS: Vendor, Cisco [26] 57 VT=25 TL=51 h323-setup-time=*16:02:48.681 PST Fri
Dec 31 1999
00:03:13: RADIUS: Vendor, Cisco [26] 59 VT=28 TL=53 h323-connect-time=*16:02:48.946
PST Fri Dec 31 1999
00:03:13: RADIUS: Vendor, Cisco [26] 62 VT=29 TL=56 h323-disconnect-time=*16:03:11.306
PST Fri Dec 31 1999
00:03:13: RADIUS: Vendor, Cisco [26] 32 VT=30 TL=26 h323-disconnect-cause=10
00:03:13: RADIUS: Vendor, Cisco [26] 28 VT=31 TL=22 h323-voice-quality=0
00:03:13: RADIUS: Vendor, Cisco [26] 46 VT=24 TL=40 h323-conf-id=8F3A3163 B4980003 0 29BD0
00:03:13: RADIUS: Acct-Session-Id [44] 10 "00000002"
00:03:13: RADIUS: Acct-Input-Octets [42] 6 0
00:03:13: RADIUS: Acct-Output-Octets [43] 6 88000
00:03:13: RADIUS: Acct-Input-Packets [47] 6 0
00:03:13: RADIUS: Acct-Output-Packets [48] 6 550
00:03:13: RADIUS: Acct-Session-Time [46] 6 22
00:03:13: RADIUS: Vendor, Cisco [26] 30 VT=01 TL=24 subscriber=RegularLine
00:03:13: RADIUS: Vendor, Cisco [26] 35 VT=01 TL=29 h323-ivr-out=Tariff:Unknown
00:03:13: RADIUS: Vendor, Cisco [26] 22 VT=01 TL=16 pre-bytes-in=0
00:03:13: RADIUS: Vendor, Cisco [26] 23 VT=01 TL=17 pre-bytes-out=0
00:03:13: RADIUS: Vendor, Cisco [26] 21 VT=01 TL=15 pre-paks-in=0
00:03:13: RADIUS: Vendor, Cisco [26] 22 VT=01 TL=16 pre-paks-out=0

```

```
00:03:13: RADIUS: Vendor, Cisco [26] 22 VT=01 TL=16 nas-rx-speed=0
00:03:13: RADIUS: Vendor, Cisco [26] 22 VT=01 TL=16 nas-tx-speed=0
00:03:13: RADIUS: Delay-Time [41] 6 0
00:03:13: RADIUS: Received from id 2 10.0.0.0:1824, Accounting-response, len 20
```

Compact Debugging Output Example

A new EXEC command, **debug radius brief**, enables this abbreviated output option. The following sample output displays only the client/server interaction and minimum packet information (packet type, ID and so forth).

```
router# debug radius brief
```

```
Radius protocol debugging is on
Radius packet hex dump debugging is off
Radius protocol in brief format debugging is on
00:05:21: RADIUS: Initial Transmit ISDN 0:D:23 id 6 10.0.0.1:1824, Accounting-Request, len
358
00:05:21: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to 4085554206
00:05:26: RADIUS: Retransmit id 6
00:05:31: RADIUS: Tried all servers.
00:05:31: RADIUS: No valid server found. Trying any viable server
00:05:31: RADIUS: Tried all servers.
00:05:31: RADIUS: No response for id 7
00:05:31: RADIUS: Initial Transmit ISDN 0:D:23 id 8 10.0.0.0:1823, Access-Request, len 171
00:05:36: RADIUS: Retransmit id 8
00:05:36: RADIUS: Received from id 8 10.0.0.0:1823, Access-Accept, len 115
00:05:47: %ISDN-6-DISCONNECT: Interface Serial0:22 disconnected from 4085554206, call
lasted 26 seconds
00:05:47: RADIUS: Initial Transmit ISDN 0:D:23 id 9 10.0.0.1:1824, Accounting-Request, len
775
00:05:47: RADIUS: Received from id 9 1.7.157.1:1824, Accounting-response, len 20
```

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug radius**

Glossary

AAA — authentication, authorization, and accounting. Pronounced “triple a.”

ASCII — American Standard Code for Information Interchange. 8-bit code for character representation (7 bits plus parity).

attribute — Form of information items provided by the X.500 Directory Service. The directory information base consists of entries, each containing one or more attributes. Each attribute consists of a type identifier together with one or more values.

IETF — Internet Engineering Task Force. Task force consisting of over 80 working groups responsible for developing Internet standards. The IETF operates under the auspices of ISOC.

RADIUS — Remote Authentication Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time.

VoIP — Voice over IP. The capability to carry normal telephony-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network. In VoIP, the DSP segments the voice signal into frames, which then are coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323.

VSA — vendor-specific attribute. An attribute that has been implemented by a particular vendor. It uses the attribute Vendor-Specific to encapsulate the resulting AV pair: essentially, Vendor-Specific = protocol:attribute = value.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



RADIUS Logical Line ID

First Published: November 25, 2002

Last Updated: December 17, 2007

The RADIUS Logical Line ID feature, also known as the Logical Line Identification (LLID) Blocking feature enables administrators to track their customers on the basis of the physical lines on which customer calls originate. Administrators use a virtual port that does not change as customers move from one physical line to another. This virtual port facilitates the maintenance of the administrator's customer profile database and allows the administrator to do additional security checks on customers.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for RADIUS Logical Line ID” section on page 9](#).

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for RADIUS Logical Line ID, page 2](#)
- [Restrictions for RADIUS Logical Line ID, page 2](#)
- [Information About RADIUS Logical Line ID, page 2](#)
- [How to Configure RADIUS Logical Line ID, page 3](#)
- [Configuration Examples for RADIUS Logical Line ID, page 5](#)
- [Additional References, page 7](#)
- [Command Reference, page 8](#)
- [Feature Information for RADIUS Logical Line ID, page 9](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2002, 2003, 2005–2007 Cisco Systems, Inc. All rights reserved.

- [Glossary, page 11](#)

Prerequisites for RADIUS Logical Line ID

Although this feature can be used with any RADIUS server, some RADIUS servers may require modifications to their dictionary files to allow the Calling-Station-ID attribute to be returned in Access-Accept messages. For example, the Merit RADIUS server does not support LLID downloading unless you modify its dictionary as follows: “ATTRIBUTE Calling-Station-Id 31 string (*, *)”

Restrictions for RADIUS Logical Line ID

The RADIUS Logical Line ID feature supports RADIUS only. TACACS+ is not supported.

This feature can be applied only toward PPP over Ethernet over ATM (PPPoEoATM) and PPP over Ethernet over VLAN (PPPoEoVLAN) (Dot1Q) calls; no other calls, such as ISDN, can be used.

Information About RADIUS Logical Line ID

LLID is an alphanumeric string (which must be a minimum of one character and a maximum of 253 characters) that is a logical identification of a subscriber line. LLID is maintained in a customer profile database on a RADIUS server. When the customer profile database receives a preauthorization request from the access router, the RADIUS server sends the LLID to the router as the Calling-Station-ID attribute (attribute 31).

The Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) sends a preauthorization request to the customer profile database when the LAC is configured for preauthorization. Configure the LAC for preauthorization using the **subscriber access** command.



Note

Downloading the LLID is referred to as “preauthorization” because it occurs before either service (domain) authorization or user authentication and authorization occur.

The customer profile database on the RADIUS server consists of user profiles for each physical network access server (NAS) port that is connected to the router. Each user profile contains a profile matched to a username (attribute 1) representing the physical port on the router. When the router is configured for preauthorization, it queries the customer profile database using a username representative of the physical NAS port making the connection to the router. When a match is found in the customer profile database, the customer profile database returns an Access-Accept message containing the LLID in the user profile. The LLID is defined in the Access-Accept record as the Calling-Station-ID attribute.

The preauthorization process can also provide the real username being used for authentication to the RADIUS server. Because the physical NAS port information is being used as the username (attribute 1), RADIUS attribute 77 (Connect-Info) can be configured to contain the authentication username. This configuration allows the RADIUS server to provide additional validation on the authorization request if it chooses, such as analyzing the username for privacy rules, before returning an LLID back to the router.

How to Configure RADIUS Logical Line ID

See the following sections for configuration tasks for the RADIUS Logical Line ID feature. Each task in the list is identified as either required or optional.

- [Configuring Preauthorization, page 3](#) (required)
- [Configuring the LLID in a RADIUS User Profile, page 4](#) (required)
- [Verifying Logical Line ID, page 4](#) (optional)

Configuring Preauthorization

To download the LLID and configure the LAC for preauthorization, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip radius source-interface** *interface-name*
4. **subscriber access {pppoe | pppoa} pre-authorize nas-port-id [default | list-name][send username]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip radius source-interface <i>interface-name</i> Example: Router (config)# ip radius source-interface Loopback1	Specifies the IP address portion of the username for the preauthorization request.
Step 4	subscriber access {pppoe pppoa} pre-authorize nas-port-id [default list-name][send username] Example: Router (config)# subscriber access pppoe pre-authorize nas-port-id mlist_llid send username	Enables the LLID to be downloaded so the router can be configured for preauthorization. The send username option specifies that you include the authentication username of the session inside the Connect-Info (attribute 77) in the Access-Request message.

Configuring the LLID in a RADIUS User Profile

To configure the user profile for preauthorization, add a NAS port user to the customer profile database and add RADIUS Internet Engineering Task Force (IETF) attribute 31 (Calling-Station-ID) to the user profile.

SUMMARY STEPS

1. `UserName=nas_port: ip-address:slot/module/port/vpi.vci`
2. `UserName=nas-port: ip-address:slot/module/port/vlan-id`
3. `Calling-Station-Id = "string (*,*)"`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>UserName=nas_port: ip-address:slot/module/port/vpi.vci</code>	(Optional) Adds a PPPoE over ATM NAS port user.
Step 2	<code>User-Name=nas-port: ip-address:slot/module/port/vlan-id</code>	(Optional) Adds a PPPoE over VLAN NAS port user.
Step 3	<code>Calling-Station-Id = "string (*,*)"</code>	Adds attribute 31 to the user profile. <ul style="list-style-type: none"> • String—One or more octets, containing the phone number from which the user placed the call.

Verifying Logical Line ID

To verify feature functionality, perform the following steps.

SUMMARY STEPS

1. `enable`
2. `debug radius`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: <code>Router> enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<code>debug radius</code> Example: <code>Router# debug radius</code>	Checks to see that RADIUS attribute 31 is the LLID in the Accounting-Request on LAC and in the Access-Request and Accounting-Request on the LNS.

Configuration Examples for RADIUS Logical Line ID

This section provides the following configuration examples:

- [LAC for Preauthorization Configuration: Example, page 5](#)
- [RADIUS User Profile for LLID: Example, page 6](#)

LAC for Preauthorization Configuration: Example

The following example shows how to configure your LAC for preauthorization by downloading the LLID:

```
aaa new-model
aaa group server radius sg_llid
  server 172.31.164.106 auth-port 1645 acct-port 1646
aaa group server radius sg_water
  server 172.31.164.106 auth-port 1645 acct-port 1646
aaa authentication ppp default group radius
aaa authorization cfg-commands
aaa authorization network default group sg_water
aaa authorization network mlist_llid group sg_llid
aaa session-id common
!
username s7200_2 password 0 lab
username s5300 password 0 lab
username sg_water password 0 lab
vpdn enable
!
vpdn-group 2
  request-dialin
  protocol l2tp
  domain water.com
  domain water.com#184
  initiate-to ip 10.1.1.1
  local name s7200_2
  l2tp attribute clid mask-method right * 255 match #184
!
vpdn-group 3
  accept dialin
  protocol pppoe
  virtual-template 1
!
! Enable the LLID to be downloaded.
subscriber access pppoe pre-authorize nas-port-id mlist_llid send username
!
interface Loopback0
  ip address 10.1.1.2 255.255.255.0
!
interface Loopback1
  ip address 10.1.1.1 255.255.255.0
!
interface Ethernet1/0
  ip address 10.1.1.8 255.255.255.0 secondary
  ip address 10.0.58.111 255.255.255.0
  no cdp enable
!
interface ATM4/0
  no ip address
  no atm ilmi-keepalive
!
```

```

interface ATM4/0.1 point-to-point
 pvc 1/100
  encapsulation aal5snap
  protocol pppoe
!
interface virtual-template1
 no ip unnumbered Loopback0
 no peer default ip address
 ppp authentication chap
!
radius-server host 172.31.164.120 auth-port 1645 acct-port 1646 key rad123
radius-server host 172.31.164.106 auth-port 1645 acct-port 1646 key rad123
ip radius source-interface Loopback1

```

RADIUS User Profile for LLID: Example

The following example shows how to configure the user profile for LLID querying for PPPoEoVLAN and PPPoEoATM and how to add attribute 31:

```

pppoeovlan
-----
nas-port:10.1.0.3:6/0/0/0 Password = "cisco",
  Service-Type = Outbound,
  Calling-Station-ID = "cat-example"

pppoeoa
-----
nas-port:10.1.0.3:6/0/0/1.100 Password = "cisco",
  Service-Type = Outbound,
  Calling-Station-ID = "cat-example"

```

Additional References

The following sections provide references related to RADIUS Logical Line ID.

Related Documents

Related Topic	Document Title
AAA authentication	“Configuring AAA Preauthentication” section in the “Configuring RADIUS” chapter in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4
Attribute screening for access requests	“RADIUS Attribute Screening” section in the “Configuring RADIUS” chapter in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4
Broadband access: PPP and routed bridge encapsulation	“Configuring Broadband Access: PPP and Routed Bridge Encapsulation” chapter in the <i>Cisco IOS Wide-Area Networking Configuration Guide</i> , Release 12.2
Dial technologies	<i>Cisco IOS Dial Technologies Configuration Guide</i> , Release 12.4

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **subscriber access**

Feature Information for RADIUS Logical Line ID

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for RADIUS Logical Line ID

Feature Name	Releases	Feature Information
RADIUS Logical Line ID	12.2(13)T 12.2(15)B 12.3(14)YM1 12.4(2)T 12.3(14)YM2 12.2(28)SB 12.2(31)SB2 12.2(33)SRC	<p>The RADIUS Logical Line ID feature, also known as the Logical Line Identification (LLID) Blocking feature enables administrators to track their customers on the basis of the physical lines on which customer calls originate.</p> <p>This feature was introduced in Cisco IOS Release 12.2(13)T.</p> <p>This feature was integrated into Cisco IOS Release 12.2(15)B.</p> <p>This feature was integrated into Cisco IOS Release 12.3(14)YM1, and the send username keyword was added to the subscriber access command.</p> <p>This feature was integrated into Cisco IOS Release 12.4(2)T.</p> <p>This feature was integrated into Cisco IOS Release 12.3(14)YM2.</p> <p>This feature was integrated into Cisco IOS Release 12.2(28)SB.</p> <p>This feature was integrated into Cisco IOS Release 12.2(31)SB2.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRC.</p> <p>The subscriber access command was introduced by this feature.</p>
Calling Station ID Attribute 31	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Table 1 **Feature Information for RADIUS Logical Line ID**

Feature Name	Releases	Feature Information
LLID Blocking	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
RADIUS Logical Line ID	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Glossary

LLID Blocking—A feature that enables administrators to track their customers on the basis of the physical lines on which the calls of the customers originate. Also known as RADIUS Logical Line ID.

RADIUS Logical Line ID—A feature that enables administrators to track their customers on the basis of the physical lines on which the calls of the customers originate. Also known as LLID Blocking.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2002, 2003, 2005–2007 Cisco Systems, Inc. All rights reserved.



RADIUS NAS-IP-Address Attribute Configurability

First Published: November 19, 2003

Last Updated: December 3, 2007

The RADIUS NAS-IP-Address Attribute Configurability feature allows an arbitrary IP address to be configured and used as RADIUS attribute 4, NAS-IP-Address, without changing the source IP address in the IP header of the RADIUS packets. This feature may be used for situations in which service providers are using a cluster of small network access servers (NASs) to simulate a large NAS to improve scalability. This feature allows the NASs to behave as a single RADIUS client from the perspective of the RADIUS server.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for RADIUS NAS-IP-Address Attribute Configurability” section on page 8](#).

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for RADIUS NAS-IP-Address Attribute Configurability, page 2](#)
- [Restrictions for RADIUS NAS-IP-Address Attribute Configurability, page 2](#)
- [Information About RADIUS NAS-IP-Address Attribute Configurability, page 2](#)
- [How to Configure RADIUS NAS-IP-Address Attribute Configurability, page 3](#)
- [Configuration Examples for RADIUS NAS-IP-Address Attribute Configurability, page 5](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2003–2004, 2006–2007 Cisco Systems, Inc. All rights reserved.

- [Additional References, page 6](#)
- [Command Reference, page 7](#)
- [Feature Information for RADIUS NAS-IP-Address Attribute Configurability, page 8](#)

Prerequisites for RADIUS NAS-IP-Address Attribute Configurability

The following requirements are necessary before configuring this feature:

- Experience with IP Security (IPSec) and configuring both RADIUS servers and authentication, authorization, and accounting (AAA) is necessary.
- RADIUS server and AAA lists must be configured.

Restrictions for RADIUS NAS-IP-Address Attribute Configurability

The following restrictions apply if a cluster of RADIUS clients are being used to simulate a single RADIUS client for scalability. Solutions, or workarounds, to the restrictions are also provided.

- RADIUS attribute 44, Acct-Session-Id, may overlap among sessions from different NASs.

There are two solutions. Either the **radius-server attribute 44 extend-with-addr** or **radius-server unique-ident** command can be used on NAS routers to specify different prepending numbers for different NAS routers.

- RADIUS server-based IP address pool for different NASs must be managed.

The solution is to configure different IP address pool profiles for different NASs on the RADIUS server. Different NASs use different pool usernames to retrieve them.

- RADIUS request message for sessions from different NASs must be differentiated.

One of the solutions is to configure different format strings for RADIUS attribute 32, NAS-Identifier, using the **radius-server attribute 32 include-in-access-req** command on different NASs.

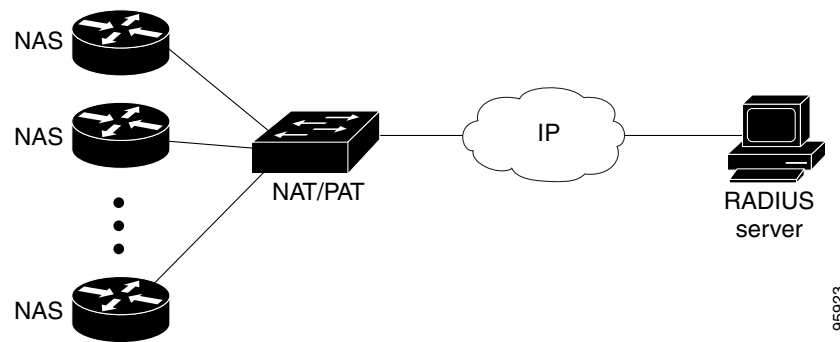
Information About RADIUS NAS-IP-Address Attribute Configurability

To simulate a large NAS RADIUS client using a cluster of small NAS RADIUS clients, as shown in [Figure 1](#), a Network Address Translation (NAT) or Port Address Translation (PAT) device is inserted in a network. The device is placed between a cluster of NASs and the IP cloud that is connected to a RADIUS server. When RADIUS traffic from different NASs goes through the NAT or PAT device, the source IP addresses of the RADIUS packets are translated to a single IP address, most likely an IP address on a loopback interface on the NAT or PAT device. Different User Datagram Protocol (UDP) source ports are assigned to RADIUS packets from different NASs. When the RADIUS reply comes

back from the server, the NAT or PAT device receives it, uses the destination UDP port to translate the destination IP address back to the IP address of the NAS, and forwards the reply to the corresponding NAS.

Figure 1 demonstrates how the source IP addresses of several NASs are translated to a single IP address as they pass through the NAT or PAT device on the way to the IP cloud.

Figure 1 NAS Addresses Translated to a Single IP Address



RADIUS servers normally check the source IP address in the IP header of the RADIUS packets to track the source of the RADIUS requests and to maintain security. The NAT or PAT solution satisfies these requirements because only a single source IP address is used even though RADIUS packets come from different NAS routers.

However, when retrieving accounting records from the RADIUS database, some billing systems use RADIUS attribute 4, NAS-IP-Address, in the accounting records. The value of this attribute is recorded on the NAS routers as their own IP addresses. The NAS routers are not aware of the NAT or PAT that runs between them and the RADIUS server; therefore, different RADIUS attribute 4 addresses will be recorded in the accounting records for users from the different NAS routers. These addresses eventually expose different NAS routers to the RADIUS server and to the corresponding billing systems.

Using the RADIUS NAS-IP-Address Attribute Configurability Feature

The RADIUS NAS-IP-Address Attribute Configurability feature allows you to freely configure an arbitrary IP address as RADIUS NAS-IP-Address, RADIUS attribute 4. By manually configuring the same IP address, most likely the IP address on the loopback interface of the NAT or PAT device, for all the routers, you can hide a cluster of NAS routers behind the NAT or PAT device from the RADIUS server.

How to Configure RADIUS NAS-IP-Address Attribute Configurability

This section contains the following procedures:

- [Configuring RADIUS NAS-IP-Address Attribute Configurability, page 4](#)
- [Monitoring and Maintaining RADIUS NAS-IP-Address Attribute Configurability, page 4](#)

Configuring RADIUS NAS-IP-Address Attribute Configurability

Before configuring the RADIUS NAS-IP-Address Attribute Configurability feature, you must have configured the RADIUS servers or server groups and AAA method lists.

To configure the RADIUS NAS-IP-Address Attribute Configurability feature, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute 4 ip-address**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	radius-server attribute 4 ip-address Example: Router (config)# radius-server attribute 4 10.2.1.1	Configures an IP address to be used as the RADIUS NAS-IP-Address, attribute 4.

Monitoring and Maintaining RADIUS NAS-IP-Address Attribute Configurability

To monitor the RADIUS attribute 4 address that is being used inside the RADIUS packets, use the **debug radius** command.

SUMMARY STEPS

1. **enable**
2. **debug radius**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example: Router> enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	debug radius	Displays information associated with RADIUS.
	Example: Router# debug radius	

Examples

The following sample output is from the **debug radius** command:

```
Router# debug radius

RADIUS/ENCODE(0000001C): acct_session_id: 29
RADIUS(0000001C): sending
RADIUS(0000001C): Send Access-Request to 10.0.0.10:1645 id 21645/17, len 81
RADIUS: authenticator D0 27 34 C0 F0 C4 1C 1B - 3C 47 08 A2 7E E1 63 2F
RADIUS: Framed-Protocol      [7]  6  PPP                               [1]
RADIUS: User-Name            [1]  18  "shashi@pepsi.com"
RADIUS: CHAP-Password        [3]  19  *
RADIUS: NAS-Port-Type        [61]  6  Virtual                         [5]
RADIUS: Service-Type         [6]  6  Framed                          [2]
RADIUS: NAS-IP-Address       [4]  6  10.0.0.21
UDP: sent src=10.1.1.1(21645), dst=10.0.0.10(1645), length=109
UDP: rcvd src=10.0.0.10(1645), dst=10.1.1.1(21645), length=40
RADIUS: Received from id 21645/17 10.0.0.10:1645, Access-Accept, len 32
RADIUS: authenticator C6 99 EC 1A 47 0A 5F F2 - B8 30 4A 4C FF 4B 1D F0
RADIUS: Service-Type         [6]  6  Framed                          [2]
RADIUS: Framed-Protocol      [7]  6  PPP                               [1]
RADIUS(0000001C): Received from id 21645/17
```

Configuration Examples for RADIUS NAS-IP-Address Attribute Configurability

This section provides the following configuration example:

- [Configuring a RADIUS NAS-IP-Address Attribute Configurability: Example, page 5](#)

Configuring a RADIUS NAS-IP-Address Attribute Configurability: Example

The following example shows that IP address 10.0.0.21 has been configured as the RADIUS NAS-IP-Address attribute:

```
radius-server attribute 4 10.0.0.21
radius-server host 10.0.0.10 auth-port 1645 acct-port 1646 key cisco
```

Additional References

The following sections provide references related to RADIUS NAS-IP-Address Attribute Configurability.

Related Documents

Related Topic	Document Title
Configuring AAA	“Authentication, Authorization, and Accounting (AAA)” section of <i>Cisco IOS Security Configuration Guide</i>
Configuring RADIUS	“ Configuring RADIUS ” chapter of <i>Cisco IOS Security Configuration Guide</i>
RADIUS commands	Cisco IOS Security Command Reference

Standards

Standards	Title
No new or modified standards are supported by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module.

- **radius-server attribute 4**

For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

Feature Information for RADIUS NAS-IP-Address Attribute Configurability

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for RADIUS NAS-IP-Address Attribute Configurability

Feature Name	Releases	Feature Information
RADIUS NAS-IP-Address Attribute Configurability	12.3(3)B	This feature allows an arbitrary IP address to be configured and used as RADIUS attribute 4, NAS-IP-Address, without changing the source IP address in the IP header of the RADIUS packets.
	12.3(7)T	
	12.2(28)SB	
	12.2(33)SRC	
	Cisco IOS XE Release 2.1	
		This feature was introduced into Cisco IOS Release 12.3(3)B.
		This feature was integrated into Cisco IOS Release 12.3(7)T.
		This feature was integrated into Cisco IOS Release 12.2(28)SB.
		This feature was integrated into Cisco IOS Release 12.2(33)SRC.
		In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.
		The radius-server attribute 4 command was introduced this feature.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2003–2004, 2006–2007 Cisco Systems, Inc. All rights reserved.



RADIUS Route Download

First Published: February 25, 2002

Last Updated: December 17, 2007

The RADIUS Route Download feature allows users to configure their network access server (NAS) to direct RADIUS authorization. Users configure a separate named method list (in addition to the default method list) for static route download requests sent by their NAS to authorization, authentication, and accounting (AAA) servers.

Before this feature, RADIUS authorization for static route download requests was sent only to AAA servers specified by the default method list.

This feature extends the functionality of the **aaa route download** command to allow users to specify the name of the method list that will be used to direct static route download requests to the AAA servers. The **aaa route download** command may be used to specify a separate method list for downloading static routes. This method list can be added by using the **aaa authorization configuration** command.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for RADIUS Route Download](#)” section on page 6.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2002, 2006, 2007 Cisco Systems, Inc. All rights reserved.

Contents

- [Prerequisites, page 2](#)
- [Configuration Tasks, page 2](#)
- [Configuration Examples, page 3](#)
- [Additional References, page 4](#)
- [Command Reference, page 5](#)
- [Feature Information for RADIUS Route Download, page 6](#)

Prerequisites

AAA network security must be enabled before you perform the tasks in this feature. For information about enabling AAA, refer to the AAA section in the *Cisco IOS Security Configuration Guide*, Release 12.4.

Configuration Tasks

Use the following sections to configure the RADIUS Route Download feature.

- [Configuring RADIUS Route Download](#)
- [Verifying RADIUS Route Download](#)

Configuring RADIUS Route Download

To configure the NAS to send static route download requests to the servers specified by a named method list, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# aaa authorization configuration <i>method-name</i> [radius tacacs+ group <i>group-name</i>]	Downloads static route configuration information from the AAA server using RADIUS.
Step 2	Router(config)# aaa route download [<i>time</i>] [authorization <i>method-list</i>]	Enables the static route download feature. Use the authorization <i>method-list</i> attributes to specify a named method list to which RADIUS authorization requests for static route downloads are sent.

Verifying RADIUS Route Download

To verify the routes that are installed, use the **show ip route** command in EXEC mode.

To display information that is associated with RADIUS, use the **debug radius** command in privileged EXEC mode.

Configuration Examples

This section provides the following configuration examples:

- [RADIUS Route Download Configuration Example](#)

RADIUS Route Download Configuration Example

The following example shows how to configure the NAS to send static route download requests to the servers specified by the method list named “list1”:

```
aaa new-model
aaa group server radius rad1
    server 10.2.2.2 auth-port 1645 acct-port 1646
!
aaa group server tacacs+ tac1
    server 172.17.3.3
!
aaa authorization configuration default group radius
aaa authorization configuration list1 group rad1 group tac1
aaa route download 1 authorization list1

tacacs-server host 172.17.3.3
tacacs-server key cisco
tacacs-server administration
!
radius-server host 10.2.2.2 auth-port 1645 acct-port 1646
radius-server key cisco
```

Additional References

The following sections provide references related to RADIUS Route Download.

Related Documents

Related Topic	Document Title
AAA Overview	“AAA Overview” chapter in the Cisco IOS Security Configuration Guide , Release 12.4
Configuring Large-Scale Dial-Out	“Configuring Large-Scale Dial-Out” chapter in the Cisco IOS Dial Technologies Configuration Guide , Release 12.4
Cisco IOS Dial Technologies	Cisco IOS Dial Technologies Command Reference , Release 12.4

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **aaa route download**

Feature Information for RADIUS Route Download

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for RADIUS Route Download

Feature Name	Releases	Feature Information
RADIUS Route Download	12.2(8)T 12.2(28)SB 12.2(33)SRC	<p>The RADIUS Route Download feature allows users to configure their network access server (NAS) to direct RADIUS authorization. Users configure a separate named method list (in addition to the default method list) for static route download requests sent by their NAS to authorization, authentication, and accounting (AAA) servers.</p> <p>This feature was introduced into Cisco IOS Release 12.2(8)T.</p> <p>This feature was integrated into Cisco IOS Release 12.2(28)SB.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRC.</p> <p>The aaa route download command was introduced by this feature.</p>

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2002, 2006, 2007 Cisco Systems, Inc. All rights reserved.



RADIUS Server Load Balancing

First Published: March 20, 2006
Last Updated: December 17, 2007

The RADIUS Server Load Balancing feature distributes authentication, authorization, and accounting (AAA) authentication and accounting transactions across servers in a server group. These servers can then share the transaction load, resulting in faster responses to incoming requests by optimally using available servers.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for RADIUS Server Load Balancing](#)” section on page 19.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for RADIUS Server Load Balancing, page 2](#)
- [Restrictions for RADIUS Server Load Balancing, page 2](#)
- [Information About RADIUS Server Load Balancing, page 2](#)
- [How to Configure RADIUS Server Load Balancing, page 4](#)
- [Configuration Examples for RADIUS Server Load Balancing, page 8](#)
- [Additional References, page 16](#)
- [Command Reference, page 18](#)
- [Feature Information for RADIUS Server Load Balancing, page 19](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2006–2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for RADIUS Server Load Balancing

- AAA must be configured on your RADIUS server.
- RADIUS must be configured for functions such as authentication, accounting, or static route download.
- AAA RADIUS server groups must be established.

Restrictions for RADIUS Server Load Balancing

- Load balancing is not supported on proxy RADIUS servers.
- Incoming RADIUS requests, such as Packet of Disconnect (POD) requests, are not supported.
- Load balancing is not supported for private server-groups.

Information About RADIUS Server Load Balancing

To configure the RADIUS Server Load Balancing feature, you must understand the following concepts:

- [How RADIUS Server Load Balancing Works, page 2](#)
- [How Transactions Are Load-Balanced Across RADIUS Server Groups, page 3](#)
- [RADIUS Server Status and Automated Testing, page 3](#)

How RADIUS Server Load Balancing Works

Load balancing distributes batches of transactions to servers within a server group. It assigns each batch of transactions to the server with the lowest number of outstanding transactions in its queue. The process of assigning a batch of transactions is as follows:

- The first transaction is received for a new batch.
- All server transaction queues are checked.
- The server with the lowest number of outstanding transactions is identified.
- The identified server is assigned the next batch of transactions.

Batch size is a user configured parameter. Changes in batch size may impact CPU load and network throughput. As batch size increases, CPU load decreases and network throughput increases. However, if a large batch size is used, all available server resources may not be fully utilized. As batch size decreases, CPU load increases, and network throughput decreases. It is recommended that the default batch size, 25, be used because it is optimal for high throughput, without adversely impacting CPU load.

**Note**

There is no set number for large or small batch sizes. As a frame of reference, a batch size greater than 50 is considered large and a batch size less than 25 is considered small.

**Note**

If you have ten or more servers in a server group, it is recommended that a high batch size be set in order to reduce CPU load.

How Transactions Are Load-Balanced Across RADIUS Server Groups

You can configure load balancing either per named RADIUS server group or for the global RADIUS server group. This server group must be referred to as “radius” in the AAA method lists. All public servers that are part of this server group will then be load balanced.

Authentication and accounting can be configured to use the same server or different servers. In some cases, the same server is used for preauthentication, authentication, or accounting transactions for a session. The preferred server, which is an internal setting and set as default, tells AAA to use same server for the start and stop record for a session regardless of server cost. When using the preferred server setting, it is expected that the server used for the initial transaction (for example, authentication), the preferred server, should also be part of any other server group that is used for a subsequent transaction (for example, accounting).

The preferred server is used unless one of the following states is true:

- The **ignore-preferred-server** keyword is used.
- The preferred server is dead.
- The preferred server is in quarantine.
- The want server flag has been set, overriding the preferred server setting.

The want server flag, an internal setting, is used when the same server must be used for all stages of a multistage transaction regardless of server cost. If the want server is not available, the transaction fails.

You may want to use the **ignore-preferred-server** keyword if you have either of the following configurations:

- Dedicated authentication server and a separate dedicated accounting server.
- Network where you can track all call record statistics and call record details, including start- and stop-records, and those records are stored on separate servers.

Also, if you have a configuration where your authentication servers are a superset of your accounting servers, then the preferred server will not be used.

RADIUS Server Status and Automated Testing

The RADIUS Server Load Balancing feature takes server status into account when assigning batches. Only servers that are verified alive are sent transaction batches. It is recommended that you test the status all RADIUS load-balanced servers, including low usage servers (for example, backup servers).

Transactions are not sent to a server that is marked dead. A server is marked dead until its timer expires, at which time it is in quarantine. A server is in quarantine until it is verified alive by the RADIUS automated tester functionality.

The RADIUS automated tester uses the following steps to determine if a server is alive and available to process transactions:

- A request is sent periodically to the server for a test user ID.
- If an Access-Reject message is returned from the server, the server is alive.
- If no message is returned from the server, it is not alive; that is, the server is either dead or quarantined.

If transactions have been sent to a server that is not responding, before it is marked dead, that transaction is failed over to the next available server. It is recommended that the retry reorder mode for failed transactions be used.

When using the RADIUS automated tester, verify that the test packets being sent by the network access server (NAS) to the AAA servers are being responded to. If the servers are not configured correctly, the packets may be dropped and the server erroneously marked dead.

**Caution**

It is recommended that a test user, one that is not defined on the RADIUS server, be used for RADIUS server automated testing to protect against security issues that may arise if the test user is not correctly configured.

**Note**

If you want to check load balancing transactions at a specific point in time, you can use the **test aaa group** command.

How to Configure RADIUS Server Load Balancing

This section contains the following procedures that allow you to configure load balancing:

- [Enabling Load Balancing for Named RADIUS Server Group, page 4](#)
- [Enabling Load Balancing for Global RADIUS Server Group, page 5](#)
- [Troubleshooting RADIUS Server Load Balancing, page 6](#)

Enabling Load Balancing for Named RADIUS Server Group

Use the following task to enable RADIUS Server Load Balancing for a named server group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server host** {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**idle-time** *seconds*]
4. **aaa group server radius** *group-name*
5. **load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	radius-server host {hostname ip-address} [test username user-name] [auth-port port-number] [ignore-auth-port] [acct-port port-number] [ignore-acct-port] [idle-time seconds] Example: Router(config)# radius-server host 192.0.2.1 test username test1 idle-time 1	Enables RADIUS automated testing. <ul style="list-style-type: none"> The test username keyword must be used to enable RADIUS automated testing, followed by the value for the <i>user-name</i> argument. By default, auth-port is tested using port 1645. Use ignore-auth-port to turn off testing of the authentication port. By default, acct-port is tested using port 1645. Use ignore-acct-port to turn off testing of the accounting port. By default, the idle-time is 3600 seconds. The range is 1 – 35791.
Step 4	aaa group server radius group-name Example: Router(config)# aaa group server radius rad-sg	Enters server group configuration mode.
Step 5	load-balance method least-outstanding [batch-size number] [ignore-preferred-server] Example: Router(config-sg)# load-balance method least-outstanding batch-size 30	Enables least-outstanding load balancing for a server group. <ul style="list-style-type: none"> By default, the batch-size is set to 25. A range of 1 – 2147483647 may be used. By default, the preferred server is enabled. If you want to disable the preferred-server setting, use the keyword ignore-preferred-server.

Enabling Load Balancing for Global RADIUS Server Group

Use the following task to enable RADIUS Server Load Balancing for the global RADIUS server group. This is the group referred to as “radius” in the AAA method lists.

SUMMARY STEPS

- enable
- configure terminal

3. **radius-server host** {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**idle-time** *seconds*]
4. **radius-server load-balance method least-outstanding** [**batch-size** *number*] [**ignore-preferred-server**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	radius-server host { <i>hostname</i> <i>ip-address</i> } [test username <i>user-name</i>] [auth-port <i>port-number</i>] [ignore-auth-port] [acct-port <i>port-number</i>] [ignore-acct-port] [idle-time <i>seconds</i>] Example: Router(config)# radius-server host 192.0.2.1 test username test1 idle-time 1	Enables RADIUS automated testing. <ul style="list-style-type: none"> The test username keyword must be used to enable RADIUS automated testing, followed by the value for the <i>user-name</i> argument. By default, auth-port is tested using port 1645. Use ignore-auth-port to turn off testing of the authentication port. By default, acct-port is tested using port 1645. Use ignore-acct-port to turn off testing of the accounting port. By default, the idle-time is 3600 seconds. The range is 1 – 35791.
Step 4	radius-server load-balance method least-outstanding [batch-size <i>number</i>] [ignore-preferred-server] Example: Router(config)# radius-server load-balance method least-outstanding	Enables least-outstanding load balancing for the global RADIUS server group. <ul style="list-style-type: none"> By default, the batch-size is set to 25. A range of 1 – 2147483647 may be used. By default, the preferred server is enabled. If you want to disable the preferred server setting, use the ignore-preferred-server keyword.

Troubleshooting RADIUS Server Load Balancing

After configuring the RADIUS Server Load Balancing feature, you may monitor the idle timer, dead timer, load balancing server selection, or issue a manual test command to verify server status.

Use the following commands as appropriate for troubleshooting the RADIUS Server Load Balancing feature:

- The **debug aaa test** command can be used to determine when the idle timer or dead timer has expired, when test packets are sent, the status of the server, or to verify server state.

- The **debug aaa sg-server selection** command can be used to examine which server is being selected for load balancing.
- The **test aaa group** command can be used to manually verify RADIUS load-balanced server status.

SUMMARY STEPS

1. **debug aaa test**
2. **debug aaa sg-server selection**
3. **test aaa group group-name username password new-code**

DETAILED STEPS

Step 1 The idle timer is used to check the server status and is updated with or without any incoming requests. It is useful to monitor the idle timer to determine if there are nonresponsive servers and to keep your RADIUS server status updated in order to efficiently utilize your available resources. For instance, an updated idle timer would help ensure that incoming requests are being sent to servers that are alive.

The dead timer is used either to determine that a server is dead or to update a dead server's status appropriately.

Monitoring server selection can help you determine how often the server selection changes. This is effective in analyzing if there is a bottleneck, a large number of queued up requests, or if only specific servers are processing incoming requests.

For example, the following debug output shows when the idle-timer has expired:

```
Router# debug aaa test
```

```
Jul 16 00:07:01: AAA/SG/TEST: Server (192.0.2.245:1700,1701) quarantined.
Jul 16 00:07:01: AAA/SG/TEST: Sending test request(s) to server (192.0.2.245:1700,1701)
Jul 16 00:07:01: AAA/SG/TEST: Sending 1 Access-Requests, 1 Accounting-Requests in current batch.
Jul 16 00:07:01: AAA/SG/TEST(Req#: 1): Sending test AAA Access-Request.
Jul 16 00:07:01: AAA/SG/TEST(Req#: 1): Sending test AAA Accounting-Request.
Jul 16 00:07:01: AAA/SG/TEST: Obtained Test response from server (192.0.2.245:1700,1701)
Jul 16 00:07:01: AAA/SG/TEST: Obtained Test response from server (192.0.2.245:1700,1701)
Jul 16 00:07:01: AAA/SG/TEST: Necessary responses received from server (192.0.2.245:1700,1701)
Jul 16 00:07:01: AAA/SG/TEST: Server (192.0.2.245:1700,1701) marked ALIVE. Idle timer set for 60 sec(s).
Jul 16 00:07:01: AAA/SG/TEST: Server (192.0.2.245:1700,1701) removed from quarantine.
```

Step 2 For example, the following debug output shows 5 access requests being sent to a server group with a batch size of 3:

```
Router# debug aaa sg-server selection
```

```
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [3] transactions remaining in batch. Reusing server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [2] transactions remaining in batch. Reusing server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [1] transactions remaining in batch. Reusing server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
```

```

Jul 16 03:15:05: AAA/SG/SERVER_SELECT: No more transactions in batch. Obtaining a new
server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining a new least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Server[0] load: 3
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Server[1] load: 0
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Server[2] load: 0
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Selected Server[1] with load 0
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [3] transactions remaining in batch.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: Obtaining least loaded server.
Jul 16 03:15:05: AAA/SG/SERVER_SELECT: [2] transactions remaining in batch. Reusing
server.

```

Step 3 The following example shows the response from a load-balanced RADIUS server that is alive when the username “test” does not match a user profile. The server is verified alive when it issues an Access-Reject response to a AAA packet generated by the **test aaa group** command.

```
Router# test aaa group SG1 test lab new-code
```

```

00:06:07: RADIUS/ENCODE(00000000):Orig. component type = INVALID
00:06:07: RADIUS/ENCODE(00000000): dropping service type, "radius-server attribute 6
on-for-login-auth" is off
00:06:07: RADIUS(00000000): Config NAS IP: 192.0.2.4
00:06:07: RADIUS(00000000): sending
00:06:07: RADIUS/ENCODE: Best Local IP-Address 192.0.2.141 for Radius-Server 192.0.2.176
00:06:07: RADIUS(00000000): Send Access-Request to 192.0.2.176:1645 id 1645/1, len 50
00:06:07: RADIUS: authenticator CA DB F4 9B 7B 66 C8 A9 - D1 99 4E 8E A4 46 99 B4
00:06:07: RADIUS: User-Password [2] 18 *
00:06:07: RADIUS: User-Name [1] 6 "test"
00:06:07: RADIUS: NAS-IP-Address [4] 6 192.0.2.141
00:06:07: RADIUS: Received from id 1645/1 192.0.2.176:1645, Access-Reject, len 44
00:06:07: RADIUS: authenticator 2F 69 84 3E F0 4E F1 62 - AB B8 75 5B 38 82 49 C3
00:06:07: RADIUS: Reply-Message [18] 24
00:06:07: RADIUS: 41 75 74 68 65 6E 74 69 63 61 74 69 6F 6E 20 66 [Authentication f]
00:06:07: RADIUS: 61 69 6C 75 72 65 [failure]
00:06:07: RADIUS(00000000): Received from id 1645/1
00:06:07: RADIUS/DECODE: Reply-Message fragments, 22, total 22 bytes
Router#

```

Configuration Examples for RADIUS Server Load Balancing

This section provides the following RADIUS Server Load Balancing feature configuration examples:

- [Global RADIUS Server Group: Examples, page 9](#)
- [Named RADIUS Server Group: Examples, page 11](#)
- [Idle Timer Monitoring: Examples, page 13](#)
- [Preferred Server with the Same Authentication and Authorization Server: Example](#)
- [Preferred Server with Different Authentication and Authorization Servers: Example](#)
- [Preferred Server with Overlapping Authentication and Authorization Servers: Example](#)
- [Preferred Server with Authentication Servers As a Subset of Authorization Servers: Example](#)
- [Preferred Server with Authentication Servers As a Superset of Authorization Servers: Example](#)

Global RADIUS Server Group: Examples

The following example shows how to enable load balancing for global RADIUS server groups. It is shown in three parts: the current configuration of RADIUS command output, debug output, and AAA server status information. You can use the delimiting characters to display only the relevant parts of the configuration.

Server Configuration and Enabling Load Balancing for Global RADIUS Server Group: Example

The following shows the relevant RADIUS configuration.

```
Router# show running-config | include radius
```

```
aaa authentication ppp default group radius
aaa accounting network default start-stop group radius
radius-server host 192.0.2.238 auth-port 2095 acct-port 2096 key cisco
radius-server host 192.0.2.238 auth-port 2015 acct-port 2016 key cisco
radius-server load-balance method least-outstanding batch-size 5
```

The lines in the current configuration of RADIUS command output above are defined as follows:

- The **aaa authentication ppp** command authenticates all PPP users using RADIUS.
- The **aaa accounting** command enables the sending of all accounting requests to the AAA server once the client is authenticated and after the disconnect using the keyword **start-stop**.
- The **radius-server host** command defines the IP address of the RADIUS server host with the authorization and accounting ports specified and the authentication and encryption key identified.
- The **radius-server load-balance** command enables load balancing for the global radius server groups with the batch size specified.

Debug Output for Global RADIUS Server Group: Example

The debug output below shows the selection of preferred server and processing of requests for the configuration above.

```
Router# show debug
```

```
General OS:
```

```
AAA server group server selection debugging is on
```

```
#
```

```
<sending 10 pppoe requests>
```

```
Router#
```

```
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):No preferred server available.
```

```
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
```

```
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new server.
```

```
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
```

```
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:0
```

```
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
```

```
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
```

```
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
```

```
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):Server (192.0.2.238:2095,2096) now being used as preferred server
```

```
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):No preferred server available.
```

```
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
```

```
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing server.
```

```

*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):Server (192.0.2.238:2015,2016) now
being used as preferred server.

```

Server Status Information for Global RADIUS Server Group: Example

The output below shows the AAA server status for the global RADIUS server group configuration example.

Router# **show aaa server**

```

RADIUS:id 4, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
  State:current UP, duration 3175s, previous duration 0s
  Dead:total time 0s, count 0
  Quarantined:No
  Authen:request 6, timeouts 1
    Response:unexpected 1, server error 0, incorrect 0, time 1841ms
    Transaction:success 5, failure 0
  Author:request 0, timeouts 0
    Response:unexpected 0, server error 0, incorrect 0, time 0ms
    Transaction:success 0, failure 0
  Account:request 5, timeouts 0
    Response:unexpected 0, server error 0, incorrect 0, time 3303ms
    Transaction:success 5, failure 0
  Elapsed time since counters last cleared:2m

RADIUS:id 5, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
  State:current UP, duration 3175s, previous duration 0s
  Dead:total time 0s, count 0
  Quarantined:No
  Authen:request 6, timeouts 1
    Response:unexpected 1, server error 0, incorrect 0, time 1955ms
    Transaction:success 5, failure 0
  Author:request 0, timeouts 0

```

```

Response:unexpected 0, server error 0, incorrect 0, time 0ms
Transaction:success 0, failure 0
Account:request 5, timeouts 0
Response:unexpected 0, server error 0, incorrect 0, time 3247ms
Transaction:success 5, failure 0
Elapsed time since counters last cleared:2m

```

The output shows the status of two RADIUS servers. Both servers are up and, in the last 2 minutes, have successfully processed:

- 5 out of 6 authentication requests
- 5 out of 5 accounting requests

Named RADIUS Server Group: Examples

The following example shows load balancing enabled for a named RADIUS server group. It is shown in three parts: the current configuration of RADIUS command output, debug output, and AAA server status information.

Server Configuration and Enabling Load Balancing for Named RADIUS Server Group: Example

The following shows the relevant RADIUS configuration.

```

Router# show running-config
.
.
.
aaa group server radius server-group1
  server 192.0.2.238 auth-port 2095 acct-port 2096
  server 192.0.2.238 auth-port 2015 acct-port 2016
  load-balance method least-outstanding batch-size 5
!
aaa authentication ppp default group server-group1
aaa accounting network default start-stop group server-group1
.
.
.

```

The lines in the current configuration of RADIUS command output above are defined as follows:

- The **aaa group server radius** command shows the configuration of a server group with two member servers.
- The **load-balance** command enables load balancing for the global radius server groups with the batch size specified.
- The **aaa authentication ppp** command authenticates all PPP users using RADIUS.
- The **aaa accounting** command enables the sending of all accounting requests to the AAA server once the client is authenticated and after the disconnect using the **start-stop** keyword.

Debug Output for Named RADIUS Server Group: Example

The debug output below shows the selection of preferred server and processing of requests for the configuration above.

```

Router#

```

```

*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[0] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):Server (192.0.2.238:2015,2016) now
being used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000032):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
.
.
.

```

Server Status Information for Named RADIUS Server Group Example

The output below shows the AAA server status for the named RADIUS server group configuration example.

```
Router# show aaa servers
```

```

RADIUS:id 8, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
State:current UP, duration 3781s, previous duration 0s

```

```

Dead:total time 0s, count 0
Quarantined:No
Authen:request 0, timeouts 0
      Response:unexpected 0, server error 0, incorrect 0, time 0ms
      Transaction:success 0, failure 0
Author:request 0, timeouts 0
      Response:unexpected 0, server error 0, incorrect 0, time 0ms
      Transaction:success 0, failure 0
Account:request 0, timeouts 0
      Response:unexpected 0, server error 0, incorrect 0, time 0ms
      Transaction:success 0, failure 0
Elapsed time since counters last cleared:0m

RADIUS:id 9, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
State:current UP, duration 3781s, previous duration 0s
Dead:total time 0s, count 0
Quarantined:No
Authen:request 0, timeouts 0
      Response:unexpected 0, server error 0, incorrect 0, time 0ms
      Transaction:success 0, failure 0
Author:request 0, timeouts 0
      Response:unexpected 0, server error 0, incorrect 0, time 0ms
      Transaction:success 0, failure 0
Account:request 0, timeouts 0
      Response:unexpected 0, server error 0, incorrect 0, time 0ms
      Transaction:success 0, failure 0
Elapsed time since counters last cleared:0m

```

The output shows the status of two RADIUS servers. Both servers are alive, and no requests have been processed since the counters were cleared 0 minutes ago.

Idle Timer Monitoring: Examples

The following example shows idle timer and related server state for load balancing enabled for a named RADIUS server group. It is shown in two parts: the current configuration of RADIUS command output and debug output.

Server Configuration and Enabling Load Balancing for Idle Timer Monitoring: Example

The following shows the relevant RADIUS configuration.

```

Router# show running-config | include radius

aaa group server radius server-group1
radius-server host 192.0.2.238 auth-port 2095 acct-port 2096 test username junk1 idle-time
1 key cisco
radius-server host 192.0.2.238 auth-port 2015 acct-port 2016 test username junk1 idle-time
1 key cisco
radius-server load-balance method least-outstanding batch-size 5

```

The lines in the current configuration of RADIUS command output above are defined as follows:

- The **aaa group server radius** command shows the configuration of a server group.
- The **radius-server host** command defines the IP address of the RADIUS server host with the authorization and accounting ports specified and the authentication and encryption key identified.

- The **radius-server load-balance** command enables load balancing for the radius server with the batch size specified.

Debug Output for Idle Timer Monitoring: Example

The debug output below shows the test requests being sent to servers. The response to the test request sent to the server is received, the server is removed from quarantine as appropriate, marked alive, and then the idle timer is reset.

```
Router#
*Feb 28 13:52:20.835:AAA/SG/TEST:Server (192.0.2.238:2015,2016) quarantined.
*Feb 28 13:52:20.835:AAA/SG/TEST:Sending test request(s) to server (192.0.2.238:2015,2016)
*Feb 28 13:52:20.835:AAA/SG/TEST:Sending 1 Access-Requests, 1 Accounting-Requests in
current batch.
*Feb 28 13:52:20.835:AAA/SG/TEST(Req#:1):Sending test AAA Access-Request.
*Feb 28 13:52:20.835:AAA/SG/TEST(Req#:1):Sending test AAA Accounting-Request.
*Feb 28 13:52:21.087:AAA/SG/TEST:Obtained Test response from server
(192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Obtained Test response from server
(192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Necessary responses received from server
(192.0.2.238:2015,2016)
*Feb 28 13:52:22.651:AAA/SG/TEST:Server (192.0.2.238:2015,2016) marked ALIVE. Idle timer
set for 60 secs(s).
*Feb 28 13:52:22.651:AAA/SG/TEST:Server (192.0.2.238:2015,2016) removed from quarantine.
.
.
.
```

Preferred Server with the Same Authentication and Authorization Server: Example

The following example shows an authentication server group and an authorization server group that use the same servers, 209.165.200.225 and 209.165.200.226. Both server groups have the preferred server flag enabled.

```
aaa group server radius authentication-group
  server 209.165.200.225 key radkey1
  server 209.165.200.226 key radkey2

aaa group server radius accounting-group
  server 209.165.200.225 key radkey1
  server 209.165.200.226 key radkey2
```

Once a preferred server is selected for a session, all transactions for that session will continue to use the original preferred server. The servers 209.165.200.225 and 209.165.200.226 will be load balanced based on sessions rather than transactions.

Preferred Server with Different Authentication and Authorization Servers: Example

The following example shows an authentication server group that uses servers 209.165.200.225 and 209.165.200.226 and an authorization server group that uses servers 209.165.201.1 and 209.165.201.2. Both server groups have the preferred server flag enabled.

```
aaa group server radius authentication-group
server 209.165.200.225 key radkey1
server 209.165.200.226 key radkey2
```

```
aaa group server radius accounting-group
server 209.165.201.1 key radkey3
server 209.165.201.2 key radkey4
```

The authentication server group and the accounting server group do not share any common servers. A preferred server will never be found for accounting transactions, therefore, authentication and accounting servers will be load balanced based on transactions. Start and stop records will be sent to the same server for a session.

Preferred Server with Overlapping Authentication and Authorization Servers: Example

The following example shows an authentication server group that uses servers 209.165.200.225, 209.165.200.226, and 209.165.201.1 and an accounting server group that uses servers 209.165.201.1 and 209.165.201.2. Both server groups have the preferred server flag enabled.

```
aaa group server radius authentication-group
server 209.165.200.225 key radkey1
server 209.165.200.226 key radkey2
server 209.165.201.1 key radkey3
```

```
aaa group server radius accounting-group
server 209.165.201.1 key radkey3
server 209.165.201.2 key radkey4
```

If all servers have equal transaction processing capability, one-third of all authentication transactions will be directed towards server 209.165.201.1. Therefore, one-third of all accounting transactions will also be directed towards server 209.165.201.1. The remaining two-thirds accounting transactions will be load balanced equally between servers 209.165.201.1 and 209.165.201.2. The server 209.165.201.1 will receive fewer authentication transactions since server 209.165.201.1 will have outstanding accounting transactions.

Preferred Server with Authentication Servers As a Subset of Authorization Servers: Example

The following example shows an authentication server group that uses servers 209.165.200.225 and 209.165.200.226 and an authorization server group that uses servers 209.165.200.225, 209.165.200.226, and 209.165.201.1. Both server groups have the preferred server flag enabled.

```
aaa group server radius authentication-group
  server 209.165.200.225 key radkey1
  server 209.165.200.226 key radkey2

aaa group server radius accounting-group
  server 209.165.200.225 key radkey1
  server 209.165.200.226 key radkey2
  server 209.165.201.1 key radkey3
```

One-half of all authentication transactions will be sent to server 209.165.200.225 and the other half to server 209.165.200.226. Servers 209.165.200.225 and 209.165.200.226 will be the preferred servers for authentication and accounting transaction, therefore there will be an equal distribution of authentication and accounting transactions across servers 209.165.200.225 and 209.165.200.226. Server 209.165.201.1 will be relatively unused.

Preferred Server with Authentication Servers As a Superset of Authorization Servers: Example

The following example shows an authentication server group that uses servers 209.165.200.225 and 209.165.200.226, and 209.165.201.1 and an authorization server group that uses servers 209.165.200.225 and 209.165.200.226. Both server groups have the preferred server flag enabled.

```
aaa group server radius authentication-group
  server 209.165.200.225 key radkey1
  server 209.165.200.226 key radkey2
  server 209.165.201.1 key radkey3

aaa group server radius accounting-group
  server 209.165.200.225 key radkey1
  server 209.165.200.226 key radkey2
```

Initially, one-third of authentication transactions will be assigned to each server in the authorization server group. As accounting transactions are generated for more sessions, the accounting transactions will only be sent to servers 209.165.200.225 and 209.165.200.226, since the preferred server flag is on. As servers 209.165.200.225 and 209.165.200.226 begin to process more transactions, authentication transactions will start to be sent to server 209.165.201.1. The transaction requests authenticated by server 209.165.201.1, will not have any preferred server setting and will be split between servers 209.165.200.225 and 209.165.200.226, which negates the use of the preferred server flag. This configuration should be used cautiously.

Additional References

The following sections provide references related to the RADIUS Server Load Balancing feature.

Related Documents

Related Topic	Document Title
AAA and RADIUS	“Authentication, Authorization, and Accounting (AAA)” section in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4
AAA Server Groups	“AAA Server Groups” chapter in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4
RADIUS Configuration	“Configuring RADIUS” chapter in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4
Failover retry reorder mode	“RADIUS Server Reorder on Failure” section in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
<ul style="list-style-type: none">None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug aaa sg-server selection**
- **debug aaa test**
- **load-balance (server-group)**
- **radius-server host**
- **radius-server load-balance**
- **test aaa group**

Feature Information for RADIUS Server Load Balancing

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for RADIUS Server Load Balancing

Feature Name	Releases	Feature Information
RADIUS Server Load Balancing	12.2(28)SB 12.4(11)T 12.2(33)SRC	The RADIUS Server Load Balancing feature distributes authentication, authorization, and accounting (AAA) authentication and accounting transactions across servers in a server group. These servers can then share the transaction load, resulting in faster responses to incoming requests by optimally using available servers. This feature was integrated into Cisco IOS Release 12.2(28)SB. This feature was integrated into Cisco IOS Release 12.4(11)T. This feature was integrated into Cisco IOS Release 12.2(33)SRC.
RADIUS Server Load Balancing porting	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2006–2007 Cisco Systems, Inc. All rights reserved.



RADIUS Support of 56-Bit Acct Session-Id

The RADIUS Support of 56-Bit Acct Session-Id feature introduces a new 32-bit authentication, authorization, and accounting (AAA) variable, acct-session-id-count. The first eight bits of the acct-session-id-count variable are reserved for the unique identifier variable, a unique number assigned to the accounting session which is preserved between reloads. The acct-session-id-count variable is used in addition to the existing 32-bit acct-session-id variable, RADIUS attribute 44, providing a total of 56 bits of to represent the actual Accounting Session Identifier (ID). Benefits of this feature include the following:

- The 8-bit unique identifier variable allows accounting sessionIDs to be identified if a reload occurs.
- The additional space provided by the acct-session-id-count variable can keep track of acct-session-id wrapping when there is a high volume of traffic, such as voice calls. By incrementing each time the acct-session-id variable wraps, the acct-session-id-count variable preserves accounting information.

Feature Specifications for RADIUS Support of 56-Bit Acct Session-Id

Feature History

Release	Modification
12.3(2)T	This feature was introduced.

Supported Platforms

Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco AS5850

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for RADIUS Support of 56-Bit Acct Session-Id, page 2](#)
- [Information About RADIUS Support of 56-Bit Acct Session-Id, page 2](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [How to Configure RADIUS Support of 56-Bit Acct Session-Id](#), page 3
- [Configuration Examples for RADIUS Support of 56-Bit Acct Session-Id](#), page 4
- [Additional References](#), page 4
- [Command Reference](#), page 6

Prerequisites for RADIUS Support of 56-Bit Acct Session-Id

AAA accounting must be configured. For more information about configuring AAA accounting, refer to the “*Configuring Accounting*” chapter in the [Cisco IOS Security Configuration Guide](#), Release 12.2.

Information About RADIUS Support of 56-Bit Acct Session-Id

To configure the RADIUS Support of 56-bit Acct Session-Id feature, you must understand the following concepts:

- [Acct-Session-Id Attribute](#), page 2
- [Acct-Session-Id-Count Attribute](#), page 2
- [Benefits of RADIUS Support of 56-Bit Acct Session-Id](#), page 3

Acct-Session-Id Attribute

RADIUS attribute 44, Accounting Session ID, is a unique accounting identifier that makes it easy to match start and stop records in a log file. Accounting session ID numbers restart at 1 each time the router is power-cycled or the software is reloaded. RADIUS attribute 44 is automatically enabled when AAA accounting is configured.

The acct-session-id variable is a 32-bit variable that can take on values from 00000000–FFFFFFFF.

Acct-Session-Id-Count Attribute

The new acct-session-id-count variable is a 32-bit variable. The first eight bits of the variable are reserved for the unique identifier variable, an identifier that allows the RADIUS server to identify an accounting session if a reload occurs. The remaining 24 bits of the acct-session-id-count variable acts as a counter variable. When the first acct-session-id variable is assigned, this counter variable is set to 1. The variable increments by 1 every time the acct-session-id variable wraps, preventing the loss of accounting information.

The acct-session-id-count variable can take on values from ##000000–##FFFFFF, where ## represents the eight bits that are reserved for the unique identifier variable.

The acct-session-id-count and acct-session-id variables are concatenated before being sent to the RADIUS server, resulting in the acct-session variable being represented as the following:

##000000 00000000–##FFFFFF FFFFFFFF

This allows a total of 56 bits to be used for acct-session-id space.

Benefits of RADIUS Support of 56-Bit Acct Session-Id

Allows RADIUS Servers to Identify Accounting Sessions After a Reload

The 8-bit unique identifier variable allows accounting session identities to be identified if a reload occurs.

Provides Accounting Information Space for High Volume Traffic

The additional space provided by the acct-session-id-count variable can keep track of acct-session-id wrapping when there is a high volume of traffic, such as voice calls. By incrementing each time the acct-session-id variable wraps, the acct-session-id-count variable preserves accounting information.

How to Configure RADIUS Support of 56-Bit Acct Session-Id

This section contains the following procedure:

- [Configuring RADIUS Support of 56-Bit Acct Session-Id, page 3](#)

Configuring RADIUS Support of 56-Bit Acct Session-Id

This task enables the acct-session-id-count variable containing the unique identifier variable.

SUMMARY STEPS

1. `enable`
2. `radius-server unique-ident id`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	radius-server unique-ident <i>id</i> Example: Router(config)# radius-server unique-ident 5	Enables the acct-session-id-count variable containing the unique identifier variable. <ul style="list-style-type: none">• The <i>id</i> argument specifies the unique identifier represented by the first eight bits of the acct-session-id-count variable. Valid values range from 0 to 255.

Configuration Examples for RADIUS Support of 56-Bit Acct Session-Id

This section contains the following configuration example:

- [Configuring RADIUS Support of 56-Bit Acct Session-Id Example, page 4](#)

Configuring RADIUS Support of 56-Bit Acct Session-Id Example

The following example configures AAA authentication, enables RADIUS attribute 44 in access request packets, and enables the acct-session-id-count variable and sets the unique identifier variable to 5:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server unique-ident 5
```

Additional References

For additional information related to the RADIUS Support of 56-Bit Acct Session-Id feature, refer to the following references:

- [Related Documents, page 5](#)
- [Standards, page 5](#)
- [MIBs, page 5](#)
- [RFCs, page 6](#)
- [Technical Assistance, page 6](#)

Related Documents

Related Topic	Document Title
Additional information about configuring RADIUS	“Configuring RADIUS” chapter in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.2
Additional information about configuring accounting	“Configuring Accounting” chapter in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.2
Additional information about AAA RADIUS attributes	“RADIUS Attributes” section in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.2
Additional RADIUS commands	The <i>Cisco IOS Security Command Reference</i> , Release 12.3 T

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

RFCs ¹	Title
RFC 2139	RADIUS Accounting

1. Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **radius-server unique-iden**

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



RADIUS Tunnel Preference for Load Balancing and Fail-Over

Feature History

Release	Modification
12.2(4)T	This feature was introduced.

This document describes the RADIUS Tunnel Preference for Load Balancing and Fail-Over feature in Cisco IOS Release 12.2(4)T. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 4](#)
- [Supported Standards, MIBs, and RFCs, page 5](#)
- [Prerequisites, page 5](#)
- [Configuration Tasks, page 5](#)
- [Configuration Example, page 6](#)
- [Command Reference, page 6](#)
- [Glossary, page 6](#)

Feature Overview

The RADIUS Tunnel Preference for Load Balancing and Fail-Over feature provides load balancing and fail-over virtual private dialup network (VPDN) home gateway (HGW) groups in a standardized fashion. This feature introduces new software functionality; no new command is associated with this feature.

Industry-Standard Rather Than Proprietary Attributes

Until Cisco IOS Release 12.2(4)T, load balancing and fail-over functionality for a Layer 2 Tunnel Protocol network server (LNS) was provided by the Cisco proprietary Vendor Specific Attribute (VSA). In a multivendor network environment, using VSA on a RADIUS server can cause interoperability issues



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

among network access servers (NASs) manufactured by different vendors. Even though some RADIUS server implementations can send VSAs that the requesting NAS can understand, the user still must maintain different VSAs for the same purpose in a single-service profile.

A consensus regarding the tunnel attributes that are to be used in a multivendor network environment is defined in RFC 2868. In RFC 2868, Tunnel-Server-Endpoint, in conjunction with the Tunnel-Medium-Type, specifies the address to which the NAS should initiate a new session. If multiple Tunnel-Server-Endpoint attributes are defined in one tagged attribute group, they are interpreted as equal-cost load-balancing HGWs.

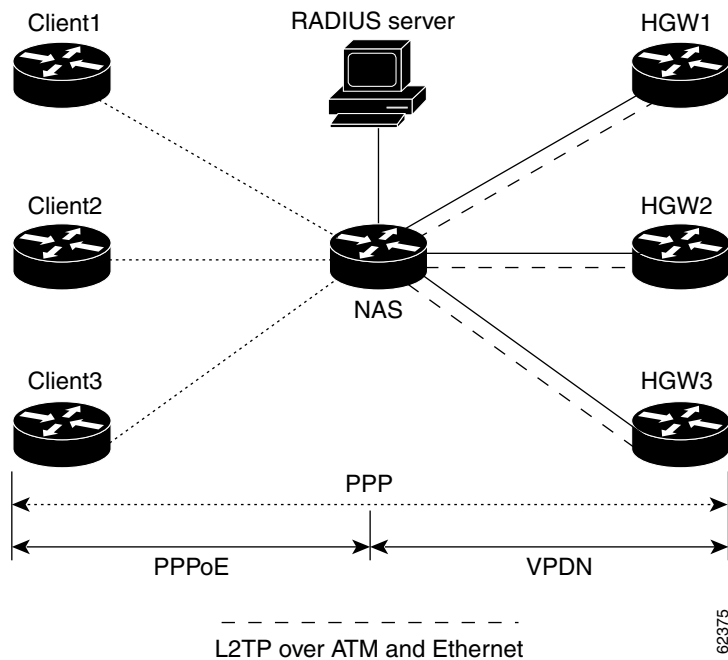
The Tunnel-Preference attribute defined in RFC 2868 can be used as a measure to form load balancing and fail-over HGW groups. When the Tunnel-Preference values of different tagged attribute groups are the same, the Tunnel-Server-Endpoint of those attribute groups is considered to have the same priority unless otherwise specified. When the Tunnel-Preference values of some attribute groups are higher (they have a lower preference) than other attribute groups, their Tunnel-Server-Endpoint attributes will have higher priority values. When an attribute group has a higher priority value, that attribute group will be used for fail-over in case the attribute groups with lower priority values are unavailable for the connections.

Until Cisco IOS Release 12.2(4)T, a specially formatted string would be transported within a Cisco VSA “vpdn:ip-addresses” string to a NAS for the purpose of HGW load balancing and fail-over. For example, 10.0.0.1 10.0.0.2 10.0.0.3/2.0.0.1 2.0.0.2 would be interpreted as IP addresses 10.0.0.1, 10.0.0.2, and 10.0.0.3 for the first group for load balancing. New sessions are projected to these three addresses based on the least-load-first algorithm. This algorithm uses its local knowledge to select an HGW that has the least load to initiate the new session. In this example, the addresses 2.0.0.1 and 2.0.0.2 in the second group have a lower priority and are applicable only when all HGWs specified in the first group fail to respond to the new connection request, thereby making 2.0.0.1 and 2.0.0.2 the fail-over addresses. See the section “[Configuration Example](#)” for an example of how to configure these fail-over addresses in a RADIUS tunnel profile.

Load Balancing and Fail-Over in a Multivendor Network

The RADIUS Tunnel Preference for Load Balancing and Fail-Over feature was designed for large multivendor networks that use VPDN Layer 2 tunnels over WAN links such as ATM and Ethernet, such as the configuration shown in [Figure 1](#).

Figure 1 Typical Load Balancing and Fail-Over in a Multivendor Network



In the configuration shown in [Figure 1](#), the NAS uses tunnel profiles downloaded from the RADIUS server to establish VPDN Layer 2 tunnels for load balancing and fail-over. The Point-to-Point over Ethernet (PPPoE) protocol is used as the client to generate PPP sessions.

Benefits

The RADIUS Tunnel Preference for Load Balancing and Fail-Over feature provides industry-standard load balancing and fail-over functionality for an LNS, rather than requiring the use of a Cisco proprietary VSA. The feature conforms to the tunnel attributes that are to be used in a multivendor network environment as defined in RFC 2868, thereby eliminating interoperability issues among NASs manufactured by different vendors.

Restrictions

The following restrictions and limitations apply to the RADIUS Tunnel Preference for Load Balancing and Fail-Over feature:

- This feature does not support VPDN dial-out networks; it is designed only for dial-in applications.
- The maximum number of LNSs allowed in the network is 1550, which is 50 per tag attribute group and a limit of 31 tags.
- This feature requires a RADIUS server implementation to support RFC 2868.

Related Features and Technologies

The RADIUS Tunnel Preference for Load Balancing and Fail-Over feature is used in VPDNs. Additionally, familiarity with the following technologies and protocols is recommended:

- ATM
- Ethernet
- L2TP and L2F
- PPP and PPPoE
- RADIUS servers

See the next section for a list of documentation that describes these technologies and protocols.

Related Documents

- “Basic Dial-in VPDN Configuration Using VPDN Groups” at http://www.cisco.com/warp/public/793/access_dial/2.html
- *Cisco IOS Dial Technologies Command Reference*, Release 12.2
- *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2, the chapters in the part “Virtual Templates, Profiles, and Networks”
- *Cisco IOS Security Command Reference*, Release 12.2
- *Cisco IOS Security Configuration Guide*, Release 12.2, the chapter “Configuring RADIUS” and the appendix “RADIUS Attributes”
- “Which VPN Solution is Right for You?” at http://www.cisco.com/warp/public/707/which_vpn.html
- *Cisco IOS Wide-Area Networking Command Reference*, Release 12.2
- *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.2, the chapter “Configuring Broadband Access: PPP and Routed Bridge Encapsulation”

Supported Platforms

This feature is platform independent and was either developed for or tested on the following Cisco routers:

- Cisco 800 series
- Cisco 1600 series
- Cisco 1700 series
- Cisco 2600 series
- Cisco 3600 series
- Cisco 7100 series
- Cisco 7200 series

See the next section for information about Feature Navigator and how to use this tool to determine the platforms and software images in which this feature is available.

Determining Platform Support Through Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Feature Navigator. Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. As of May 2001, Feature Navigator supports M, T, E, S, and ST releases. You can access Feature Navigator at the following URL:

<http://www.cisco.com/go/fn>

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

RFCs

RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*

Prerequisites

Configuring VPDNs and HGW groups is beyond the scope of this document. Refer to the documentation listed in the section “[Related Documents](#)” for the tasks and commands to configure these types of networks.

Configuration Tasks

This feature has no new configuration commands; however, see the next section for an example of how to implement the RADIUS Tunnel Preference for Load Balancing and Fail-Over feature in a RADIUS tunnel profile.

Configuration Example

The following example shows how to create RADIUS tunnel profiles:

```
net3 Password = "cisco" Service-Type = Outbound
    Tunnel-Type = :0:L2TP,
    Tunnel-Medium-Type = :0:IP,
    Tunnel-Server-Endpoint = :0:"1.1.3.1",
    Tunnel-Assignment-Id = :0:"1",
    Tunnel-Preference = :0:1,
    Tunnel-Password = :0:"welcome"

    Tunnel-Type = :1:L2TP,
    Tunnel-Medium-Type = :1:IP,
    Tunnel-Server-Endpoint = :1:"1.1.5.1",
    Tunnel-Assignment-Id = :1:"1",
    Tunnel-Preference = :1:1,
    Tunnel-Password = :1:"welcome"

    Tunnel-Type = :2:L2TP,
    Tunnel-Medium-Type = :2:IP,
    Tunnel-Server-Endpoint = :2:"1.1.4.1",
    Tunnel-Assignment-Id = :2:"1",
    Tunnel-Preference = :2:1,
    Tunnel-Password = :2:"welcome"

    Tunnel-Type = :3:L2TP,
    Tunnel-Medium-Type = :3:IP,
    Tunnel-Server-Endpoint = :3:"1.1.6.1",
    Tunnel-Assignment-Id = :3:"1",
    Tunnel-Preference = :3:1,
    Tunnel-Password = :3:"welcome"
```

The section [“Feature Overview”](#) describes how fail-over addresses are selected in these profiles. The section [“Related Documents”](#) lists documentation that describes how to create RADIUS tunnel profiles.

Command Reference

None

Glossary

HGW—home gateway. A gateway that terminates Layer 2 tunneling protocols such as L2TP.

home gateway—See HGW.

L2TP—Layer 2 Tunnel Protocol. An Internet Engineering Task Force (IETF) standards track protocol defined in RFC 2661 that provides tunneling of PPP. Based upon the best features of L2F and PPTP, L2TP provides an industry-wide interoperable method of implementing VPDN.

L2TP network server—See LNS.

Layer 2 Tunnel Protocol—See L2TP.

LNS—L2TP network server. A node that acts as one side of an L2TP tunnel endpoint and is a peer to the NAS or L2TP access concentrator (LAC). The LNS is the logical termination point of a PPP session that is being tunneled from the remote system by the access server. Analogous to the Layer 2 Forwarding (L2F) HGW.

NAS—network access server. Cisco platform or collection of platforms that interfaces between the packet world (the Internet, for example) and the circuit world (the public switched telephone network, for example).

network access server—See NAS.

Request for Comments—See RFCs.

RFCs—Request for Comments. A series of notes about the Internet collected by the Internet Engineering Task Force (IETF). Started in 1969, the IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture. RFCs define many aspects of computer communication, focusing on networking protocols, procedures, programs, and concepts.

virtual private dialup network—See VPDN.

VPDN—virtual private dialup network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



RADIUS Server Reorder on Failure

First Published: May 19, 2003

Last Updated: December 17, 2007

The RADIUS Server Reorder on Failure feature provides for failover to another server in the server group during periods of high load or when server failure occurs. Subsequent to the failure, all RADIUS traffic is directed to the new server. Traffic is switched from the new server to another server in the server group only if the new server also fails. Traffic is not automatically switched back to the first server.

By spreading the RADIUS transactions across multiple servers, authentication and accounting requests are serviced more quickly.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for RADIUS Server Reorder on Failure](#)” section on [page 12](#).

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for RADIUS Server Reorder on Failure, page 2](#)
- [Restrictions for RADIUS Server Reorder on Failure, page 2](#)
- [Information About RADIUS Server Reorder on Failure, page 2](#)
- [How to Configure RADIUS Server Reorder on Failure, page 3](#)
- [Configuration Examples for RADIUS Server Reorder on Failure, page 7](#)
- [Additional References, page 10](#)
- [Command Reference, page 11](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2003, 2006–2007 Cisco Systems, Inc. All rights reserved.

- [Feature Information for RADIUS Server Reorder on Failure, page 12](#)

Prerequisites for RADIUS Server Reorder on Failure

- Before you can configure your RADIUS server to perform reorder on failure, you must enable authentication, authorization, and accounting (AAA) by using the **aaa new-model** command. (Refer to the chapter “[AAA Overview](#)” in the *Cisco IOS Security Configuration Guide*, Release 12.3.)
- You must also have RADIUS configured, for functions such as authentication, accounting, or static route download.

Restrictions for RADIUS Server Reorder on Failure

- An additional 4 bytes of memory is required per server group. However, because most server configurations have only a small number of server groups configured, the additional 4 bytes should have a minimal impact on performance.
- Some RADIUS features within the Cisco IOS software set may not be capable of using this feature. If a RADIUS feature cannot use the RADIUS Server Reorder on Failure feature, your server behaves as though the reorder feature is not configured.

Information About RADIUS Server Reorder on Failure

To configure the RADIUS Server Reorder on Failure feature, you must understand the following concepts:

- [RADIUS Server Failure, page 2](#)
- [How the RADIUS Server Reorder on Failure Feature Works, page 3](#)

RADIUS Server Failure

If the RADIUS Server Reorder on Failure feature is not configured and server failure occurs:

1. A new RADIUS transaction has to be performed.
2. A RADIUS packet for the transaction is sent to the first server in the group that is not marked dead (as per the configured deadtime) and is retransmitted for the configured number of retransmissions.
3. If all of those retransmits time out (as per the configured timeout), the router transmits the packet to the next nondead server in the list for the configured number of retransmissions.
4. Step 3 is repeated until the specified maximum number of transmissions per transaction have been made. If the end of the list is reached before the maximum number of transmissions has been reached, the router goes back to the beginning of the list and continue from there.

If at any time during this process, a server meets the dead-server detection criteria (not configurable; it varies depending on the version of Cisco IOS software being used), the server is marked as dead for the configured deadtime.

How the RADIUS Server Reorder on Failure Feature Works

If you have configured the RADIUS Server Reorder on Failure feature, the decision about which RADIUS server to use as the initial server is as follows:

- The network access server (NAS) maintains the status of “flagged” server, which is the first server to which a transmission is sent.
- After the transmission is sent to the flagged server, the transmission is sent to the flagged server again for the configured number of retransmissions.
- The NAS then sequentially sends the transmission through the list of nondead servers in the server group, starting with the one listed after the flagged server, until the configured transaction maximum tries is reached or until a response is received.
- At boot time, the flagged server is the first server in the server group list as was established using the **radius-server host** command.
- If the flagged server is marked as dead (even if the dead time is zero), the first nondead server listed after the flagged server becomes the flagged server.
- If the flagged server is the last server in the list, and it is marked as dead, the flagged server becomes the first server in the list that is not marked as dead.
- If all servers are marked as dead, the transaction fails, and no change is made to the flagged server.
- If the flagged server is marked as dead, and the dead timer expires, nothing happens.

**Note**

Some types of transmissions (for example, Challenge Handshake Authentication Protocol [CHAP], Microsoft CHAP [MS-CHAP], and Extensible Authentication Protocol [EAP]) require multiple roundtrips to a single server. For these special transactions, the entire sequence of roundtrips to the server are treated as though they were one transmission.

When RADIUS Servers Are Dead

A server can be marked as dead if the criteria in 1 and 2 are met:

1. The server has not responded to at least the configured number of retransmissions as specified by the **radius-server transaction max-tries** command.
2. The server has not responded to any request for at least the configured timeout. The server is marked dead only if both criteria (this and the one listed above) are met. The marking of a server as dead, even if the dead time is zero, is significant for the RADIUS server retry method reorder system.

How to Configure RADIUS Server Reorder on Failure

This section contains the following procedures.

- [Configuring a RADIUS Server to Reorder on Failure, page 4](#) (required)
- [Monitoring RADIUS Server Reorder on Failure, page 5](#) (optional)

Configuring a RADIUS Server to Reorder on Failure

Perform this task to configure a server in a server group to direct traffic to another server in the server group when the first server fails.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server retry method reorder**
5. **radius-server retransmit {retries}**
6. **radius-server transaction max-tries {number}**
1. **radius-server host {hostname | ip-address} [key string]**
2. **radius-server host {hostname | ip-address} [key string]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Router (config)# aaa new-model	Enables the AAA access control model.
Step 4	radius-server retry method reorder Example: Router (config)# radius-server retry method reorder	Specifies the reordering of RADIUS traffic retries among a server group.
Step 5	radius-server retransmit {retries} Example: Router (config)# radius-server retransmit 1	Specifies the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up. The <i>retries</i> argument is the maximum number of retransmission attempts. The default is 3 attempts.

	Command or Action	Purpose
Step 6	radius-server transaction max-tries <i>{number}</i> Example: Router (config)# radius-server transaction max-tries 3	Specifies the maximum number of transmissions per transaction that may be retried on a RADIUS server. The <i>number</i> argument is the total number of transmissions per transaction. If this command is not configured, the default is eight transmissions. Note This command is global across all RADIUS servers for a given transaction.
Step 7	radius-server host <i>{hostname ip-address}</i> [key <i>string</i>] Example: Router (config)# radius-server host 10.2.3.4 key radi23	Specifies a RADIUS server host. Note You can also configure a global key for all RADIUS servers that do not have a per-server key configured by issuing the radius-server key command.
Step 8	radius-server host <i>{hostname ip-address}</i> [key <i>string</i>] Example: Router (config)# radius-server host 10.5.6.7 key rad234	Specifies a RADIUS server host. Note At least two servers must be configured.

Monitoring RADIUS Server Reorder on Failure

To monitor the server-reorder-on-failure process on your router, use the following commands:

SUMMARY STEPS

1. **enable**
2. **debug aaa sg-server selection**
3. **debug radius**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	debug aaa sg-server selection Example: Router# debug aaa sg-server selection	Displays information about why the RADIUS and TACAC+ server group system in the router is choosing a particular server.
Step 3	debug radius Example: Router# debug radius	Displays information about why the router is choosing a particular RADIUS server.

Examples

The following two debug outputs display the behavior of the RADIUS Server Reorder on Failure feature:

Debug 1

In the following sample output, the RADIUS Server Reorder on Failure feature is configured. The server retransmits are set to 0 (so each server is tried just one time before failover to the next configured server), and the transmissions per transaction are set to 4 (the transmissions stop on the third failover). The third server in the server group (10.107.164.118) has accepted the transaction on the third transmission (second failover).

```
00:38:35: %SYS-5-CONFIG-I: Configured from console by console
00:38:53: RADIUS/ENCODE(0000000F) : ask "Username: "
00:38:53: RADIUS/ENCODE(0000000F) : send packet; GET-USER
00:38:58: RADIUS/ENCODE(0000000F) : ask "Password: "
00:38:58: RADIUS/ENCODE(0000000F) : send packet; GET-PASSWORD
00:38:59: RADIUS: AAA Unsupported [152] 4
00:38:59: RADIUS: 7474 [tt]
00:38:59: RADIUS(0000000F) : Storing nasport 2 in rad-db
00:38:59: RADIUS/ENCODE(0000000F) : dropping service type, "radius-server attribute 6
on-for-login-auth" is off
00:38:59: RADIUS(0000000F) : Config NAS IP: 0.0.0.0
00:38:59: RADIUS/ENCODE(0000000F) : acct-session-id: 15
00:38:59: RADIUS(0000000F) : sending
00:38:59: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 192.1.1.1
00:38:59: RADIUS(0000000F) : Send Access-Request to 10.10.10.10:1645 id 21645/11, len 78
00:38:59: RADIUS:: authenticator 4481 E6 65 2D 5F 6F OA -1E F5 81 8F 4E 1478 9C
00:38:59: RADIUS: User-Name [1] 7 "username1"
00:38:59: RADIUS: User-Password [2] 18 *
00:38:59: RADIUS: NAS-Port fsl 6 2
00:38:59: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
00:38:59: RADIUS: Calling-Station-Id [31] 15 "10.19.192.23"
00:39:00: RADIUS: NAS-IP-Address [4] 6 10.0.1.130
00:39:02: RADIUS: Fail-over to (10.2.2.2:1645,1646) for id 21645/11
00:39:02: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 192.2.2.2
00:39:04: RADIUS: Fail-over to (10.107.164.118:1645,1646) for id 21645/11
00:39:04: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server
128.107.164.118
```



```
00:39:05: RADIUS: Received from id 21645/11 10.107.164.118:1645, Access-Accept, len 26
00:39:05: RADIUS: authenticator 5609 56 F9 64 4E DF 19- F3 A2 DD 73 EE 3F 9826
00:39:05: RADIUS: Service-Type [6] 6 Login [1]
```

Debug 2

In the following sample output, the RADIUS Server Reorder on Failure feature is configured. The server retransmits are set to 0, and the transmissions per transaction are set to 8. In this transaction, the transmission to server 10.10.10.0 has failed on the eighth transmission.

```
00:42:30: RADIUS(00000011): Received from id 21645/13
00:43:34: RADIUS/ENCODE(00000012) : ask "Username: "
00:43:34: RADIUS/ENCODE(00000012) : send packet; GET-USER
00:43:39: RADIUS/ENCODE(00000012) : ask "Password: "
00:43:39: RADIUS/ENCODE(00000012) : send packet; GET-PASSWORD
00:43:40: RADIUS: AAA Unsupported [152] 4
00:43:40: RADIUS: 7474 [tt]
00:43:40: RADIUS(00000012) : Storing nasport 2 in rad-db
00:43:40: RADIUS/ENCODE(00000012): dropping service type, "radius-server attribute 6
on-for-login-auth" is off
00:43:40: RADIUS(00000012) : Co~fig NAS IP: 0.0.0.0
00:43:40: RADIUS/ENCODE(00000012) : acct-session-id: 18
00:43:40: RADIUS(00000012) : sending
00:43:40: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.107.164.118
00:43:40: RADIUS(00000012) : Send Access-Request to 10.107.164.118:1645 id 21645/14, len
78 00:43:40: RADIUS: authenticator B8 OA 51 3A AF A6 0018 -B3 2E 94 5E 07 OB 2A IF
00:43:40: RADIUS: User-Name [1] 7 "username1" 00:43:40: RADIUS: User-Password [2] 18 *
00:43:40: RADIUS: NAS-Port [5] 6 2
00:43:40: RADIUS: NAS-Port-Type [61] 6 Virtual [5] 00:43:40: RADIUS: Calling-Station-]d
[31] 15 "172.19.192.23" 00:43:40: RADIUS: NAS-IP-Address [4] 6 10.0.1.130
00:43:42: RADIUS: Fail-over to (10.10.10.10:1645,1646) for id 21645/14
00:43:42: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.1.1.1
00:43:44: RADIUS: Fail-over to (10.2.2.2:1645,1646) for id 21645/14
00:43:44: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.2.2.2
00:43:46: RADIUS: Fail-over to (10.107.164.118:1645,1646) for id 21645/14
00:43:46: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.107.164.118
00:43:48: RADIUS: Fail-over to (10.10.10.10:1645,1646) for id 21645/14
00:43:48: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.1.1.1
00:43:50: RADIUS: Fail-over to (10.2.2.2:1645,1646) for id 21645/14
00:43:50: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.2.2.2
00:43:52: RADIUS: Fail-over to (10.107.164.118:1645,1646) for id 21645/14
00:43:52: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.107.164.118
00:43:54: RADIUS: Fail-over to (10.10.10.10:1645,1646) for id 21645/14
00:43:54: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.1.1.1
00:43:56: RADIUS: No response from (10.10.10.10:1645,1646) for id 21645/14 00:43:56:
RADIUS/DECODE: parse response no app start; FAIL 00:43:56: RADIUS/DECODE: parse response;
FAIL
```

Configuration Examples for RADIUS Server Reorder on Failure

This section provides the following configuration examples:

- [Configuring a RADIUS Server to Reorder on Failure Example, page 8](#)
- [Determining Transmission Order When RADIUS Servers Are Dead, page 8](#)

Configuring a RADIUS Server to Reorder on Failure Example

The following configuration example shows that a RADIUS server is configured to reorder on failure. The maximum number of transmissions per transaction that may be retried on the RADIUS server is six.

```
aaa new-model
radius-server retry method reorder
radius-server retransmit 0
radius-server transaction max-tries 6
radius-server host 10.2.3.4 key rad123
radius-server host 10.5.6.7 key rad123
```

Determining Transmission Order When RADIUS Servers Are Dead

If at boot time you have configured the following:

```
aaa new-model
radius-server retry method reorder
radius-server retransmit 0
radius-server transaction max-tries 6
radius-server host 10.2.3.4
radius-server host 10.5.6.7
```

and both servers are down, but not yet marked dead, for the first transaction you would see the transmissions as follows:

```
10.2.3.4
10.5.6.7
10.2.3.4
10.5.6.7
10.2.3.4
10.5.6.7
```

If you configure the reorder as follows:

```
aaa new-model
radius-server retry method reorder
radius-server retransmit 1
radius-server transaction max-tries 3
radius-server host 10.2.3.4
radius-server host 10.4.5.6
```

and both RADIUS servers are not responding to RADIUS packets but are not yet marked dead (as after the NAS boots), the transmissions for the first transaction are as follows:

```
10.2.3.4
10.2.3.4
10.4.5.6
```

Subsequent transactions may be transmitted according to a different pattern. The transmissions depend on whether the criteria for marking one (or both) servers as dead have been met, and as per the server flagging pattern already described.

If you configure the reorder as follows:

```
aaa new-model
radius-server retry method reorder
radius-server retransmit 1
radius-server max-tries-per-transaction 8
radius-server host 10.1.1.1
radius-server host 10.2.2.2
radius-server host 10.3.3.3
radius-server timeout 3
```

And the RADIUS server 10.1.1.1 is not responding to RADIUS packets but is not yet marked as dead, and the remaining two RADIUS servers are live, you see the following:

For the first transaction:

```
10.1.1.1
10.1.1.1
10.2.2.2
```

For any additional transaction initiated for any transmissions before the server is marked as dead:

```
10.1.1.1
10.1.1.1
10.2.2.2
```

For transactions initiated thereafter:

```
10.2.2.2
```

If servers 10.2.2.2 and 10.3.3.3 then go down as well, you see the following transmissions until servers 10.2.2.2 and 10.3.3.3 meet the criteria for being marked as dead:

```
10.2.2.2
10.2.2.2
10.3.3.3
10.3.3.3
10.1.1.1
10.1.1.1
10.2.2.2
10.2.2.2
```

The above is followed by the failure of the transmission and by the next method in the method list being used (if any).

If servers 10.2.2.2 and 10.3.3.3 go down but server 10.1.1.1 comes up at the same time, you see the following:

```
10.2.2.2
10.2.2.2
10.3.3.3
10.3.3.3
10.1.1.1
```

When servers 10.2.2.2 and 10.3.3.3 are then marked as dead, you see the following:

```
10.1.1.1
```

Additional References

The following sections provide references related to RADIUS Server Reorder on Failure.

Related Documents

Related Topic	Document Title
RADIUS	The chapter “ Configuring RADIUS ” in the <i>Cisco IOS Security Configuration Guide</i>
AAA and RADIUS commands	Cisco IOS Security Command Reference
Enabling AAA	“ AAA Overview ” chapter in the <i>Cisco IOS Security Configuration Guide</i>

Standards

Standards	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug aaa sg-server selection**
- **radius-server retry method reorder**
- **radius-server transaction max-tries**

Feature Information for RADIUS Server Reorder on Failure

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for RADIUS Server Reorder on Failure

Feature Name	Releases	Feature Information
RADIUS Server Reorder on Failure	12.3(1) 12.2(28)SB 12.2(33)SRC Cisco IOS XE Release 2.1	The RADIUS Server Reorder on Failure feature provides for failover to another server in the server group during periods of high load or when server failure occurs. This feature was introduced in 12.3(1). This feature was integrated into Cisco IOS Release 12.2(28)SB. This feature was integrated into Cisco IOS Release 12.2(33)SRC. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers. The following commands were introduced or modified by this feature: debug aaa sg-server selection, radius-server retry method reorder, radius-server transaction max-tries.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2003, 2006–2007 Cisco Systems, Inc. All rights reserved.



Tunnel Authentication via RADIUS on Tunnel Terminator

Feature History

Release	Modification
12.2(15)B	This feature was introduced on the Cisco 6400 series, Cisco 7200 series, and Cisco 7400 series.
12.3(4)T	This feature was integrated into Cisco IOS Release 12.3(4)T.

- [Feature Overview, page 1](#)
- [Supported Platforms, page 3](#)
- [Supported Standards, MIBs, and RFCs, page 4](#)
- [Prerequisites, page 4](#)
- [Configuration Tasks, page 4](#)
- [Configuration Examples, page 6](#)
- [Command Reference, page 7](#)
- [Glossary, page 8](#)

Feature Overview

The Tunnel Authentication via RADIUS on Tunnel Terminator feature allows the Layer 2 Tunneling Protocol (L2TP) network server (LNS) to perform remote authentication and authorization with RADIUS on incoming L2TP access concentrator (LAC) dialin connection requests. This feature also allows the L2TP LAC to perform remote authentication and authorization with RADIUS on incoming L2TP LNS dialout connection requests.

Before the introduction of this feature, the LNS could only perform L2TP tunnel authentication and authorization locally. These processes can be difficult to maintain across numerous LNSs, especially if the number of virtual private dialup network (VPDN) groups is large, because the LAC information must be configured under the VPDN group configurations of the LNS. Remote RADIUS authentication and authorization allows users to store the LAC configurations on the RADIUS server, thereby avoiding the



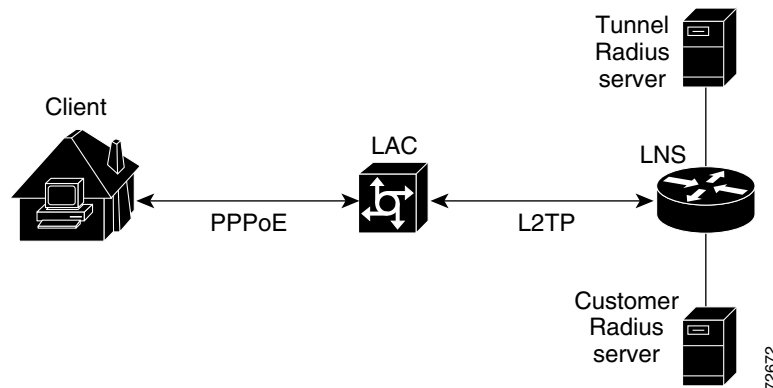
Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

need to store information locally. Thus, the new LAC information can be added to the RADIUS server as necessary, and the group of LNSs can authenticate and authorize by using a common user database on RADIUS.

Figure 1 and the corresponding steps explain how this feature works.

Figure 1 *LNS Remote RADIUS Tunnel Authentication and Authorization for L2TP Dialin Calls Topology*



- After the LNS receives a start-control-connection request (SCCRQ), it starts tunnel authentication and submits a request to RADIUS with the LAC hostname and the dummy password “cisco.” (If the LNS determines that authorization should be performed locally, it will search the VPDN group configurations.)



Note To change the dummy password, use the **vpdn tunnel authorization password** command.

- If the password sent by the LNS matches the password that is configured in the RADIUS server, the server will return attribute 90 (Tunnel-Client-Auth-ID) and attribute 69 (Tunnel-Password) after the LAC information is located. Otherwise, the RADIUS server replies back with an access-reject, and the LNS drops the tunnel.
- The LNS will check for the following attribute information from the RADIUS reply:
 - Attribute 90 (Tunnel-Client-Auth-ID), which is used as the LAC hostname. If this attribute does not match the LAC hostname, the tunnel will be dropped.
 - Attribute 69 (Tunnel-Password), which is used for the L2TP CHAP-like authentication shared secret. This attribute is compared against the LAC challenge attribute-value pair (AVP) that was received in the SCCRQ. If this attribute does not match the AVP, the tunnel will be dropped.
- If both attributes match, the L2TP tunnel will be established. Thereafter, you can proceed with PPP negotiation and authentication with the remote client.



Note PPP remote authentication is done to a potential different customer RADIUS server by a separate access-request/access-accept sequence. The tunnel authorization may be done by a different tunnel RADIUS server.

New RADIUS Attributes

To help implement this feature, the following two new Cisco-specific RADIUS attributes have been introduced:

- Cisco:Cisco-Avpair = “vpdn:dout-dialer = <LAC dialer number>”—Specifies which LAC dialer to use on the LAC for a dialout configuration.
- Cisco:Cisco-Avpair = “vpdn:vpdn-vtemplate = <vtemplate number>”—Specifies the virtual template number that will be used for cloning on the LNS for a dialin configuration. (This attribute is the RADIUS counterpart for the virtual-template under the vpdn-group configuration.)

**Note**

The service-type in the RADIUS user’s profile for the tunnel initiator should always be set to “Outbound.”

Benefits

This feature allows tunnel authentication and authorization to occur via a remote RADIUS server instead of local configuration on the tunnel terminator. Thus, users no longer have to configure LAC or LNS data in a VPDN group when an LNS or LAC is configured for incoming dialin or dialout L2TP tunnel termination; this information can now be added to a remote RADIUS server, providing a more manageable and scalable solution for L2TP tunnel authentication and authorization on the tunnel terminator.

Restrictions

This is applicable only to L2TP; that is, protocols such as (Layer 2 Forwarding) L2F and Point-to-Point Tunneling Protocol (PPTP) are not supported.

Related Documents

- The chapter “Configuring Virtual Private Networks” in the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2
- The appendix “RADIUS Attributes” in the *Cisco IOS Security Configuration Guide*, Release 12.2
- *Cisco IOS Dial Technologies Command Reference*, Release 12.2
- *Cisco IOS Security Command Reference*, Release 12.2

Supported Platforms

- Cisco 6400 series
- Cisco 7200 series
- Cisco 7400 series

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

RFCs

RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*

Prerequisites

Before configuring this feature, you should define a RADIUS server group. For information on completing this task, refer to the chapter “Configuring RADIUS” in the *Cisco IOS Security Configuration Guide*, Release 12.2.

Configuration Tasks

See the following sections for configuration tasks for the Tunnel Authentication via RADIUS on Tunnel Terminator feature. Each task in the list is identified as either required or optional.

- [Configuring the LNS or LAC for Remote RADIUS Tunnel Authentication and Authorization](#) (required)
- [Verifying Remote RADIUS Tunnel Authentication and Authorization Configurations](#) (optional)

Configuring the LNS or LAC for Remote RADIUS Tunnel Authentication and Authorization

To configure an LNS or LAC for incoming dialin or dialout L2TP tunnel termination, use the following commands in global configuration:

	Command	Purpose
Step 1	Router(config)# aaa authorization network { default <i>list-name</i> } <i>method1</i> [<i>method2...</i>]	Defines an AAA authorization method list for network services.
Step 2	Router(config)# vpdn tunnel authorization network { <i>method-list-name</i> default }	Specifies the AAA authorization method list that will be used for remote tunnel hostname-based authorization. <ul style="list-style-type: none"> If the <i>list-name</i> argument was specified in the aaa authorization command, you use that list name here. If the default keyword was specified in the aaa authorization command, you must choose that keyword, which specifies the default authorization methods that are listed with the aaa authorization command here.
Step 3	Router(config)# vpdn tunnel authorization virtual-template <i>vtemplate-number</i>	(Optional) Selects the default virtual template from which to clone virtual access interfaces.
Step 4	Router(config)# vpdn tunnel authorization password <i>password</i>	(Optional) Configures a “dummy” password for the RADIUS authorization request to retrieve the tunnel configuration that is based on the remote tunnel hostname. <p>Note If this command is not enabled, the password will always be “cisco.”</p>

Verifying Remote RADIUS Tunnel Authentication and Authorization Configurations

To verify that the L2TP tunnel is up, use the **show vpdn tunnel** command in EXEC mode. One tunnel and one session must be set up.

```
Router# show vpdn tunnel
```

```
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name  State Remote Address  Port  Sessions VPDN Group
4571  61568 csidtw13 est    10.0.195.4      1701  1         ?
```

```
LocID RemID TunID Intf      Username                      State Last Chg
4      11      4571 Vi4.1      csidtw9@cisco.com            est   00:02:29
```

```
%No active L2F tunnels
%No active PPTP tunnels
%No active PPPoE tunnels
```

To verify that the AAA authorization RADIUS server is configured on the LNS and that the LNS can receive attributes 90 and 69 from the RADIUS server, perform the following steps:

Step 1 Enable the **debug radius** command on the LNS.

Step 2 Enable the **show logging** command on the LNS and ensure that “access-accept” is in the output and that attributes 90 and 69 can be seen in the RADIUS reply.

```
00:32:56: RADIUS: Received from id 21645/5 172.19.192.50:1645, Access-Accept, len 81
00:32:56: RADIUS:  authenticator 73 2B 1B C2 33 71 93 19 - 62 AC 3E BE 0D 13 14 85
00:32:56: RADIUS:  Service-Type      [6]  6  Outbound                               [5]
00:32:56: RADIUS:  Tunnel-Type      [64]  6  00:L2TP                               [3]
00:32:56: RADIUS:  Tunnel-Medium-Type [65]  6  00:IPv4                               [1]
```

```

00:32:56: RADIUS: Tunnel-Client-Auth-I[90] 6 00:"csidtwl3"
00:32:56: RADIUS: Tunnel-Password [69] 8 *
00:32:56: RADIUS: Vendor, Cisco [26] 29
00:32:56: RADIUS: Cisco AVpair [1] 23 "vpdn:vpdn-vtemplate=1"

```

To verify that the L2TP tunnel has been established and that the LNS can perform PPP negotiation and authentication with the remote client, perform the following steps:

-
- Step 1** Enable the **debug ppp negotiation** and **debug ppp authentication** commands on LNS.
- Step 2** Enable the **show logging** command on LNS and observe that LNS receives a PPP CHAP challenge and then sends a PPP CHAP “SUCCESS” to the client.

```

00:38:50: ppp3 PPP: Received LOGIN Response from AAA = PASS
00:38:50: ppp3 PPP: Phase is FORWARDING, Attempting Forward
00:38:50: Vi4.1 Tnl/Sn4571/4 L2TP: Session state change from wait-for-service-selection
to established
00:38:50: Vi4.1 PPP: Phase is AUTHENTICATING, Authenticated User
00:38:50: Vi4.1 CHAP: O SUCCESS id 1 len 4

```

- Step 3** After PPP authentication is successful, observe from the debug output that PPP negotiation has started, that the LNS has received LCP (IPCP) packets, and that negotiation is successful.

```

00:38:50: Vi4.1 IPCP: State is Open
00:38:50: Vi4.1 IPCP: Install route to 200.1.1.4

```

Configuration Examples

This section provides the following configuration examples:

- [L2TP Network Server \(LNS\) Configuration Example](#)
- [RADIUS User Profile for Remote RADIUS Tunnel Authentication Example](#)

L2TP Network Server (LNS) Configuration Example

The following example shows how to configure the LNS to enable remote RADIUS tunnel authentication and authorization:

```

! Define a RADIUS server group
aaa group server radius VPDN-group
 server 64.102.48.91 auth-port 1645 acct-port 1646
!
! RADIUS configurations only
aaa authorization network mymethodlist group VPDN-Group
vpdn tunnel authorization network mymethodlist
vpdn tunnel authorization virtual-template 10

```

RADIUS User Profile for Remote RADIUS Tunnel Authentication Example

The following are examples of RADIUS user profiles for the LNS to terminate L2TP tunnels from a LAC. In the first user profile, the final line is optional if the **vpdn tunnel authorization virtual-template** command is used. Also, the first RADIUS user profile is for L2TP dialin, and the second RADIUS user profile is for L2TP dialout.

The service-type in the RADIUS user's profile for the tunnel initiator should always be set to "Outbound."

```
csidtw13 Password = "cisco"
        Service-Type = Outbound,
        Tunnel-Type = :0:L2TP,
        Tunnel-Medium-Type = :0:IP,
        Tunnel-Client-Auth-ID = :0:"csidtw13",
        Tunnel-Password = :0:"cisco"
        Cisco:Cisco-Avpair = "vpdn:vpdn-vtemplate=1"

csidtw1 Password = "cisco"
        Service-Type = Outbound,
        Tunnel-Type = :0:L2TP,
        Tunnel-Medium-Type = :0:IP,
        Tunnel-Client-Auth-ID = :0:"csidtw1",
        Tunnel-Password = :0:"cisco"
        Cisco:Cisco-Avpair = "vpdn:dout-dialer=2"
```

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **vpdn tunnel authorization network**
- **vpdn tunnel authorization password**
- **vpdn tunnel authorization virtual-template**

Glossary

L2TP—Layer 2 Tunnel Protocol. A Layer 2 tunneling protocol that enables an ISP or other access service to create a virtual tunnel to link customer remote sites or remote users with corporate home networks. In particular, a network access server (NAS) at the ISP point of presence (POP) exchanges PPP messages with the remote users and communicates by L2F or L2TP requests and responses with the customer tunnel server to set up tunnels.

LAC—L2TP access concentrator. A network access server (NAS) to which the client directly connects and through which PPP frames are tunneled to the L2TP network server (LNS). The LAC need only implement the media over which L2TP is to operate to pass traffic to one or more LNSs. The LAC may tunnel any protocol carried within PPP. The LAC initiates incoming calls and receives outgoing calls. A LAC is analogous to an L2F network access server.

LNS—L2TP network server. A termination point for L2TP tunnels and an access point where PPP frames are processed and passed to higher layer protocols. An LNS can operate on any platform that terminates PPP. The LNS handles the server side of the L2TP protocol. L2TP relies only on the single medium over which L2TP tunnels arrive. The LNS initiates outgoing calls and receives incoming calls. An LNS is analogous to a home gateway in L2F technology.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



TACACS+



Configuring TACACS+

Feature History

Release	Modification
Cisco IOS	For information about feature support in Cisco IOS software, use Cisco Feature Navigator.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

This chapter discusses how to enable and configure TACACS+, which provides detailed accounting information and flexible administrative control over authentication and authorization processes. TACACS+ is facilitated through AAA and can be enabled only through AAA commands.

For a complete description of the TACACS+ commands used in this chapter, refer to the chapter “TACACS+ Commands” in the *Cisco IOS Security Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature, or refer to the software release notes for a specific release. For more information, see the section “Identifying Supported Platforms” in the chapter “Using Cisco IOS Software.”

In This Chapter

This chapter includes the following sections:

- [About TACACS+](#)
- [TACACS+ Operation](#)
- [TACACS+ Configuration Task List](#)
- [TACACS+ AV Pairs](#)
- [TACACS+ Configuration Examples](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

About TACACS+

TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or network access server. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation. You must have access to and must configure a TACACS+ server before the configured TACACS+ features on your network access server are available.

TACACS+ provides for separate and modular authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service—authentication, authorization, and accounting—independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

The goal of TACACS+ is to provide a methodology for managing multiple network access points from a single management service. The Cisco family of access servers and routers and the Cisco IOS user interface (for both routers and access servers) can be network access servers.

Network access points enable traditional “dumb” terminals, terminal emulators, workstations, personal computers (PCs), and routers in conjunction with suitable adapters (for example, modems or ISDN adapters) to communicate using protocols such as Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), Compressed SLIP (CSLIP), or AppleTalk Remote Access (ARA) protocol. In other words, a network access server provides connections to a single user, to a network or subnetwork, and to interconnected networks. The entities connected to the network through a network access server are called *network access clients*; for example, a PC running PPP over a voice-grade circuit is a network access client. TACACS+, administered through the AAA security services, can provide the following services:

- **Authentication**—Provides complete control of authentication through login and password dialog, challenge and response, messaging support.

The authentication facility provides the ability to conduct an arbitrary dialog with the user (for example, after a login and password are provided, to challenge a user with a number of questions, like home address, mother’s maiden name, service type, and social security number). In addition, the TACACS+ authentication service supports sending messages to user screens. For example, a message could notify users that their passwords must be changed because of the company’s password aging policy.
- **Authorization**—Provides fine-grained control over user capabilities for the duration of the user’s session, including but not limited to setting autocommands, access control, session duration, or protocol support. You can also enforce restrictions on what commands a user may execute with the TACACS+ authorization feature.
- **Accounting**—Collects and sends information used for billing, auditing, and reporting to the TACACS+ daemon. Network managers can use the accounting facility to track user activity for a security audit or to provide information for user billing. Accounting records include user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

The TACACS+ protocol provides authentication between the network access server and the TACACS+ daemon, and it ensures confidentiality because all protocol exchanges between a network access server and a TACACS+ daemon are encrypted.

You need a system running TACACS+ daemon software to use the TACACS+ functionality on your network access server.

Cisco makes the TACACS+ protocol specification available as a draft RFC for those customers interested in developing their own TACACS+ software.

TACACS+ Operation

When a user attempts a simple ASCII login by authenticating to a network access server using TACACS+, the following process typically occurs:

1. When the connection is established, the network access server will contact the TACACS+ daemon to obtain a username prompt, which is then displayed to the user. The user enters a username and the network access server then contacts the TACACS+ daemon to obtain a password prompt. The network access server displays the password prompt to the user, the user enters a password, and the password is then sent to the TACACS+ daemon.

**Note**

TACACS+ allows an arbitrary conversation to be held between the daemon and the user until the daemon receives enough information to authenticate the user. This is usually done by prompting for a username and password combination, but may include other items, such as mother's maiden name, all under the control of the TACACS+ daemon.

2. The network access server will eventually receive one of the following responses from the TACACS+ daemon:
 - a. **ACCEPT**—The user is authenticated and service may begin. If the network access server is configured to require authorization, authorization will begin at this time.
 - b. **REJECT**—The user has failed to authenticate. The user may be denied further access, or will be prompted to retry the login sequence depending on the TACACS+ daemon.
 - c. **ERROR**—An error occurred at some time during authentication. This can be either at the daemon or in the network connection between the daemon and the network access server. If an **ERROR** response is received, the network access server will typically try to use an alternative method for authenticating the user.
 - d. **CONTINUE**—The user is prompted for additional authentication information.
3. A PAP login is similar to an ASCII login, except that the username and password arrive at the network access server in a PAP protocol packet instead of being typed in by the user, so the user is not prompted. PPP CHAP logins are also similar in principle.

Following authentication, the user will also be required to undergo an additional authorization phase, if authorization has been enabled on the network access server. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

4. If TACACS+ authorization is required, the TACACS+ daemon is again contacted and it returns an **ACCEPT** or **REJECT** authorization response. If an **ACCEPT** response is returned, the response will contain data in the form of attributes that are used to direct the **EXEC** or **NETWORK** session for that user, determining services that the user can access.

Services include the following:

- a. Telnet, rlogin, Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), or EXEC services
- b. Connection parameters, including the host or client IP address, access list, and user timeouts

TACACS+ Configuration Task List

To configure your router to support TACACS+, you must perform the following tasks:

- Use the **aaa new-model** global configuration command to enable AAA. AAA must be configured if you plan to use TACACS+. For more information about using the **aaa new-model** command, refer to the chapter “AAA Overview”.
- Use the **tacacs-server host** command to specify the IP address of one or more TACACS+ daemons. Use the **tacacs-server key** command to specify an encryption key that will be used to encrypt all exchanges between the network access server and the TACACS+ daemon. This same key must also be configured on the TACACS+ daemon.
- Use the **aaa authentication** global configuration command to define method lists that use TACACS+ for authentication. For more information about using the **aaa authentication** command, refer to the chapter “Configuring Authentication”.
- Use **line** and **interface** commands to apply the defined method lists to various interfaces. For more information, refer to the chapter “Configuring Authentication”.
- If needed, use the **aaa authorization** global command to configure authorization for the network access server. Unlike authentication, which can be configured per line or per interface, authorization is configured globally for the entire network access server. For more information about using the **aaa authorization** command, refer to the “Configuring Authorization” chapter.
- If needed, use the **aaa accounting** command to enable accounting for TACACS+ connections. For more information about using the **aaa accounting** command, refer to the “Configuring Accounting” chapter.

To configure TACACS+, perform the tasks in the following sections:

- [Identifying the TACACS+ Server Host](#) (Required)
- [Setting the TACACS+ Authentication Key](#) (Optional)
- [Configuring AAA Server Groups](#) (Optional)
- [Configuring AAA Server Group Selection Based on DNIS](#) (Optional)
- [Specifying TACACS+ Authentication](#) (Required)
- [Specifying TACACS+ Authorization](#) (Optional)
- [Specifying TACACS+ Accounting](#) (Optional)

For TACACS+ configuration examples using the commands in this chapter, refer to the “[TACACS+ Configuration Examples](#)” section at the end of this chapter.

Identifying the TACACS+ Server Host

The **tacacs-server host** command enables you to specify the names of the IP host or hosts maintaining a TACACS+ server. Because the TACACS+ software searches for the hosts in the order specified, this feature can be useful for setting up a list of preferred daemons.

To specify a TACACS+ host, use the following command in global configuration mode:

Command	Purpose
Router(config)# tacacs-server host <i>hostname</i> [single-connection] [port <i>integer</i>] [timeout <i>integer</i>] [key <i>string</i>]	Specifies a TACACS+ host.

Using the **tacacs-server host** command, you can also configure the following options:

- Use the **single-connection** keyword to specify single-connection (only valid with CiscoSecure Release 1.0.1 or later). Rather than have the router open and close a TCP connection to the daemon each time it must communicate, the single-connection option maintains a single open connection between the router and the daemon. This is more efficient because it allows the daemon to handle a higher number of TACACS operations.



Note The daemon must support single-connection mode for this to be effective, otherwise the connection between the network access server and the daemon will lock up or you will receive spurious errors.

- Use the **port** *integer* argument to specify the TCP port number to be used when making connections to the TACACS+ daemon. The default port number is 49.
- Use the **timeout** *integer* argument to specify the period of time (in seconds) the router will wait for a response from the daemon before it times out and declares an error.



Note Specifying the timeout value with the **tacacs-server host** command overrides the default timeout value set with the **tacacs-server timeout** command for this server only.

- Use the **key** *string* argument to specify an encryption key for encrypting and decrypting all traffic between the network access server and the TACACS+ daemon.



Note Specifying the encryption key with the **tacacs-server host** command overrides the default key set by the global configuration **tacacs-server key** command for this server only.

Because some of the parameters of the **tacacs-server host** command override global settings made by the **tacacs-server timeout** and **tacacs-server key** commands, you can use this command to enhance security on your network by uniquely configuring individual TACACS+ connections.

Setting the TACACS+ Authentication Key

To set the global TACACS+ authentication key and encryption key, use the following command in global configuration mode:

Command	Purpose
Router(config)# tacacs-server key <i>key</i>	Sets the encryption key to match that used on the TACACS+ daemon.



Note You must configure the same key on the TACACS+ daemon for encryption to be successful.

Configuring AAA Server Groups

Configuring the router to use AAA server groups provides a way to group existing server hosts. This allows you to select a subset of the configured server hosts and use them for a particular service. A server group is used in conjunction with a global server-host list. The server group lists the IP addresses of the selected server hosts.

Server groups can include multiple host entries as long as each entry has a unique IP address. If two different host entries in the server group are configured for the same service—for example, accounting—the second host entry configured acts as fail-over backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server will try the second host entry for accounting services. (The TACACS+ host entries will be tried in the order in which they are configured.)

To define a server host with a server group name, enter the following commands starting in global configuration mode. The listed server must exist in global configuration mode:

	Command	Purpose
Step 1	Router(config)# tacacs-server host <i>name</i> [single-connection] [port <i>integer</i>] [timeout <i>integer</i>] [key <i>string</i>]	Specifies and defines the IP address of the server host before configuring the AAA server-group. Refer to the “ Identifying the TACACS+ Server Host ” section of this chapter for more information on the tacacs-server host command.
Step 2	Router(config-if)# aaa group server { radius tacacs+ } <i>group-name</i>	Defines the AAA server-group with a group name. All members of a group must be the same type; that is, RADIUS or TACACS+. This command puts the router in server group subconfiguration mode.
Step 3	Router(config-sg)# server <i>ip-address</i> [auth-port <i>port-number</i>] [acct-port <i>port-number</i>]	Associates a particular TACACS+ server with the defined server group. Use the auth-port <i>port-number</i> option to configure a specific UDP port solely for authentication. Use the acct-port <i>port-number</i> option to configure a specific UDP port solely for accounting. Repeat this step for each TACACS+ server in the AAA server group. Note Each server in the group must be defined previously using the tacacs-server host command.

Configuring AAA Server Group Selection Based on DNIS

Cisco IOS software allows you to authenticate users to a particular AAA server group based on the Dialed Number Identification Service (DNIS) number of the session. Any phone line (a regular home phone or a commercial T1/PRI line) can be associated with several phone numbers. The DNIS number identifies the number that was called to reach you.

For example, suppose you want to share the same phone number with several customers, but you want to know which customer is calling before you pick up the phone. You can customize how you answer the phone because DNIS allows you to know which customer is calling when you answer.

Cisco routers with either ISDN or internal modems can receive the DNIS number. This functionality allows users to assign different TACACS+ server groups for different customers (that is, different TACACS+ servers for different DNIS numbers). Additionally, using server groups you can specify the same server group for AAA services or a separate server group for each AAA service.

Cisco IOS software provides the flexibility to implement authentication and accounting services in several ways:

- Globally—AAA services are defined using global configuration access list commands and applied in general to all interfaces on a specific network access server.
- Per interface—AAA services are defined using interface configuration commands and applied specifically to the interface being configured on a specific network access server.
- DNIS mapping—You can use DNIS to specify an AAA server to supply AAA services.

Because AAA configuration methods can be configured simultaneously, Cisco has established an order of precedence to determine which server or groups of servers provide AAA services. The order of precedence is as follows:

- Per DNIS—If you configure the network access server to use DNIS to identify which server group provides AAA services, then this method takes precedence over any additional AAA selection method.
- Per interface—If you configure the network access server per interface to use access lists to determine how a server provides AAA services, this method takes precedence over any global configuration AAA access lists.
- Globally—If you configure the network access server by using global AAA access lists to determine how the security server provides AAA services, this method has the lowest precedence.



Note

Prior to configuring AAA Server Group Selection Based on DNIS, you must configure the remote security servers associated with each AAA server group. See the sections [“Identifying the TACACS+ Server Host”](#) and [“Configuring AAA Server Groups”](#) in this chapter.

To configure the router to select a particular AAA server group based on the DNIS of the server group, configure DNIS mapping. To map a server group with a group name with DNIS number, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# aaa dnis map enable	Enables DNIS mapping.
Step 2	Router(config)# aaa dnis map <i>dnis-number</i> authentication ppp group <i>server-group-name</i>	Maps a DNIS number to a defined AAA server group; the servers in this server group are being used for authentication.
Step 3	Router(config)# aaa dnis map <i>dnis-number</i> accounting network [none start-stop stop-only] group <i>server-group-name</i>	Maps a DNIS number to a defined AAA server group; the servers in this server group are being used for accounting.

Specifying TACACS+ Authentication

After you have identified the TACACS+ daemon and defined an associated TACACS+ encryption key, you must define method lists for TACACS+ authentication. Because TACACS+ authentication is operated via AAA, you need to issue the **aaa authentication** command, specifying TACACS+ as the authentication method. For more information, refer to the chapter “Configuring Authentication.”

Specifying TACACS+ Authorization

AAA authorization enables you to set parameters that restrict a user’s access to the network. Authorization via TACACS+ may be applied to commands, network connections, and EXEC sessions. Because TACACS+ authorization is facilitated through AAA, you must issue the **aaa authorization** command, specifying TACACS+ as the authorization method. For more information, refer to the chapter “Configuring Authorization.”

Specifying TACACS+ Accounting

AAA accounting enables you to track the services users are accessing as well as the amount of network resources they are consuming. Because TACACS+ accounting is facilitated through AAA, you must issue the **aaa accounting** command, specifying TACACS+ as the accounting method. For more information, refer to the chapter “Configuring Accounting.”

TACACS+ AV Pairs

The network access server implements TACACS+ authorization and accounting functions by transmitting and receiving TACACS+ attribute-value (AV) pairs for each user session. For a list of supported TACACS+ AV pairs, refer to the appendix “TACACS+ Attribute-Value Pairs.”

TACACS+ Configuration Examples

The following sections provide TACACS+ configuration examples:

- [TACACS+ Authentication Examples](#)
- [TACACS+ Authorization Example](#)
- [TACACS+ Accounting Example](#)
- [TACACS+ Server Group Example](#)
- [AAA Server Group Selection Based on DNIS Example](#)
- [TACACS+ Daemon Configuration Example](#)

TACACS+ Authentication Examples

The following example shows how to configure TACACS+ as the security protocol for PPP authentication:

```
aaa new-model
```



```
aaa authentication ppp test group tacacs+ local
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
 ppp authentication chap pap test
```

The lines in the preceding sample configuration are defined as follows:

- The **aaa new-model** command enables the AAA security services.
- The **aaa authentication** command defines a method list, “test,” to be used on serial interfaces running PPP. The keyword **group tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.
- The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 10.1.2.3. The **tacacs-server key** command defines the shared encryption key to be “goaway.”
- The **interface** command selects the line, and the **ppp authentication** command applies the test method list to this line.

The following example shows how to configure TACACS+ as the security protocol for PPP authentication, but instead of the “test” method list, the “default” method list is used.

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
 ppp authentication chap default
```

The lines in the preceding sample configuration are defined as follows:

- The **aaa new-model** command enables the AAA security services.
- The **aaa authentication** command defines a method list, “default,” to be used on serial interfaces running PPP. The keyword **default** means that PPP authentication is applied by default to all interfaces. The **if-needed** keyword means that if the user has already authenticated by going through the ASCII login procedure, then PPP authentication is not necessary and can be skipped. If authentication is needed, the keyword **group tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.
- The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 10.1.2.3. The **tacacs-server key** command defines the shared encryption key to be “goaway.”
- The **interface** command selects the line, and the **ppp authentication** command applies the default method list to this line.

The following example shows how to create the same authentication algorithm for PAP, but it calls the method list “MIS-access” instead of “default”:

```
aaa new-model
aaa authentication pap MIS-access if-needed group tacacs+ local
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
 ppp authentication pap MIS-access
```

The lines in the preceding sample configuration are defined as follows:

- The **aaa new-model** command enables the AAA security services.

- The **aaa authentication** command defines a method list, “MIS-access,” to be used on serial interfaces running PPP. The method list, “MIS-access,” means that PPP authentication is applied to all interfaces. The **if-needed** keyword means that if the user has already authenticated by going through the ASCII login procedure, then PPP authentication is not necessary and can be skipped. If authentication is needed, the keyword **group tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.
- The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 10.1.2.3. The **tacacs-server key** command defines the shared encryption key to be “goaway.”
- The **interface** command selects the line, and the **ppp authentication** command applies the default method list to this line.

The following example shows the configuration for a TACACS+ daemon with an IP address of 10.2.3.4 and an encryption key of “apple”:

```
aaa new-model
aaa authentication login default group tacacs+ local
tacacs-server host 10.2.3.4
tacacs-server key apple
```

The lines in the preceding sample configuration are defined as follows:

- The **aaa new-model** command enables the AAA security services.
- The **aaa authentication** command defines the default method list. Incoming ASCII logins on all interfaces (by default) will use TACACS+ for authentication. If no TACACS+ server responds, then the network access server will use the information contained in the local username database for authentication.
- The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 10.2.3.4. The **tacacs-server key** command defines the shared encryption key to be “apple.”

TACACS+ Authorization Example

The following example shows how to configure TACACS+ as the security protocol for PPP authentication using the default method list; it also shows how to configure network authorization via TACACS+:

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
aaa authorization network default group tacacs+
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
  ppp authentication chap default
```

The lines in the preceding sample configuration are defined as follows:

- The **aaa new-model** command enables the AAA security services.
- The **aaa authentication** command defines a method list, “default,” to be used on serial interfaces running PPP. The keyword **default** means that PPP authentication is applied by default to all interfaces. The **if-needed** keyword means that if the user has already authenticated by going through the ASCII login procedure, then PPP authentication is not necessary and can be skipped. If authentication is needed, the keyword **group tacacs+** means that authentication will be done

through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.

- The **aaa authorization** command configures network authorization via TACACS+. Unlike authentication lists, this authorization list always applies to all incoming network connections made to the network access server.
- The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 10.1.2.3. The **tacacs-server key** command defines the shared encryption key to be “goaway.”
- The **interface** command selects the line, and the **ppp authentication** command applies the default method list to this line.

TACACS+ Accounting Example

The following example shows how to configure TACACS+ as the security protocol for PPP authentication using the default method list; it also shows how to configure accounting via TACACS+:

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
aaa accounting network default stop-only group tacacs+
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
  ppp authentication chap default
```

The lines in the preceding sample configuration are defined as follows:

- The **aaa new-model** command enables the AAA security services.
- The **aaa authentication** command defines a method list, “default,” to be used on serial interfaces running PPP. The keyword **default** means that PPP authentication is applied by default to all interfaces. The **if-needed** keyword means that if the user has already authenticated by going through the ASCII login procedure, then PPP authentication is not necessary and can be skipped. If authentication is needed, the keyword **group tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.
- The **aaa accounting** command configures network accounting via TACACS+. In this example, accounting records describing the session that just terminated will be sent to the TACACS+ daemon whenever a network connection terminates.
- The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 10.1.2.3. The **tacacs-server key** command defines the shared encryption key to be “goaway.”
- The **interface** command selects the line, and the **ppp authentication** command applies the default method list to this line.

TACACS+ Server Group Example

The following example shows how to create a server group with three different TACACS+ servers members:

```
aaa group server tacacs tacgroup1
  server 172.16.1.1
  server 172.16.1.21
```

```
server 172.16.1.31
```

AAA Server Group Selection Based on DNIS Example

The following example shows how to select TACACS+ server groups based on DNIS to provide specific AAA services:

```
! This command enables AAA.
aaa new-model
!
! The following set of commands configures the TACACS+ servers that will be associated
! with one of the defined server groups.
tacacs-server host 172.16.0.1
tacacs-server host 172.17.0.1
tacacs-server host 172.18.0.1
tacacs-server host 172.19.0.1
tacacs-server host 172.20.0.1
tacacs-server key abcdefg

! The following commands define the sg1 TACACS+ server group and associate servers
! with it.
aaa group server tacacs sg1
    server 172.16.0.1
    server 172.17.0.1
! The following commands define the sg2 TACACS+ server group and associate a server
! with it.
aaa group server tacacs sg2
    server 172.18.0.1
! The following commands define the sg3 TACACS+ server group and associate a server
! with it.
aaa group server tacacs sg3
    server 172.19.0.1
! The following commands define the default-group TACACS+ server group and associate
! a server with it.
aaa group server tacacs default-group
    server 172.20.0.1
!
! The next set of commands configures default-group tacacs server group parameters.
aaa authentication ppp default group default-group
aaa accounting network default start-stop group default-group
!
! The next set of commands enables DNIS mapping and maps DNIS numbers to the defined
! RADIUS server groups. In this configuration, all PPP connection requests using DNIS
! 7777 are sent to the sg1 server group. The accounting records for these connections
! (specifically, start-stop records) are handled by the sg2 server group. Calls with a
! DNIS of 8888 use server group sg3 for authentication and server group default-group
! for accounting. Calls with a DNIS of 9999 use server group default-group for
! authentication and server group sg3 for accounting records (stop records only). All
! other calls with DNIS other than the ones defined use the server group default-group
! for both authentication and stop-start accounting records.
aaa dnis map enable
aaa dnis map 7777 authentication ppp group sg1
aaa dnis map 7777 accounting network start-stop group sg2
aaa dnis map 8888 authentication ppp group sg3
aaa dnis map 9999 accounting network stop-only group sg3
```

TACACS+ Daemon Configuration Example

The following example shows a sample configuration of the TACACS+ daemon. The precise syntax used by your TACACS+ daemon may be different from what is included in this example.

```
user = mci_customer1 {  
  chap = cleartext "some chap password"  
  service = ppp protocol = ip {  
    inacl#1="permit ip any any precedence immediate"  
    inacl#2="deny igrp 0.0.1.2 255.255.0.0 any"  
  }  
}
```

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



REVIEW DRAFT - CISCO CONFIDENTIAL

Per VRF for TACACS+ Servers

First Published: March 1, 2004

Last Updated: September 30, 2008

The Per VRF for TACACS+ Servers feature allows per virtual route forwarding (per VRF) to be configured for authentication, authorization, and accounting (AAA) on TACACS+ servers.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Per VRF for TACACS+ Servers”](#) section on page 8.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Per VRF for TACACS+ Servers, page 2](#)
- [Restrictions for Per VRF for TACACS+ Servers, page 2](#)
- [Information About Per VRF for TACACS+ Servers, page 2](#)
- [How to Configure Per VRF for TACACS+ Servers, page 2](#)
- [Configuration Examples for Per VRF for TACACS+ Servers, page 5](#)
- [Additional References, page 6](#)
- [Command Reference, page 7](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

REVIEW DRAFT – CISCO CONFIDENTIAL

Prerequisites for Per VRF for TACACS+ Servers

- TACACS+ server access is required.
- Experience configuring TACACS+, AAA and per VRF AAA, and group servers is necessary.

Restrictions for Per VRF for TACACS+ Servers

- The VRF instance must be specified before per VRF for a TACACS+ server is configured.

Information About Per VRF for TACACS+ Servers

To configure the Per VRF for TACACS+ Servers feature, the following concept should be understood:

- [Per VRF for TACACS+ Servers Overview, page 2](#)

Per VRF for TACACS+ Servers Overview

The Per VRF for TACACS+ Servers feature allows per VRF AAA to be configured on TACACS+ servers. Prior to Cisco IOS Release 12.3(7)T, this functionality was available only on RADIUS servers.

How to Configure Per VRF for TACACS+ Servers

This section contains the following procedures:

- [Configuring Per VRF on a TACACS+ Server, page 2](#) (required)
- [Verifying Per VRF for TACACS+ Servers, page 4](#) (optional)

Configuring Per VRF on a TACACS+ Server

The initial steps in this procedure are used to configure AAA and a server group, create a VRF routing table, and configure an interface. Steps 10 through 13 are used to configure the per VRF on a TACACS+ server feature:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf *vrf-name***
4. **rd *route-distinguisher***
5. **exit**
6. **interface *interface-name***
7. **ip vrf forwarding *vrf-name***

REVIEW DRAFT – CISCO CONFIDENTIAL

8. **ip address** *ip-address mask* [**secondary**]
9. **exit**
10. **aaa group server tacacs+** *group-name*
11. **server-private** {*ip-address* | *name*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*]
12. **ip vrf forwarding** *vrf-name*
13. **ip tacacs source-interface** *subinterface-name*
14. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip vrf <i>vrf-name</i> Example: Router (config)# ip vrf cisco	Configures a VRF table and enters VRF configuration mode.
Step 4	rd <i>route-distinguisher</i> Example: Router (config-vrf)# rd 100:1	Creates routing and forwarding tables for a VRF instance.
Step 5	exit Example: Router (config-vrf)# exit	Exits VRF configuration mode.
Step 6	interface <i>interface-name</i> Example: Router (config)# interface Loopback0	Configures an interface and enters interface configuration mode.
Step 7	ip vrf forwarding <i>vrf-name</i> Example: Router (config-if)# ip vrf forwarding cisco	Configures a VRF for the interface.
Step 8	ip address <i>ip-address mask</i> [secondary] Example: Router (config-if)# ip address 10.0.0.2 255.0.0.0	Sets a primary or secondary IP address for an interface.

REVIEW DRAFT—CISCO CONFIDENTIAL

	Command or Action	Purpose
Step 9	exit Example: Router (config-if)# exit	Exits interface configuration mode.
Step 10	aaa group server tacacs+ group-name Example: Router (config)# aaa group server tacacs+ tacacs1	Groups different TACACS+ server hosts into distinct lists and distinct methods and enters server-group configuration mode.
Step 11	server-private {ip-address name} [nat] [single-connection] [port port-number] [timeout seconds] [key [0 7] string] Example: Router (config-sg-tacacs+)# server-private 10.1.1.1 port 19 key cisco	Configures the IP address of the private TACACS+ server for the group server.
Step 12	ip vrf forwarding vrf-name Example: Router (config-sg-tacacs+)# ip vrf forwarding cisco	Configures the VRF reference of a AAA TACACS+ server group.
Step 13	ip tacacs source-interface subinterface-name Example: Router (config-sg-tacacs+)# ip tacacs source-interface Loopback0	Uses the IP address of a specified interface for all outgoing TACACS+ packets.
Step 14	exit Example: Router (config-sg-tacacs)# exit	Exits server-group configuration mode.

Verifying Per VRF for TACACS+ Servers

To verify the per VRF TACACS+ configuration, perform the following steps:

**Note**

The **debug** commands may be used in any order.

SUMMARY STEPS

1. **enable**
2. **debug tacacs authentication**
3. **debug tacacs authorization**
4. **debug tacacs accounting**
5. **debug tacacs packets**

REVIEW DRAFT – CISCO CONFIDENTIAL**DETAILED STEPS**

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	debug tacacs authentication Example: Router# debug tacacs authentication	Displays information about AAA/TACACS+ authentication.
Step 3	debug tacacs authorization Example: Router# debug tacacs authorization	Displays information about AAA/TACACS+ authorization.
Step 4	debug tacacs accounting Example: Router# debug tacacs accounting	Displays information about accountable events as they occur.
Step 5	debug tacacs packets Example: Router# debug tacacs packets	Displays information about TACACS+ packets.

Configuration Examples for Per VRF for TACACS+ Servers

This section includes the following configuration example:

- [Configuring Per VRF for TACACS+ Servers: Example, page 5](#)

Configuring Per VRF for TACACS+ Servers: Example

The following output example shows that the group server **tacacs1** is configured for per VRF AAA services:

```

aaa group server tacacs+ tacacs1
  server-private 10.1.1.1 port 19 key cisco
  ip vrf forwarding cisco
  ip tacacs source-interface Loopback0

ip vrf cisco
rd 100:1

interface Loopback0
ip address 10.0.0.2 255.0.0.0
ip vrf forwarding cisco

```

REVIEW DRAFT – CISCO CONFIDENTIAL

Additional References

The following sections provide references related to Per VRF for TACACS+ Servers.

Related Documents

Related Topic	Document Title
Configuring TACACS+	“ Configuring TACACS+ ” chapter of the “Security Server Protocols” section of the <i>Cisco IOS Security Configuration Guide</i>
Per VRF AAA	Per VRF AAA
Cisco IOS commands	Cisco Master Commands list, Release 12.4T
Security commands	Cisco IOS Security Command Reference , Release 12.4T

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

REVIEW DRAFT – CISCO CONFIDENTIAL

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html.

- **ip tacacs source-interface**
- **ip vrf forwarding (server-group)**
- **server-private (TACACS+)**

REVIEW DRAFT – CISCO CONFIDENTIAL

Feature Information for Per VRF for TACACS+ Servers

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Per VRF for TACACS+ Servers

Feature Name	Releases	Feature Information
Per VRF for TACACS+ Servers	12.3(7)T 12.3(11)T 12.2(33)SXI	The Per VRF for TACACS+ Servers feature allows per virtual route forwarding (per VRF) to be configured for authentication, authorization, and accounting (AAA) on TACACS+ servers. This feature was introduced in Cisco IOS Release 12.3(7)T. This feature was integrated into Cisco IOS Release 12.2(33)SRA1. This feature was integrated into Cisco IOS Release 12.2(33)SXI.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2004–2008 Cisco Systems, Inc. All rights reserved.



Configuring Kerberos

Feature History

Release	Modification
Cisco IOS	For information about feature support in Cisco IOS software, use Cisco Feature Navigator.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

This chapter describes the Kerberos security system. For a complete description of the Kerberos commands used in this chapter, refer to the “Kerberos Commands” chapter in the *Cisco IOS Security Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature, or refer to the software release notes for a specific release. For more information, see the section “Identifying Supported Platforms” in the chapter “Using Cisco IOS Software.”

In This Chapter

This chapter includes the following topics and tasks:

- [About Kerberos](#)
- [Kerberos Client Support Operation](#)
- [Kerberos Configuration Task List](#)
- [Kerberos Configuration Examples](#)

About Kerberos

Kerberos is a secret-key network authentication protocol, developed at the Massachusetts Institute of Technology (MIT), that uses the Data Encryption Standard (DES) cryptographic algorithm for encryption and authentication. Kerberos was designed to authenticate requests for network resources.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Kerberos, like other secret-key systems, is based on the concept of a trusted third party that performs secure verification of users and services. In the Kerberos protocol, this trusted third party is called the key distribution center (KDC).

The primary use of Kerberos is to verify that users and the network services they use are really who and what they claim to be. To accomplish this, a trusted Kerberos server issues tickets to users. These tickets, which have a limited lifespan, are stored in a user's credential cache and can be used in place of the standard username-and-password authentication mechanism.

The Kerberos credential scheme embodies a concept called "single logon." This process requires authenticating a user once, and then allows secure authentication (without encrypting another password) wherever that user's credential is accepted.

Starting with Cisco IOS Release 11.2, Cisco IOS software includes Kerberos 5 support, which allows organizations already deploying Kerberos 5 to use the same Kerberos authentication database on their routers that they are already using on their other network hosts (such as UNIX servers and PCs).

The following network services are supported by the Kerberos authentication capabilities in Cisco IOS software:

- Telnet
- rlogin
- rsh
- rcp


Note

Cisco Systems' implementation of Kerberos client support is based on code developed by CyberSafe, which was derived from the MIT code. As a result, the Cisco Kerberos implementation has successfully undergone full compatibility testing with the CyberSafe Challenger commercial Kerberos server and MIT's server code, which is freely distributed.

[Table 20](#) lists common Kerberos-related terms and their definitions.

Table 20 ***Kerberos Terminology***

Term	Definition
authentication	A process by which a user or service identifies itself to another service. For example, a client can authenticate to a router or a router can authenticate to another router.
authorization	A means by which the router determines what privileges you have in a network or on the router and what actions you can perform.
credential	A general term that refers to authentication tickets, such as ticket granting tickets (TGTs) and service credentials. Kerberos credentials verify the identity of a user or service. If a network service decides to trust the Kerberos server that issued a ticket, it can be used in place of retyping in a username and password. Credentials have a default lifespan of eight hours.

Table 20 **Kerberos Terminology (continued)**

Term	Definition
instance	An authorization level label for Kerberos principals. Most Kerberos principals are of the form user@REALM (for example, smith@EXAMPLE.COM). A Kerberos principal with a Kerberos instance has the form user/instance@REALM (for example, smith/admin@EXAMPLE.COM). The Kerberos instance can be used to specify the authorization level for the user if authentication is successful. It is up to the server of each network service to implement and enforce the authorization mappings of Kerberos instances. Note that the Kerberos realm name must be in uppercase characters.
Kerberized	Applications and services that have been modified to support the Kerberos credential infrastructure.
Kerberos realm	A domain consisting of users, hosts, and network services that are registered to a Kerberos server. The Kerberos server is trusted to verify the identity of a user or network service to another user or network service. Kerberos realms must always be in uppercase characters.
Kerberos server	A daemon running on a network host. Users and network services register their identity with the Kerberos server. Network services query the Kerberos server to authenticate to other network services.
key distribution center (KDC)	A Kerberos server and database program running on a network host.
principal	Also known as a Kerberos identity, this is who you are or what a service is according to the Kerberos server.
service credential	A credential for a network service. When issued from the KDC, this credential is encrypted with the password shared by the network service and the KDC, and with the user's TGT.
SRVTAB	A password that a network service shares with the KDC. The network service authenticates an encrypted service credential by using the SRVTAB (also known as a KEYTAB) to decrypt it.
ticket granting ticket (TGT)	A credential that the key distribution center (KDC) issues to authenticated users. When users receive a TGT, they can authenticate to network services within the Kerberos realm represented by the KDC.

Kerberos Client Support Operation

This section describes how the Kerberos security system works with a Cisco router functioning as the security server. Although (for convenience or technical reasons) you can customize Kerberos in a number of ways, remote users attempting to access network services must pass through three layers of security before they can access network services.

This section includes the following sections:

- [Authenticating to the Boundary Router](#)
- [Obtaining a TGT from a KDC](#)
- [Authenticating to Network Services](#)

Authenticating to the Boundary Router

This section describes the first layer of security that remote users must pass through when they attempt to access a network. The first step in the Kerberos authentication process is for users to authenticate themselves to the boundary router. The following process describes how users authenticate to a boundary router:

1. The remote user opens a PPP connection to the corporate site router.
2. The router prompts the user for a username and password.
3. The router requests a TGT from the KDC for this particular user.
4. The KDC sends an encrypted TGT to the router that includes (among other things) the user's identity.
5. The router attempts to decrypt the TGT using the password the user entered. If the decryption is successful, the remote user is authenticated to the router.

A remote user who successfully initiates a PPP session and authenticates to the boundary router is inside the firewall but still must authenticate to the KDC directly before being allowed to access network services. This is because the TGT issued by the KDC is stored on the router and is not useful for additional authentication unless the user physically logs on to the router.

Obtaining a TGT from a KDC

This section describes how remote users who are authenticated to the boundary router authenticate themselves to a KDC.

When a remote user authenticates to a boundary router, that user technically becomes part of the network; that is, the network is extended to include the remote user and the user's machine or network. To gain access to network services, however, the remote user must obtain a TGT from the KDC. The following process describes how remote users authenticate to the KDC:

1. The remote user, at a workstation on a remote site, launches the KINIT program (part of the client software provided with the Kerberos protocol).
2. The KINIT program finds the user's identity and requests a TGT from the KDC.
3. The KDC creates a TGT, which contains the identity of the user, the identity of the KDC, and the expiration time of the TGT.
4. Using the user's password as a key, the KDC encrypts the TGT and sends the TGT to the workstation.
5. When the KINIT program receives the encrypted TGT, it prompts the user for a password (this is the password that is defined for the user in the KDC).
6. If the KINIT program can decrypt the TGT with the password the user enters, the user is authenticated to the KDC, and the KINIT program stores the TGT in the user's credential cache.

At this point, the user has a TGT and can communicate securely with the KDC. In turn, the TGT allows the user to authenticate to other network services.

Authenticating to Network Services

The following process describes how a remote user with a TGT authenticates to network services within a given Kerberos realm. Assume the user is on a remote workstation (Host A) and wants to log in to Host B.

1. The user on Host A initiates a Kerberized application (such as Telnet) to Host B.
2. The Kerberized application builds a service credential request and sends it to the KDC. The service credential request includes (among other things) the user's identity and the identity of the desired network service. The TGT is used to encrypt the service credential request.
3. The KDC tries to decrypt the service credential request with the TGT it issued to the user on Host A. If the KDC can decrypt the packet, it is assured that the authenticated user on Host A sent the request.
4. The KDC notes the network service identity in the service credential request.
5. The KDC builds a service credential for the appropriate network service on Host B on behalf of the user on Host A. The service credential contains the client's identity and the desired network service's identity.
6. The KDC then encrypts the service credential twice. It first encrypts the credential with the SRVTAB that it shares with the network service identified in the credential. It then encrypts the resulting packet with the TGT of the user (who, in this case, is on Host A).
7. The KDC sends the twice-encrypted credential to Host A.
8. Host A attempts to decrypt the service credential with the user's TGT. If Host A can decrypt the service credential, it is assured the credential came from the real KDC.
9. Host A sends the service credential to the desired network service. Note that the credential is still encrypted with the SRVTAB shared by the KDC and the network service.
10. The network service attempts to decrypt the service credential using its SRVTAB.
11. If the network service can decrypt the credential, it is assured the credential was in fact issued from the KDC. Note that the network service trusts anything it can decrypt from the KDC, even if it receives it indirectly from a user. This is because the user first authenticated with the KDC.

At this point, the user is authenticated to the network service on Host B. This process is repeated each time a user wants to access a network service in the Kerberos realm.

Kerberos Configuration Task List

For hosts and the KDC in your Kerberos realm to communicate and mutually authenticate, you must identify them to each other. To do this, you add entries for the hosts to the Kerberos database on the KDC and add SRVTAB files generated by the KDC to all hosts in the Kerberos realm. You also make entries for users in the KDC database.

This section describes how to set up a Kerberos-authenticated server-client system and contains the following topics:

- [Configuring the KDC Using Kerberos Commands](#)
- [Configuring the Router to Use the Kerberos Protocol](#)

This section assumes that you have installed the Kerberos administrative programs on a UNIX host, known as the KDC, initialized the database, and selected a Kerberos realm name and password. For instructions about completing these tasks, refer to documentation that came with your Kerberos software.

**Note**

Write down the host name or IP address of the KDC, the port number you want the KDC to monitor for queries, and the name of the Kerberos realm it will serve. You need this information to configure the router.

Configuring the KDC Using Kerberos Commands

After you set up a host to function as the KDC in your Kerberos realm, you must make entries to the KDC database for all principals in the realm. Principals can be network services on Cisco routers and hosts or they can be users.

To use Kerberos commands to add services to the KDC database (and to modify existing database information), complete the tasks in the following sections:

- [Adding Users to the KDC Database](#)
- [Creating SRVTABs on the KDC](#)
- [Extracting SRVTABs](#)

**Note**

All Kerberos command examples are based on Kerberos 5 Beta 5 of the original MIT implementation. Later versions use a slightly different interface.

Adding Users to the KDC Database

To add users to the KDC and create privileged instances of those users, use the **su** command to become root on the host running the KDC and use the `kdb5_edit` program to use the following commands in privileged EXEC mode:

	Command	Purpose
Step 1	Router# ank <i>username@REALM</i>	Use the ank (add new key) command to add a user to the KDC. This command prompts for a password, which the user must enter to authenticate to the router.
Step 2	Router# ank <i>username/instance@REALM</i>	Use the ank command to add a privileged instance of a user.

For example, to add user *loki* of Kerberos realm CISCO.COM, enter the following Kerberos command:

```
ank loki@CISCO.COM
```

**Note**

The Kerberos realm name must be in uppercase characters.

You might want to create privileged instances to allow network administrators to connect to the router at the enable level, for example, so that they need not enter a clear text password (and compromise security) to enter enable mode.

To add an instance of *loki* with additional privileges (in this case, *enable*, although it could be anything) enter the following Kerberos command:

```
ank loki/enable@CISCO.COM
```

In each of these examples, you are prompted to enter a password, which you must give to user *loki* to use at login.

The “[Enabling Kerberos Instance Mapping](#)” section describes how to map Kerberos instances to various Cisco IOS privilege levels.

Creating SRVTABs on the KDC

All routers that you want to authenticate to use the Kerberos protocol must have an SRVTAB. This section and the “[Extracting SRVTABs](#)” section describe how to create and extract SRVTABs for a router called *router1*. The section “[Copying SRVTAB Files](#)” describes how to copy SRVTAB files to the router.

To make SRVTAB entries on the KDC, use the following command in privileged EXEC mode:

Command	Purpose
Router# ark SERVICE/HOSTNAME@REALM	Use the ark (add random key) command to add a network service supported by a host or router to the KDC.

For example, to add a Kerberized authentication service for a Cisco router called *router1* to the Kerberos realm CISCO.COM, enter the following Kerberos command:

```
ark host/router1.cisco.com@CISCO.COM
```

Make entries for all network services on all Kerberized hosts that use this KDC for authentication.

Extracting SRVTABs

SRVTABs contain (among other things) the passwords or randomly generated keys for the service principals you entered into the KDC database. Service principal keys must be shared with the host running that service. To do this, you must save the SRVTAB entries to a file, then copy the file to the router and all hosts in the Kerberos realm. Saving SRVTAB entries to a file is called *extracting* SRVTABs. To extract SRVTABs, use the following command in privileged EXEC mode:

Command	Purpose
Router# xst router-name host	Use the kdb5_edit command xst to write an SRVTAB entry to a file.

For example, to write the host/router1.cisco.com@CISCO.COM SRVTAB to a file, enter the following Kerberos command:

```
xst router1.cisco.com@CISCO.COM host
```

Use the **quit** command to exit the kdb5_edit program.

Configuring the Router to Use the Kerberos Protocol

To configure a Cisco router to function as a network security server and authenticate users using the Kerberos protocol, complete the tasks in the following sections:

- [Defining a Kerberos Realm](#)
- [Copying SRVTAB Files](#)
- [Specifying Kerberos Authentication](#)
- [Enabling Credentials Forwarding](#)
- [Opening a Telnet Session to the Router](#)
- [Establishing an Encrypted Kerberized Telnet Session](#)
- [Enabling Mandatory Kerberos Authentication](#)
- [Enabling Kerberos Instance Mapping](#)
- [Monitoring and Maintaining Kerberos](#)

Defining a Kerberos Realm

For a router to authenticate a user defined in the Kerberos database, it must know the host name or IP address of the host running the KDC, the name of the Kerberos realm and, optionally, be able to map the host name or Domain Name System (DNS) domain to the Kerberos realm.

To configure the router to authenticate to a specified KDC in a specified Kerberos realm, use the following commands in global configuration mode. Note that DNS domain names must begin with a leading dot (.):

	Command	Purpose
Step 1	Router(config)# kerberos local-realm <i>kerberos-realm</i>	Defines the default realm for the router.
Step 2	Router(config)# kerberos server <i>kerberos-realm</i> { <i>hostname</i> <i>ip-address</i> } [<i>port-number</i>]	Specifies to the router which KDC to use in a given Kerberos realm and, optionally, the port number that the KDC is monitoring. (The default is 88.)
Step 3	Router(config)# kerberos realm { <i>dns-domain</i> <i>host</i> } <i>kerberos-realm</i>	(Optional) Maps a host name or DNS domain to a Kerberos realm.



Note

Because the machine running the KDC and all Kerberized hosts must interact within a 5-minute window or authentication fails, all Kerberized machines, and especially the KDC, should be running the Network Time Protocol (NTP).

The **kerberos local-realm**, **kerberos realm**, and **kerberos server** commands are equivalent to the UNIX *krb.conf* file. [Table 21](#) identifies mappings from the Cisco IOS configuration commands to a Kerberos 5 configuration file (*krb5.conf*).

Table 21 **Kerberos 5 Configuration File and Commands**

krb5.conf File	Cisco IOS Configuration Command
[libdefaults] default_realm = DOMAIN.COM	(in configuration mode) kerberos local-realm DOMAIN.COM
[domain_realm] .domain.com = DOMAIN.COM domain.com = DOMAIN.COM	(in configuration mode) kerberos realm.domain.com DOMAIN.COM kerberos realm domain.com DOMAIN.COM
[realms] kdc = DOMAIN.PIL.COM:750 admin_server = DOMAIN.PIL.COM default_domain = DOMAIN.COM	(in configuration mode) kerberos server DOMAIN.COM 172.65.44.2 (172.65.44.2 is the example IP address for DOMAIN.PIL.COM)

For an example of defining a Kerberos realm, see the section “[Defining a Kerberos Realm](#)” later in this chapter.

Copying SRVTAB Files

To make it possible for remote users to authenticate to the router using Kerberos credentials, the router must share a secret key with the KDC. To do this, you must give the router a copy of the SRVTAB you extracted on the KDC.

The most secure method to copy SRVTAB files to the hosts in your Kerberos realm is to copy them onto physical media and go to each host in turn and manually copy the files onto the system. To copy SRVTAB files to the router, which does not have a physical media drive, you must transfer them via the network using TFTP.

To remotely copy SRVTAB files to the router from the KDC, use the following command in global configuration mode:

Command	Purpose
Router(config)# kerberos srvtab remote {hostname ip-address} {filename}	Retrieves an SRVTAB file from the KDC.

When you copy the SRVTAB file from the router to the KDC, the **kerberos srvtab remote** command parses the information in this file and stores it in the router’s running configuration in the **kerberos srvtab entry** format. To ensure that the SRVTAB is available (does not need to be acquired from the KDC) when you reboot the router, use the **write memory** configuration command to write your running configuration (which contains the parsed SRVTAB file) to NVRAM.

For an example of copying SRVTAB files, see the section “[SRVTAB File Copying Example](#)” later in this chapter.

Specifying Kerberos Authentication

You have now configured Kerberos on your router. This makes it possible for the router to authenticate using Kerberos. The next step is to tell it to do so. Because Kerberos authentication is facilitated through AAA, you need to enter the **aaa authentication** command, specifying Kerberos as the authentication method. For more information, refer to the chapter “Configuring Authentication”.

Enabling Credentials Forwarding

With Kerberos configured thus far, a user authenticated to a Kerberized router has a TGT and can use it to authenticate to a host on the network. However, if the user tries to list credentials after authenticating to a host, the output will show no Kerberos credentials present.

You can optionally configure the router to forward users' TGTs with them as they authenticate from the router to Kerberized remote hosts on the network when using Kerberized Telnet, rcp, rsh, and rlogin (with the appropriate flags).

To force all clients to forward users' credentials as they connect to other hosts in the Kerberos realm, use the following command in global configuration mode:

Command	Purpose
Router(config)# kerberos credentials forward	Forces all clients to forward user credentials upon successful Kerberos authentication.

With credentials forwarding enabled, users' TGTs are automatically forwarded to the next host they authenticate to. In this way, users can connect to multiple hosts in the Kerberos realm without running the KINIT program each time to get a new TGT.

Opening a Telnet Session to the Router

To use Kerberos to authenticate users opening a Telnet session to the router from within the network, use the following command in global configuration mode:

Command	Purpose
Router(config)# aaa authentication login {default list-name} krb5_telnet	Sets login authentication to use the Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router.

Although Telnet sessions to the router are authenticated, users must still enter a clear text password if they want to enter enable mode. The **kerberos instance map** command, discussed in a later section, allows them to authenticate to the router at a predefined privilege level.

Establishing an Encrypted Kerberized Telnet Session

Another way for users to open a secure Telnet session is to use Encrypted Kerberized Telnet. With Encrypted Kerberized Telnet, users are authenticated by their Kerberos credentials before a Telnet session is established. The Telnet session is encrypted using 56-bit Data Encryption Standard (DES) encryption with 64-bit Cipher Feedback (CFB). Because data sent or received is encrypted, not clear text, the integrity of the dialed router or access server can be more easily controlled.



Note

This feature is available only if you have the 56-bit encryption image. 56-bit DES encryption is subject to U.S. Government export control regulations.

To establish an encrypted Kerberized Telnet session from a router to a remote host, use either of the following commands in EXEC command mode:

Command	Purpose
Router(config)# connect <i>host</i> [<i>port</i>] / encrypt kerberos	Establishes an encrypted Telnet session.
OR	
Router(config)# telnet <i>host</i> [<i>port</i>] / encrypt kerberos	

When a user opens a Telnet session from a Cisco router to a remote host, the router and remote host negotiate to authenticate the user using Kerberos credentials. If this authentication is successful, the router and remote host then negotiate whether or not to use encryption. If this negotiation is successful, both inbound and outbound traffic is encrypted using 56-bit DES encryption with 64-bit CFB.

When a user dials in from a remote host to a Cisco router configured for Kerberos authentication, the host and router will attempt to negotiate whether or not to use encryption for the Telnet session. If this negotiation is successful, the router will encrypt all outbound data during the Telnet session.

If encryption is not successfully negotiated, the session will be terminated and the user will receive a message stating that the encrypted Telnet session was not successfully established.

For information about enabling bidirectional encryption from a remote host, refer to the documentation specific to the remote host device.

For an example of using encrypted Kerberized Telnet to open a secure Telnet session, see the section “[Encrypted Telnet Session Example](#)” later in this chapter.

Enabling Mandatory Kerberos Authentication

As an added layer of security, you can optionally configure the router so that, after remote users authenticate to it, these users can authenticate to other services on the network only with Kerberized Telnet, rlogin, rsh, and rcp. If you do not make Kerberos authentication mandatory and Kerberos authentication fails, the application attempts to authenticate users using the default method of authentication for that network service; for example, Telnet and rlogin prompt for a password, and rsh attempts to authenticate using the local rhost file.

To make Kerberos authentication mandatory, use the following command in global configuration mode:

Command	Purpose
Router(config)# kerberos clients mandatory	Sets Telnet, rlogin, rsh, and rcp to fail if they cannot negotiate the Kerberos protocol with the remote server.

Enabling Kerberos Instance Mapping

As mentioned in the section “[Creating SRVTABs on the KDC](#),” you can create administrative instances of users in the KDC database. The **kerberos instance map** command allows you to map those instances to Cisco IOS privilege levels so that users can open secure Telnet sessions to the router at a predefined privilege level, obviating the need to enter a clear text password to enter enable mode.

To map a Kerberos instance to a Cisco IOS privilege level, use the following command in global configuration mode:

Command	Purpose
Router(config)# kerberos instance map <i>instance privilege-level</i>	Maps a Kerberos instance to a Cisco IOS privilege level.

If there is a Kerberos instance for user *loki* in the KDC database (for example, *loki/admin*), user *loki* can now open a Telnet session to the router as *loki/admin* and authenticate automatically at privilege level 15, assuming instance “admin” is mapped to privilege level 15. (See the section “[Adding Users to the KDC Database](#)” earlier in this chapter.)

Cisco IOS commands can be set to various privilege levels using the **privilege level** command.

After you map a Kerberos instance to a Cisco IOS privilege level, you must configure the router to check for Kerberos instances each time a user logs in. To run authorization to determine if a user is allowed to run an EXEC shell based on a mapped Kerberos instance, use the **aaa authorization** command with the **krb5-instance** keyword. For more information, refer to the chapter “Configuring Authorization.”

Monitoring and Maintaining Kerberos

To display or remove a current user’s credentials, use the following commands in EXEC mode:

	Command	Purpose
Step 1	Router# show kerberos creds	Lists the credentials in a current user’s credentials cache.
Step 2	Router# clear kerberos creds	Destroys all credentials in a current user’s credentials cache, including those forwarded.

For an example of Kerberos configuration, see the section “[Kerberos Configuration Examples](#)”.

Kerberos Configuration Examples

The following sections provide Kerberos configuration examples:

- [Kerberos Realm Definition Examples](#)
- [SRVTAB File Copying Example](#)
- [Kerberos Configuration Examples](#)
- [Encrypted Telnet Session Example](#)

Kerberos Realm Definition Examples

To define CISCO.COM as the default Kerberos realm, use the following command:

```
kerberos local-realm CISCO.COM
```

To tell the router that the CISCO.COM KDC is running on host 10.2.3.4 at port number 170, use the following Kerberos command:

```
kerberos server CISCO.COM 10.2.3.4 170
```

To map the DNS domain cisco.com to the Kerberos realm CISCO.COM, use the following command:

```
kerberos realm.cisco.com CISCO.COM
```

SRVTAB File Copying Example

To copy over the SRVTAB file on a host named `host123.cisco.com` for a router named `router1.cisco.com`, the command would look like this:

```
kerberos srvtab remote host123.cisco.com router1.cisco.com-new-srvtab
```

Kerberos Configuration Examples

This section provides a typical non-Kerberos router configuration and shows output for this configuration from the **write term** command, then builds on this configuration by adding optional Kerberos functionality. Output for each configuration is presented for comparison against the previous configuration.

This example shows how to use the `kdb5_edit` program to perform the following configuration tasks:

- Adding user `chet` to the Kerberos database
- Adding a privileged Kerberos instance of user `chet` (`chet/admin`) to the Kerberos database
- Adding a restricted instance of `chet` (`chet/restricted`) to the Kerberos database
- Adding workstation `chet-ss20.cisco.com`
- Adding router `chet-2500.cisco.com` to the Kerberos database
- Adding workstation `chet-ss20.cisco.com` to the Kerberos database
- Extracting SRVTABs for the router and workstations
- Listing the contents of the KDC database (with the **ldb** command)

Note that, in this sample configuration, host `chet-ss20` is also the KDC:

```
chet-ss20# sbin/kdb5_edit
kdb5_edit: ank chet
Enter password:
Re-enter password for verification:
kdb5_edit: ank chet/admin
Enter password:
Re-enter password for verification:
kdb5_edit: ank chet/restricted
Enter password:
Re-enter password for verification:
kdb5_edit: ark host/chet-ss20.cisco.com
kdb5_edit: ark host/chet-2500.cisco.com
kdb5_edit: xst chet-ss20.cisco.com host
'host/chet-ss20.cisco.com@CISCO.COM' added to keytab
'WRFILE:chet-ss20.cisco.com-new-srvtab'
kdb5_edit: xst chet-2500.cisco.com host
'host/chet-2500.cisco.com@CISCO.COM' added to keytab
'WRFILE:chet-2500.cisco.com-new-srvtab'
kdb5_edit: ldb
entry: host/chet-2500.cisco.com@CISCO.COM
entry: chet/restricted@CISCO.COM
entry: chet@CISCO.COM
entry: K/M@CISCO.COM
entry: host/chet-ss20.cisco.com@CISCO.COM
entry: krbtgt/CISCO.COM@CISCO.COM
entry: chet/admin@CISCO.COM
```

```
kdb5_edit:  q
chet-ss20#
```

The following example shows output from a **write term** command, which displays the configuration of router chet-2500. This is a typical configuration with no Kerberos authentication.

```
chet-2500# write term
Building configuration...

Current configuration:
!
! Last configuration
change at 14:03:55 PDT Mon May 13 1996
!
version 11.2
service udp-small-servers
service tcp-small-servers
!
hostname chet-2500
!
clock timezone PST -8
clock summer-time PDT recurring
aaa new-model
aaa authentication login console none
aaa authentication ppp local local
enable password sMudgKin
!
username chet-2500 password 7 sMudgkin
username chet-3000 password 7 sMudgkin
username chetin password 7 sMudgkin
!
interface Ethernet0
 ip address 172.16.0.0 255.255.255.0
!
interface Serial0
 no ip address
 shutdown
 no fair-queue
!
interface Serial1
 no ip address
 shutdown
 no fair-queue
!
interface Async2
 ip unnumbered Ethernet0
 encapsulation ppp
 shutdown
 async dynamic routing
 async mode dedicated
 no cdp enable
 ppp authentication pap local
 no tarp propagate
!
interface Async3
 ip unnumbered Ethernet0
 encapsulation ppp
 shutdown
 async dynamic address
 async dynamic routing
 async mode dedicated
 no cdp enable
 ppp authentication pap local
 no tarp propagate
```

```

!
router eigrp 109
  network 172.17.0.0
  no auto-summary
!
ip default-gateway 172.30.55.64
ip domain-name cisco.com
ip name-server 192.168.0.0
ip classless
!
!

line con 0
  exec-timeout 0 0
  login authentication console
line 1 16
  transport input all
line aux 0
  transport input all
line vty 0 4
  password sMudgKin
!
ntp clock-period 17179703
ntp peer 172.19.10.0
ntp peer 172.19.0.0
end

```

The following example shows how to enable user authentication on the router via the Kerberos database. To enable user authentication via the Kerberos database, you would perform the following tasks:

- Entering configuration mode
- Defining the Kerberos local realm
- Identifying the machine hosting the KDC
- Enabling credentials forwarding
- Specifying Kerberos as the method of authentication for login
- Exiting configuration mode (CTL-Z)
- Writing the new configuration to the terminal

```

chet-2500# configure term
Enter configuration commands, one per line. End with CNTL/Z.
chet-2500(config)# kerberos local-realm CISCO.COM
chet-2500(config)# kerberos server CISCO.COM chet-ss20
Translating "chet-ss20"...domain server (192.168.0.0) [OK]

chet-2500(config)# kerberos credentials forward
chet-2500(config)# aaa authentication login default krb5
chet-2500(config)#
chet-2500#
%SYS-5-CONFIG_I: Configured from console by console
chet-2500# write term

```

Compare the following configuration with the previous one. In particular, look at the lines beginning with the words “aaa,” “username,” and “kerberos” (lines 10 through 20) in this new configuration.

Building configuration...

```

Current configuration:
!
! Last configuration change at 14:05:54 PDT Mon May 13 1996
!

```

```

version 11.2
service udp-small-servers
service tcp-small-servers
!
hostname chet-2500
!
clock timezone PST -8
clock summer-time PDT recurring
aaa new-model
aaa authentication login default krb5
aaa authentication login console none
aaa authentication ppp local local
enable password sMudgKin
!
username chet-2500 password 7 sMudgkin
username chet-3000 password 7 sMudgkin
username chetin password 7 sMudgkin
kerberos local-realm CISCO.COM
kerberos server CISCO.COM 172.71.54.14
kerberos credentials forward
!
interface Ethernet0
 ip address 172.16.0.0 255.255.255.0
!
interface Serial0
 no ip address
 shutdown
 no fair-queue
!
interface Serial1
 no ip address
 shutdown
 no fair-queue
!
interface Async2
 ip unnumbered Ethernet0
 encapsulation ppp
 shutdown
 async dynamic routing
 async mode dedicated
 no cdp enable
 ppp authentication pap local
 no tarp propagate
!
interface Async3
 ip unnumbered Ethernet0
 encapsulation ppp
 shutdown
 async dynamic address
 async dynamic routing
 async mode dedicated
 no cdp enable
 ppp authentication pap local
 no tarp propagate
!
router eigrp 109
 network 172.17.0.0
 no auto-summary
!
ip default-gateway 172.30.55.64
ip domain-name cisco.com
ip name-server 192.168.0.0
ip classless
!

```

```

!
line con 0
  exec-timeout 0 0
  login authentication console
line 1 16
  transport input all
line aux 0
  transport input all
line vty 0 4
  password sMudgKin
!
ntp clock-period 17179703
ntp peer 172.19.10.0
ntp peer 172.19.0.0
end

```

With the router configured thus far, user chet can log in to the router with a username and password and automatically obtain a TGT, as illustrated in the next example. With possession of a credential, user chet successfully authenticates to host chet-ss20 without entering a username/password.

```

chet-ss20% telnet chet-2500
Trying 172.16.0.0 ...
Connected to chet-2500.cisco.com.
Escape character is '^]'.

```

User Access Verification

```

Username: chet
Password:

```

```

chet-2500> show kerberos creds
Default Principal: chet@CISCO.COM
Valid Starting      Expires      Service Principal
13-May-1996 14:05:39  13-May-1996 22:06:40  krbtgt/CISCO.COM@CISCO.COM

```

```

chet-2500> telnet chet-ss20
Trying chet-ss20.cisco.com (172.71.54.14)... Open
Kerberos:      Successfully forwarded credentials

```

```

SunOS UNIX (chet-ss20) (pts/7)

```

```

Last login: Mon May 13 13:47:35 from chet-ss20.cisco.c
Sun Microsystems Inc.  SunOS 5.4      Generic July 1994
unknown mode: new
chet-ss20%

```

The following example shows how to authenticate to the router using Kerberos credentials. To authenticate using Kerberos credentials, you would perform the following tasks:

- Entering configuration mode
- Remotely copying over the SRVTAB file from the KDC
- Setting authentication at login to use the Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router
- Writing the configuration to the terminal

Note that the new configuration contains a **kerberos srvtab entry** line. This line is created by the **kerberos srvtab remote** command.

```

chet-2500# configure term
Enter configuration commands, one per line.  End with CNTL/Z.

```

```

chet-2500(config)# kerberos srvtab remote earth chet/chet-2500.cisco.com-new-srvtab
Translating "earth"...domain server (192.168.0.0) [OK]

Loading chet/chet-2500.cisco.com-new-srvtab from 172.68.1.123 (via Ethernet0): !
[OK - 66/1000 bytes]

chet-2500(config)# aaa authentication login default krb5-telnet krb5
chet-2500(config)#
chet-2500#
%SYS-5-CONFIG_I: Configured from console by console
chet-2500# write term
Building configuration...

Current configuration:
!
! Last configuration change at 14:08:32 PDT Mon May 13 1996
!
version 11.2
service udp-small-servers
service tcp-small-servers
!
hostname chet-2500
!
clock timezone PST -8
clock summer-time PDT recurring
aaa new-model
aaa authentication login default krb5-telnet krb5
aaa authentication login console none
aaa authentication ppp local local
enable password sMudgKin
!
username chet-2500 password 7 sMudgkin
username chet-3000 password 7 sMudgkin
username chetin password 7 sMudgkin
kerberos local-realm CISCO.COM
kerberos srvtab entry host/chet-2500.cisco.com@CISCO.COM 0 832015393 1 1 8 7 sMudgkin
kerberos server CISCO.COM 172.71.54.14
kerberos credentials forward
!
interface Ethernet0
 ip address 172.16.0.0 255.255.255.0
!
interface Serial0
 no ip address
 shutdown
 no fair-queue
!

interface Serial1
 no ip address
 shutdown
 no fair-queue
!
interface Async2
 ip unnumbered Ethernet0
 encapsulation ppp
 shutdown
 async dynamic routing
 async mode dedicated
 no cdp enable
 ppp authentication pap local
 no tarp propagate
!
interface Async3

```



```

ip unnumbered Ethernet0
encapsulation ppp
shutdown
async dynamic address
async dynamic routing
async mode dedicated
no cdp enable
ppp authentication pap local
no tarp propagate
!
router eigrp 109
 network 172.17.0.0
 no auto-summary
!
ip default-gateway 172.30.55.64
ip domain-name cisco.com
ip name-server 192.168.0.0
ip classless
!
!
line con 0
 exec-timeout 0 0
 login authentication console
line 1 16
 transport input all
line aux 0
 transport input all
line vty 0 4
 password sMudgKin
!
ntp clock-period 17179703
ntp peer 172.19.10.0
ntp peer 172.19.0.0
end

chet-2500#

```

With this configuration, the user can Telnet in to the router using Kerberos credentials, as illustrated in the next example:

```

chet-ss20% bin/telnet -a -F chet-2500
Trying 172.16.0.0...
Connected to chet-2500.cisco.com.
Escape character is '^]'.
[ Kerberos V5 accepts you as "chet@CISCO.COM" ]

```

User Access Verification

```
chet-2500>[ Kerberos V5 accepted forwarded credentials ]
```

```

chet-2500> show kerberos creds
Default Principal:  chet@CISCO.COM
Valid Starting      Expires              Service Principal
13-May-1996 15:06:25  14-May-1996 00:08:29  krbtgt/CISCO.COM@CISCO.COM

chet-2500>q
Connection closed by foreign host.
chet-ss20%

```

The following example shows how to map Kerberos instances to Cisco's privilege levels. To map Kerberos instances to privilege levels, you would perform the following tasks:

- Entering configuration mode

- Mapping the Kerberos instance admin to privilege level 15
- Mapping the Kerberos instance restricted to privilege level 3
- Specifying that the instance defined by the **kerberos instance map** command be used for AAA Authorization
- Writing the configuration to the terminal

```

chet-2500# configure term
Enter configuration commands, one per line.  End with CNTL/Z.
chet-2500(config)# kerberos instance map admin 15
chet-2500(config)# kerberos instance map restricted 3
chet-2500(config)# aaa authorization exec default krb5-instance
chet-2500(config)#
chet-2500#
%SYS-5-CONFIG_I: Configured from console by console
chet-2500# write term
Building configuration...

Current configuration:
!
! Last configuration change at 14:59:05 PDT Mon May 13 1996
!
version 11.2
service udp-small-servers
service tcp-small-servers
!
hostname chet-2500
!
aaa new-model
aaa authentication login default krb5-telnet krb5
aaa authentication login console none
aaa authentication ppp default krb5 local
aaa authorization exec default krb5-instance
enable password sMudgKin
!
username chet-2500 password 7 sMudgkin
username chet-3000 password 7 sMudgkin
username chetin password 7 sMudgkin
ip domain-name cisco.com
ip name-server 192.168.0.0
kerberos local-realm CISCO.COM
kerberos srvtab entry host/chet-2500.cisco.com@CISCO.COM 0 832015393 1 1 8 7 sMudgkin
kerberos server CISCO.COM 172.71.54.14
kerberos instance map admin 15
kerberos instance map restricted 3
kerberos credentials forward
clock timezone PST -8
clock summer-time PDT recurring
!
interface Ethernet0
 ip address 172.16.0.0 255.255.255.0
!
interface Serial0
 no ip address
 shutdown
 no fair-queue
!
interface Serial1
 no ip address
 shutdown
 no fair-queue
!
interface Async2

```

```

ip unnumbered Ethernet0
encapsulation ppp
shutdown
async dynamic routing
async mode dedicated
no cdp enable
ppp authentication pap local
no tarp propagate
!
interface Async3
ip unnumbered Ethernet0
encapsulation ppp
shutdown
async dynamic address
async dynamic routing
async mode dedicated
no cdp enable
ppp authentication pap local
no tarp propagate
!
router eigrp 109
network 172.17.0.0
no auto-summary
!
ip default-gateway 172.30.55.64
ip classless
!
!
line con 0
exec-timeout 0 0
login authentication console
line 1 16
transport input all
line aux 0
transport input all
line vty 0 4
password sMudgKin
!
ntp clock-period 17179703
ntp peer 172.19.10.0
ntp peer 172.19.0.0
end

chet-2500#

```

The following example shows output from the three types of sessions now possible for user chet with Kerberos instances turned on:

```

chet-ss20% telnet chet-2500
Trying 172.16.0.0 ...
Connected to chet-2500.cisco.com.
Escape character is '^]'.

User Access Verification

Username: chet
Password:

chet-2500> show kerberos creds
Default Principal: chet@CISCO.COM
Valid Starting      Expires      Service Principal
13-May-1996 14:58:28 13-May-1996 22:59:29 krbtgt/CISCO.COM@CISCO.COM

chet-2500> show privilege

```

```

Current privilege level is 1
chet-2500> q
Connection closed by foreign host.
chet-ss20% telnet chet-2500
Trying 172.16.0.0 ...
Connected to chet-2500.cisco.com.
Escape character is '^]'.

```

User Access Verification

```

Username: chet/admin
Password:

```

```

chet-2500# show kerberos creds
Default Principal: chet/admin@CISCO.COM
Valid Starting      Expires      Service Principal
13-May-1996 14:59:44 13-May-1996 23:00:45 krbtgt/CISCO.COM@CISCO.COM
chet-2500# show privilege
Current privilege level is 15
chet-2500# q
Connection closed by foreign host.
chet-ss20% telnet chet-2500
Trying 172.16.0.0 ...
Connected to chet-2500.cisco.com.
Escape character is '^]'.

```

User Access Verification

```

Username: chet/restricted
Password:

```

```

chet-2500# show kerberos creds
Default Principal: chet/restricted@CISCO.COM
Valid Starting      Expires      Service Principal
13-May-1996 15:00:32 13-May-1996 23:01:33 krbtgt/CISCO.COM@CISCO.COM
chet-2500# show privilege
Current privilege level is 3
chet-2500# q
Connection closed by foreign host.
chet-ss20%

```

Encrypted Telnet Session Example

The following example shows how to establish an encrypted Telnet session from a router to a remote host named “host1”:

```

Router> telnet host1 /encrypt kerberos

```



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Traffic Filtering, Firewalls, and Virus Detection



Automatic Signature Extraction

First Published: July 19, 2007

The Automatic Signature Extraction (ASE) feature helps shorten the response time for identifying malware by dynamically extracting signatures of unknown viruses and worms traversing the network without the need for human intervention.

Before Cisco IOS Release 12.4(15)T, network protection from malware such as botnets, viruses, and worms was accomplished by deploying solutions that rely on manual signatures to identify the malware. Normally, security professionals require approximately 8 to 12 hours to generate a signature for a new piece of malware. This time interval had been acceptable for thwarting malware, but is no longer acceptable nor scalable due to the exponential increase in malware that is seen on networks.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for](#)” section on page 12.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Contents

- [Prerequisites for, page 2](#)
- [Restrictions for, page 2](#)
- [Information About, page 2](#)
- [How to Configure, page 7](#)
- [Additional References, page 9](#)
- [Command Reference, page 11](#)
- [Feature Information for, page 12](#)
- [Glossary, page 13](#)

Prerequisites for

The following prerequisites apply for the ASE collector.

See the “[Collector Operation](#)” section on [page 4](#) for more information on the ASE collector.

- The ASE collector runs on an x86-based Linux PC and must have IP connectivity to the network and ASE sensors. Threat Information Distribution Protocol (TIDP) is the communication protocol used between the Linux-based ASE collector and Cisco IOS-based ASE sensors.
- It is recommended that the ASE collector software image run on RedHat Enterprise Linux AS Release 3 or a later release.

**Note**

Contact your Cisco representative for more information about installing the ASE collector functionality on your network.

Restrictions for

Contact your Cisco representative for any restrictions concerning the ASE collector or ASE sensor implementation.

Information About

The following sections describe how the ASE feature works and how ASE is implemented on a WAN:

- [Overview, page 3](#)
- [Sensor Operation, page 3](#)
- [Collector Operation, page 4](#)
- [Automatic Signature Extraction Implementation on a Network, page 5](#)

Overview

The Automatic Signature Extraction feature is used to identify and define potential worms and viruses found in network traffic based on the following characteristics:

- Content invariance identifies that all worms have some code that remains unchanged through the infection.
- Content prevalence identifies if packet payloads were observed frequently in the network. Because worms are designed to spread, the unchanged portion of a worm's content appears frequently on a network as it spreads or attempts to spread.
- Address dispersion identifies whether the same payload is sent to and from a large number of source and destination IP address pairs.

**Note**

The ASE feature can detect e-mail viruses but is disabled by default. This feature can be enabled on the ASE collector. Contact your Cisco representative for more information.

When the ASE sensor extracts a malware signature, the ASE sensor sends the signature to the collector using the TIDP Threat Mitigation Service (TMS) to contain and mitigate the malware outbreak among TMS consumers spread across the network. The TMS framework rapidly and efficiently distributes threat information to devices on the network and generates actions to TMS consumers to either drop or redirect the packets containing the malware signature.

**Note**

See the [“Sensor Operation” section on page 3](#) for more information on this feature.

See [TIDP Based Mitigation Services](#) for more information on TMS operation.

Sensor Operation

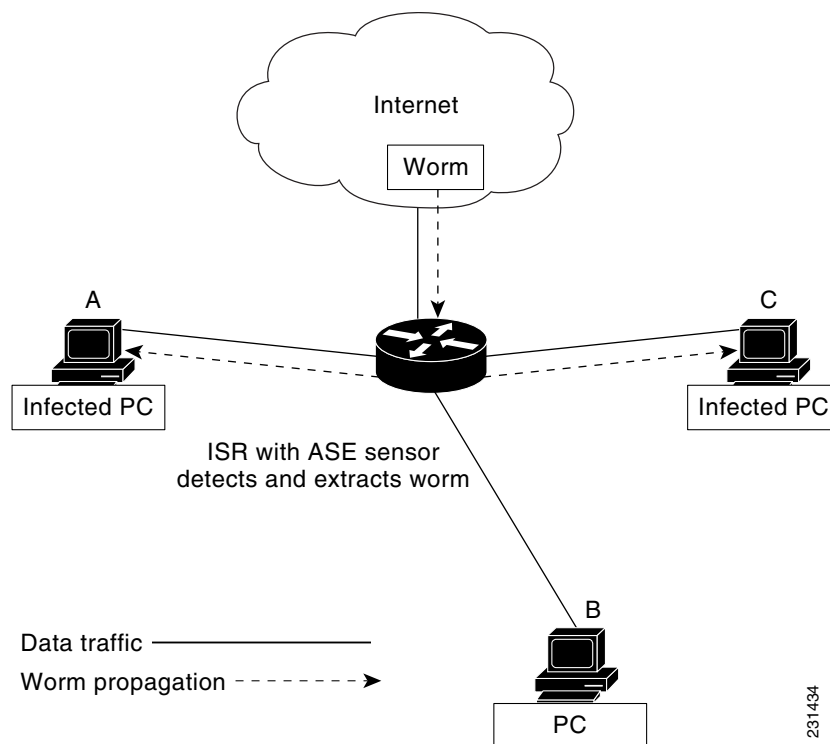
The ASE feature has two main components: a sensor and collector. The ASE sensor sifts through the contents of network traffic to reduce the number of different source and destination addresses seen in packets. To minimize the impact on the device, sensing can be enabled or disabled on a per-interface basis and traffic designated as ASE traffic can be specified. The ASE sensor observes the same traffic as the router can observe after an access list is applied.

**Note**

The sensor is unable to extract signatures from within encrypted traffic passing through a router.

[Figure 1, Cisco IOS Signature Extraction](#), shows that devices A and C are infected with the same worm. As traffic crosses the Cisco IOS router running the ASE sensor, the router extracts the worm's signature based on its address dispersion and content prevalence. Then the router sends this information to the ASE collector for further processing.

Figure 1 Cisco IOS Signature Extraction



Collector Operation

The ASE collector, which runs on a Linux-based PC, performs the following functions:

- Processes signatures it receives from the ASE sensor.
- Initiates the mitigation of signatures.
- Coordinates detection between multiple ASE sensors.
- Manages and distributes entry information and files on the network.
- Collects signatures and packets sent by the sensor.
- Analyzes extracted signatures to determine what the best signature is for a malicious packet to correctly identify a threat.
- Performs post processing of signatures to reduce false alarms.
- Maintains a signature database.
- Reduces false positives in signatures through classification.
- Manages sensor configuration such as thresholds, scanning criteria, and other parameters.
- Generates a report or reports on collected signatures.



Note

Contact your Cisco representative for more information about installing the ASE collector functionality on your network.

Automatic Signature Extraction Implementation on a Network

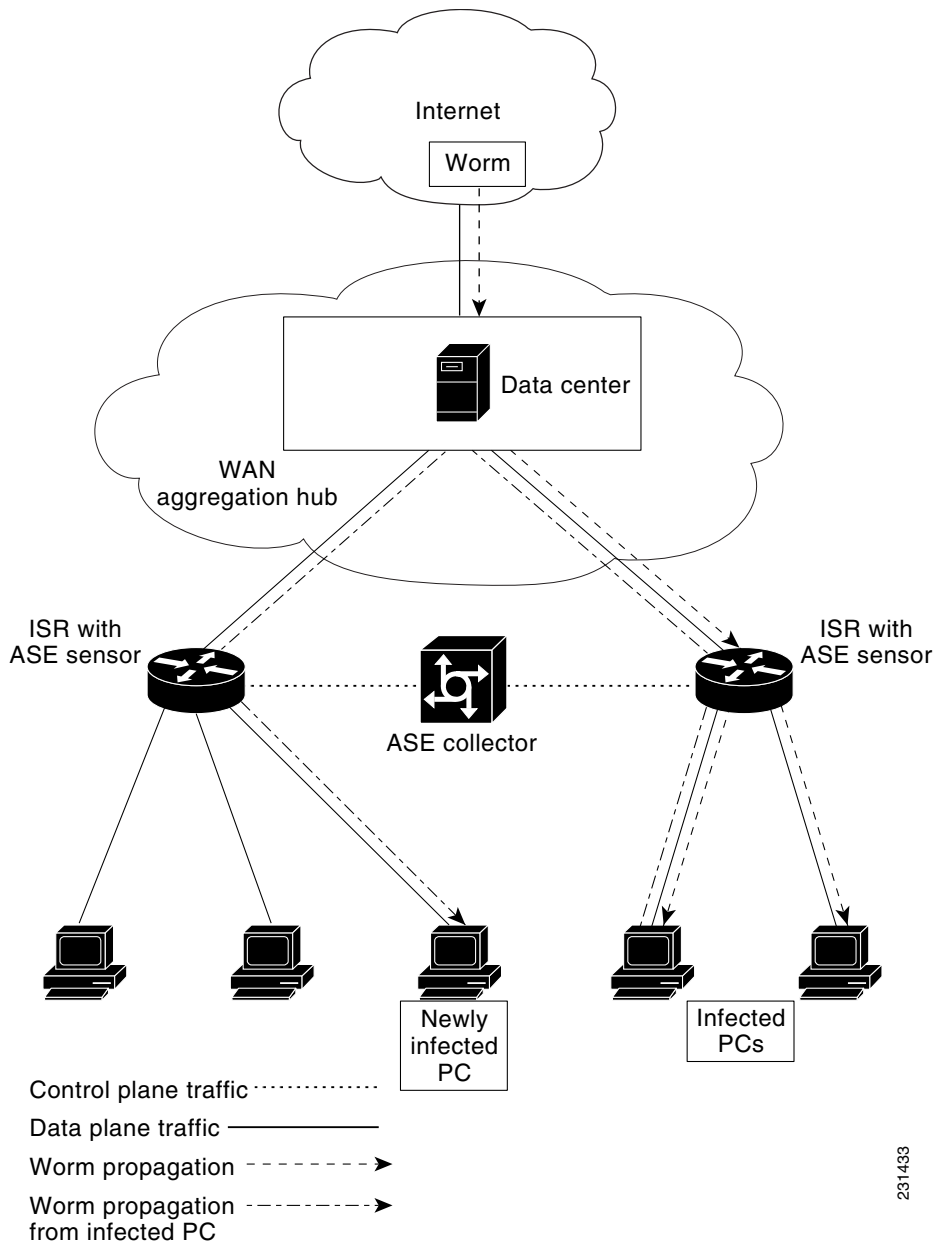
Self-propagating worms continue to grow and affect the security of hosts and networks. These malicious malware attacks often target specific victims or subnets within an enterprise organization. Specifically, a worm can affect and saturate the local network (including all hosts), the branch router, and the local WAN connection or both. The optimal location to detect, contain, and mitigate these worms is on the gateway network connection to prevent the worms from spreading to the entire network, including all connected branches.

Using the WAN Aggregation Model to Contain Malware

The ASE sensor is typically deployed on the Customer Premises Equipment (CPE) WAN so that worms closest to the source can be extracted and prevented from spreading to other areas of the enterprise network.

The WAN aggregation model refers to the traditional deployment scenario in which CPEs are terminated over WAN links to an aggregation HUB. In this model, the CPEs would serve as ASE sensors, and the aggregation HUB would provide ASE Collector functionality. [Figure 2, WAN Aggregation Model](#), shows how worm signatures are extracted at the CPEs and the HUB site with the ASE sensor and shows how the ASE sensor uses this signature information with the ASE collector to contain the outbreak.

Figure 2 WAN Aggregation Model



231433

How to Configure

This section contains the following task:

- [Configuring](#)

Configuring

This section describes how to configure the Automatic Signature Extraction sensor feature on an ISR router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ase group** *TIDP-group-number*
4. **ase collector** *ip-address*
5. **ase signature extraction**
6. **interface** *interface-type number*
7. **ase enable**
8. **end**
9. **show ase**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ase group <i>TIDP-group-number</i> Example: Router(config)# ase group 10	The group number range is between 1 and 65535, which identifies the TIDP group number used for exchange between the ASE sensor and ASE collector. Note See the Threat Information Distribution Protocol feature documentation for more information on TIDP groups.
Step 4	ase collector <i>ip-address</i> Example: Router(config)# ase collector 10.10.10.3	Enters the destination IP address of the ASE collector server so that the ASE sensor has IP connectivity to the ASE collector.
Step 5	ase signature extraction Example: Router(config)# ase signature extraction	Enables the ASE feature globally on the router.
Step 6	interface <i>interface-type number</i> Example: Router(config)# interface GigabitEthernet0/1	Enters the interface for the ASE feature, and enters interface configuration mode.
Step 7	ase enable Example: Router(config-if)# ase enable	Enables the ASE feature on this interface.

	Command or Action	Purpose
Step 8	end Example: Router(config-if)# end	Returns to privileged EXEC mode.
Step 9	show ase Example: Router# show ase	Displays the ASE run-time status. The four states are: <ul style="list-style-type: none">• Not Enabled—(Not displayed) The ASE feature is not enabled in global configuration mode.• Enabled—The ASE feature is enabled in global configuration mode, but the ASE sensor has not connected with the ASE collector.• Connected—The ASE sensor has connected with the ASE collector, but it has not completed initialization.• Online—The ASE is ready for inspecting traffic.

What to Do Next

Start the ASE collector. The ASE collector, which runs on a Linux-based PC, provides the ASE sensor software on the Cisco IOS with entries and analysis on extracted signatures.



Note

Contact your Cisco representative for more information about installing the ASE collector on your network.

After the ASE collector is started, the ASE run-time status information can be displayed by using the **show ase** command, as shown below:



Note

The ASE collector must be started in order for the ASE run-time status information to be displayed.

```
Router# show ase
ASE Information:

Collector IP: 10.10.10.3
TIDP Group   : 10
Status       : Online

Packets inspected: 1105071
Address Dispersion Threshold: 20
Prevalence Threshold: 10
Sampling set to: 1 in 64
Address Dispersion Inactivity Timer: 3600s
Prevalence Table Refresh Time: 60s
```

Additional References

The following sections provide references related to .

Related Documents

Related Topic	Document Title
Threat Information Distribution Protocol (TIDP) Mitigation Service (TMS)	TIDP Based Mitigation Services
	Threat Information Distribution Protocol
Security related information	Cisco IOS Security Configuration Guide, Release 12.4

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this release.	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **ase collector**
- **ase enable**
- **ase group**
- **ase signature extraction**
- **clear ase signatures**
- **debug ase**
- **show ase**

Feature Information for

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for

Feature Name	Releases	Feature Information
	12.4(15)T	<p>The Automatic Signature Extraction feature helps shorten the response time for identifying malware by dynamically extracting signatures for unknown viruses and worms traversing the network without the need for human intervention.</p> <p>This feature was introduced on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.</p>

Glossary

botnet—Slang term for a collection of software robots, or bots, which run autonomously or to a network of compromised “zombie” computers running distributed programs, which are usually referred to as worms, Trojan horses, or backdoors, under a common command and control infrastructure.

CPE—Customer Premises Equipment. Terminating equipment, such as a router installed at a customer site, and connected to a WAN.

ISR—Integrated Services Router. Router that supports integrated or multimedia services, including traffic management mechanisms.

malware—Detrimental software designed to infiltrate or damage a computer system without the owner's informed consent. Examples of malware include viruses, worms, botnets, spam, adware, etc.

signature—The 40 bytes of packet data that can be used to identify a piece of malware.

TIDP—Threat Information Distribution Protocol. Communication protocol used between the Linux-based Automatic Signature Extraction collector and Cisco IOS-based ASE sensors.

TMS—Threat Mitigation Service. TMS is used with the TIDP protocol to contain and mitigate the malware outbreak among TMS consumers on a network.

Virus—Hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting—that is, inserting a copy of itself into and becoming part of—another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

WAN—wide-area network. Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay, SMDS, and X.25 are examples of WANs.

worm—Computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and can consume computer resources destructively.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Access Control Lists (ACLs)



IP Access List Features Roadmap

First Published: August 18, 2006

Last Updated: August 18, 2006

This roadmap lists the access list features documented in the *Cisco IOS Security Configuration Guide* and maps them to the modules in which they appear.

Feature and Release Support

[Table 1](#) lists access list feature support for the Cisco IOS software releases 12.2S, 12.3T, and 12.4T.

Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table. *Not all features may be supported in your Cisco IOS software release*

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 **Supported Access List Features**

Release	Feature Name	Feature Description	Where Documented
Cisco IOS Releases 12.2S, 12.3T, and 12.4T			
12.2(25)S	ACL Support for Filtering IP Options	This feature allows you to filter packets having IP Options, in order to prevent routers from becoming saturated with spurious packets.	Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Supported Access List Features (continued)

12.3(4)T 12.2(25)S	ACL TCP Flags Filtering	This feature provides a flexible mechanism for filtering on TCP flags. Before Cisco IOS Release 12.3(4)T, an incoming packet was matched as long as any TCP flag in the packet matched a flag specified in the access control entry (ACE). This behavior allows for a security loophole, because packets with all flags set could get past the access control list (ACL). The ACL TCP Flags Filtering feature allows you to select any combination of flags on which to filter. The ability to match on a flag set and on a flag not set gives you a greater degree of control for filtering on TCP flags, thus enhancing security.	Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values
12.3(7)T 12.2(25)S	ACL—Named ACL Support for Noncontiguous Ports on an Access Control Entry	This feature allows you to specify noncontiguous ports in a single access control entry, which greatly reduces the number of entries required in an access control list when several entries have the same source address, destination address, and protocol, but differ only in the ports.	Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values
12.4(2)T	ACL Support for Filtering on TTL Value	You may use extended IP access lists (named or numbered) to filter packets based on their time-to-live (TTL) value, from 0 to 255. This filtering enhances your control over which packets reach a router.	Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values
12.4(6)T	ACL Manageability	The ACL Manageability feature enables users to display and clear Access Control Entry (ACE) statistics per interface and per incoming or outgoing traffic direction for access control lists (ACLs).	Displaying and Clearing IP Access List Data Using ACL Manageability http://lbgj/push_targets1/ucdit/cc/td/doc/product/software/ios124/124tcg/sec_c/tsaclsho.htm

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and

© 2007 Cisco Systems, Inc. All rights reserved.





IP Access List Overview

Feature History

Release	Modification
Cisco IOS	For information about feature support in Cisco IOS software, use Cisco Feature Navigator.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

First Published: August 18, 2006

Last Updated: August 18, 2006

Access control lists (ACLs) perform packet filtering to control which packets move through the network and where. Such control provides security by helping to limit network traffic, restrict the access of users and devices to the network, and prevent traffic from leaving a network. IP access lists can reduce the chance of spoofing and denial-of-service attacks and allow dynamic, temporary user access through a firewall.

IP access lists can also be used for purposes other than security, such as bandwidth control, restricting the content of routing updates, redistributing routes, triggering dial-on-demand (DDR) calls, limiting debug output, and identifying or classifying traffic for quality of service (QoS) features. This module provides an overview of IP access lists.

Contents

- [Information About IP Access Lists, page 2](#)
- [Where to Go Next, page 12](#)
- [Additional References, page 12](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Information About IP Access Lists

This module contains the following concepts, which you should understand before configuring an IP access control list (ACL), also known as an access list:

- [Benefits of IP Access Lists, page 2](#)
- [Border Routers and Firewall Routers Should Use Access Lists, page 3](#)
- [Definition of an Access List, page 4](#)
- [Software Processing of an Access List, page 5](#)
- [Access List Rules, page 5](#)
- [Helpful Hints for Creating IP Access Lists, page 6](#)
- [Named or Numbered Access Lists, page 7](#)
- [Standard or Extended Access Lists, page 7](#)
- [IP Packet Fields You Can Filter to Control Access, page 8](#)
- [Wildcard Mask for Addresses in an Access List, page 9](#)
- [Access List Sequence Numbers, page 9](#)
- [Access List Logging, page 10](#)
- [Additional IP Access List Features, page 10](#)
- [Time-Based and Distributed Time-Based Access Lists, page 11](#)
- [Types of IP Access Lists, page 11](#)
- [Where to Apply an Access List, page 11](#)

Benefits of IP Access Lists

Access control lists (ACLs) perform packet filtering to control which packets move through the network and where. Such control can restrict the access of users and devices to the network, providing a measure of security. Access lists can save network resources by reducing traffic. Access lists provide diverse benefits, depending on how they are used. Many of the benefits fall into the following categories:

Block Unwanted Traffic or Users

Access lists can filter incoming or outgoing packets on an interface, thereby controlling access based on source addresses, destination addresses, or user authentication. You can also use access lists to determine which types of traffic are forwarded or blocked at the router interfaces. For example, you can permit e-mail traffic to be routed, but at the same time block all Telnet traffic.

Reduce the Chance of DOS Attacks

There are a number of ways to reduce the chance of denial-of-service attacks. For example, by specifying IP source addresses, you can control whether traffic from hosts, networks, or users access your network. You can filter on specific time-to-live (TTL) values in packets to control how many hops a packet can take before reaching a router in your network. By configuring the TCP Intercept feature, you can prevent servers from being flooded with requests for a connection.

Control Access to Virtual Terminal Lines

You can place an access list on inbound vty (Telnet) line access from certain nodes or networks. You can also place an access list on outbound vty access, blocking or permitting Telnet access to other devices.

Restrict the Content of Routing Updates

Access lists can control routing updates being sent, received, or redistributed.

Provide Bandwidth Control

An access list on a slow link can prevent excess traffic.

Identify or Classify Traffic for QoS Features

Access lists can provide congestion avoidance by setting IP precedence for WRED or CAR. It can provide congestion management for class-based weighted fair queuing (WFQ), priority queuing, and custom queuing.

Trigger Dial-on-Demand (DDR) Calls

An access list can enforce dialing and disconnect criteria.

Limit Debug Command Output

An access list can limit debug output based on an address or protocol.

Provide NAT Control

Access lists can control which addresses are translated by Network Address Translation (NAT).

Authenticate Incoming RSH and RCP Requests

To enable the Cisco IOS software to receive incoming remote shell (rsh) protocol and remote copy (rcp) protocol requests, customers must configure an authentication database to control access to the router. Access lists can simplify the identification of local users, remote hosts, and remote users in the database authentication configuration.

Border Routers and Firewall Routers Should Use Access Lists

There are many reasons to configure access lists; for example, you can use access lists to restrict contents of routing updates or to provide traffic flow control. One of the most important reasons to configure access lists is to provide a basic level of security for your network by controlling access to it. If you do not configure access lists on your router, all packets passing through the router could be allowed onto all parts of your network.

An access list can allow one host to access a part of your network and prevent another host from accessing the same area. In [Figure 1](#), by applying an appropriate access list to the interfaces of the router, Host A is allowed to access the Human Resources network and Host B is prevented from accessing the Human Resources network.

Figure 1 *Traffic Filters to Prevent Traffic from Being Routed to a Network*



Access lists should be used in firewall routers, which are often positioned between your internal network and an external network such as the Internet. You can also use access lists on a router positioned between two parts of your network, to control traffic entering or exiting a specific part of your internal network.

To provide some security benefits of access lists, you should at least configure access lists on border routers—routers located at the edges of your networks. Such an access list provides a basic buffer from the outside network or from a less controlled area of your own network into a more sensitive area of your network. On these border routers, you should configure access lists for each network protocol configured on the router interfaces. You can configure access lists so that inbound traffic or outbound traffic or both are filtered on an interface.

Access lists are defined on a per-protocol basis. In other words, you should define access lists for every protocol enabled on an interface if you want to control traffic flow for that protocol.

Definition of an Access List

An access list is a sequential list consisting of at least one **permit** statement and possibly one or more **deny** statements. In the case of IP access lists, the statements can apply to IP addresses, upper-layer IP protocols, or other fields in IP packets. The access list is identified and referenced by a name or a number. The access list acts as a packet filter, filtering packets based on the criteria defined in the access list.

An access list may be configured, but it does not take effect until the access list is either applied to an interface (with the **ip access-group** command), a virtual terminal line (vty) (with the **access-class** command), or referenced by some other command that accepts an access list. Access lists have many uses, and therefore many Cisco IOS software commands accept a reference to an access list in their command syntax. Multiple commands can reference the same access list.

In the following configuration excerpt, the first three lines are an example of an IP access list named `branchoffices`, which is applied to serial interface 0 on incoming packets. No sources other than those on the networks specified by each source address and mask pair can access this interface. The destinations for packets coming from sources on network 172.20.7.0 are unrestricted. The destination for packets coming from sources on network 172.29.2.0 must be 172.25.5.4.

```
ip access-list extended branchoffices
 10 permit 172.20.7.0 0.0.0.3 any
 20 permit 172.29.2.0 0.0.0.255 host 172.25.5.4
```



```
!  
interface serial 0  
 ip access-group branchoffices in
```

Software Processing of an Access List

The following general steps describe how the Cisco IOS software processes an access list when it is applied to an interface, a vty, or referenced by some other Cisco IOS command. These steps apply to an access list that has 13 or fewer access list entries.

- The software receives an IP packet and tests parts of each packet being filtered against the conditions in the access list, one condition (**permit** or **deny** statement) at a time. For example, the software tests the source and destination addresses of the packet against the source and destination addresses in a **permit** or **deny** statement.
- If a packet does not match an access list statement, the packet is then tested against the next statement in the list.
- If a packet and an access list statement match, the rest of the statements in the list are skipped and the packet is permitted or denied as specified in the matched statement. The first entry that the packet matches determines whether the software permits or denies the packet. That is, after the first match, no subsequent entries are considered.
- If the access list denies a packet, the software discards the packet and returns an ICMP Host Unreachable message.
- If no conditions match, the software drops the packet. This is because each access list ends with an unwritten, implicit **deny** statement. That is, if the packet has not been permitted by the time it was tested against each statement, it is denied.

In later Cisco IOS releases such as Release 12.4, 12.2S, and 12.0S, by default, an access list that has more than 13 access list entries is processed differently from one that has 13 or fewer entries. In order to be more efficient, an access list with more than 13 entries is processed using a trie-based lookup algorithm. This process will happen automatically; it does not need to be configured.

Access List Rules

Keep the following rules and characteristics of access lists in mind when creating one:

- Only one access list per interface, per protocol, per direction is allowed.
- The access list must contain at least one **permit** statement or else all packets are denied.
- Because the software stops testing conditions after the first match, the order of the conditions is critical. The same **permit** or **deny** statements specified in a different order could result in a packet being passed under one circumstance and denied in another circumstance.
- If an access list is referenced by name in a command, but the access list does not exist, all packets pass. That is, an interface or command with an empty access list applied to it permits all traffic.
- Standard access lists and extended access lists cannot have the same name.
- Inbound access lists process packets arriving at the router. Incoming packets are processed before being routed to an outbound interface. An inbound access list is efficient because it saves the overhead of routing lookups if the packet is to be discarded because it is denied by the filtering tests. If the packet is permitted by the tests, it is then processed for routing. For inbound lists, **permit** means continue to process the packet after receiving it on an inbound interface; **deny** means discard the packet.

- Outbound access lists process packets before they leave the router. Incoming packets are routed to the outbound interface and then processed through the outbound access list. For outbound lists, **permit** means send it to the output buffer; **deny** means discard the packet.
- An access list can control traffic arriving at the router or leaving the router, but not traffic originating at the router.

Helpful Hints for Creating IP Access Lists

The following tips will help you avoid unintended consequences and help you create more efficient, useful access lists.

- Create the access list before applying it to an interface (or elsewhere), because if you apply a nonexistent access list to an interface and then proceed to configure the access list, the first statement is put into effect, and the implicit **deny** statement that follows could cause you immediate access problems.
- Another reason to configure an access list before applying it is because an interface with an empty access list applied to it permits all traffic.
- All access lists need at least one **permit** statement; otherwise, all packets are denied and no traffic passes.
- Because the software stops testing conditions after it encounters the first match (to either a **permit** or **deny** statement), you will reduce processing time and resources if you put the statements that packets are most likely to match at the beginning of the access list. Place more frequently occurring conditions before less frequent conditions.
- Organize your access list so that more specific references in a network or subnet appear before more general ones.
- Use the statement **permit any any** if you want to allow all other packets not already denied. Using the statement **permit any any** in effect avoids denying all other packets with the implicit deny statement at the end of an access list. Do not make your first access list entry **permit any any** because all traffic will get through; no packets will reach the subsequent testing. In fact, once you specify **permit any any**, all traffic not already denied will get through.
- Although all access lists end with an implicit **deny** statement, we recommend use of an explicit **deny** statement (for example, **deny ip any any**). On most platforms, you can display the count of packets denied by issuing the **show access-list** command, thus finding out more information about who your access list is disallowing. Only packets denied by explicit **deny** statements are counted, which is why the explicit **deny** statement will yield more complete data for you.
- While you are creating an access list or after it is created, you might want to delete an entry.
 - You cannot delete an entry from a *numbered* access list; trying to do so will delete the entire access list. If you need to delete an entry, you need to delete the entire access list and start over.
 - You can delete an entry from a *named* access list. Use the **no permit** or **no deny** command to delete the appropriate entry.
- In order to make the purpose of individual statements more scannable and easily understood at a glance, you can write a helpful remark before or after any statement by using the **remark** command.
- If you want to deny access to a particular host or network and find out if someone from that network or host is attempting to gain access, include the **log** keyword with the corresponding **deny** statement so that the packets denied from that source are logged for you.

- This hint applies to the placement of your access list. When trying to save resources, remember that an inbound access list applies the filter conditions *before* the routing table lookup. An outbound access list applies the filter conditions *after* the routing table lookup.

Named or Numbered Access Lists

All access lists must be identified by a name or a number. Named and numbered access lists have different command syntax. Named access lists are compatible with Cisco IOS Release 11.2 and later. Named access lists are more convenient than numbered access lists because you can specify a meaningful name that is easier to remember and associate with a purpose. You may reorder statements in or add statements to a named access list.

Named access list are newer than numbered access lists and support the following features that are not supported in numbered access lists:

- TCP flag filtering
- IP option filtering
- noncontiguous ports
- reflexive access lists
- ability to delete entries with the **no permit** or **no deny** command

Not all commands that accept a numbered access list will accept a named access list. For example, virtual terminal lines use only numbered access lists.

Standard or Extended Access Lists

All access lists are either standard or extended access lists. If you only intend to filter on a source address, the simpler standard access list is sufficient. For filtering on anything other than a source address, an extended access list is necessary.

- Named access lists are specified as standard or extended based on the keyword **standard** or **extended** in the **ip access-list** command syntax.
- Numbered access lists are specified as standard or extended based on their number in the **access-list** command syntax. Standard IP access lists are numbered 1 to 99 or 1300 to 1999; extended IP access lists are numbered 100 to 199 or 2000 to 2699. The range of standard IP access lists was initially only 1 to 99, and was subsequently expanded with the range 1300 to 1999 (the intervening numbers were assigned to other protocols). The extended access list range was similarly expanded.

Standard Access Lists

Standard IP access lists test only source addresses of packets (except for two exceptions). Because standard access lists test source addresses, they are very efficient at blocking traffic close to a destination. There are two exceptions when the address in a standard access list is not a source address:

- On outbound VTY access lists, when someone is trying to telnet, the address in the access list entry is used as a destination address rather than a source address.
- When filtering routes, you are filtering the network being advertised to you rather than a source address.

Extended Access Lists

Extended access lists are good for blocking traffic anywhere. Extended access lists test source and destination addresses and other IP packet data, such as protocols, TCP or UDP port numbers, type of service (ToS), precedence, TCP flags, IP options, and TTL value. Extended access lists can also provide capabilities that standard access lists cannot, such as the following:

- Filtering IP Options
- Filtering TCP flags
- Filtering noninitial fragments of packets (see the module “Refining an IP Access List”)
- Time-based entries (see the [“Time-Based and Distributed Time-Based Access Lists”](#) section on page 11 and the module “Refining an IP Access List”)
- Dynamic access lists (see the section [“Types of IP Access Lists”](#) section on page 11)
- Reflexive access lists (see the section [“Types of IP Access Lists”](#) section on page 11 and the module “Configuring IP Session Filtering [Reflexive Access Lists])

**Note**

Packets that are subject to an extended access list will not be autonomous switched.

IP Packet Fields You Can Filter to Control Access

You can use an extended access list to filter on any of the following fields in an IP packet. Source address and destination address are the two most frequently specified fields on which to base an access list:

- Source address—Specifies a source address to control packets coming from certain networking devices or hosts.
- Destination address—Specifies a destination address to control packets being sent to certain networking devices or hosts.
- Protocol—Specifies an IP protocol indicated by the keyword **eigrp**, **gre**, **icmp**, **igmp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or indicated by an integer in the range from 0 to 255 (representing an Internet protocol). If you specify a transport layer protocol (**icmp**, **igmp**, **tcp**, or **udp**), the command has a specific syntax.
 - Ports and non-contiguous ports—Specifies TCP or UDP ports by a port name or port number. The port numbers can be noncontiguous port numbers. Port numbers can be useful to filter Telnet traffic or HTTP traffic, for example.
 - TCP flags—Specifies that packets match any flag or all flags set in TCP packets. Filtering on specific TCP flags can help prevent false synchronization packets.
- IP options—Specifies IP options; one reason to filter on IP options is to prevent routers from being saturated with spurious packets containing them.
- TTL value—Specifies TTL values indicated by an operator and possibly a range of values. Filtering on TTL value can control who can reach an interface based on how many hops away the source is. Such filtering can also prevent packets from reaching the process level.

Wildcard Mask for Addresses in an Access List

Address filtering uses wildcard masking to indicate to the software whether to check or ignore corresponding IP address bits when comparing the address bits in an access list entry to a packet being submitted to the access list. By carefully setting wildcard masks, you can specify one or more IP addresses for permit or deny tests.

Wildcard masking for IP address bits uses the number 1 and the number 0 to specify how the software treats the corresponding IP address bits. A wildcard mask is sometimes referred to as an inverted mask because a 1 and 0 mean the opposite of what they mean in a subnet (network) mask.

- A wildcard mask bit 0 means *check* the corresponding bit value; they must match.
- A wildcard mask bit 1 means *ignore* that corresponding bit value; they need not match.

If you do not supply a wildcard mask with a source or destination address in an access list statement, the software assumes an implicit wildcard mask of 0.0.0.0, meaning all values must match.

Unlike subnet masks, which require contiguous bits indicating network and subnet to be ones, wildcard masks allow noncontiguous bits in the mask.

Table 1 shows examples of IP addresses and masks from an access list, along with the corresponding addresses that are considered a match.

Table 1 **Sample IP Addresses, Wildcard Masks, and Match Results**

Address	Wildcard Mask	Match Results
0.0.0.0	255.255.255.255	All addresses will match the access list conditions.
172.18.0.0/16	0.0.255.255	Network 172.18.0.0
172.18.5.2/16	0.0.0.0	Only host 172.18.5.2 matches
172.18.8.0	0.0.0.7	Only subnet 172.18.8.0/29 matches
172.18.8.8	0.0.0.7	Only subnet 172.18.8.8/29 matches
172.18.8.15	0.0.0.3	Only subnet 172.18.8.15/30 matches
10.1.2.0	0.0.252.255 (noncontiguous bits in mask)	Matches any even-numbered network in the range of 10.1.2.0 to 10.1.254.0

Access List Sequence Numbers

The ability to apply sequence numbers to IP access list entries simplifies access list changes. Prior to the IP Access List Entry Sequence Numbering feature, there was no way to specify the position of an entry within an access list. If you wanted to insert an entry in the middle of an existing list, all of the entries after the desired position had to be removed, then the new entry was added, and then all the removed entries had to be reentered. This method was cumbersome and error prone.

This feature allows users to add sequence numbers to access list entries and resequence them. When you add a new entry, you specify the sequence number so that it is in a desired position in the access list. If necessary, entries currently in the access list can be resequenced to create room to insert the new entry.

Access List Logging

The Cisco IOS software can provide logging messages about packets permitted or denied by a single standard or extended IP access list entry. That is, any packet that matches the entry will cause an informational logging message about the packet to be sent to the console. The level of messages logged to the console is controlled by the **logging console** global configuration command.

The first packet that triggers the access list entry causes an immediate logging message, and subsequent packets are collected over 5-minute intervals before they are displayed or logged. The logging message includes the access list number, whether the packet was permitted or denied, the source IP address of the packet, and the number of packets from that source permitted or denied in the prior 5-minute interval.

However, you can use the **ip access-list log-update** command to set the number of packets that, when match an access list (and are permitted or denied), cause the system to generate a log message. You might want to do this to receive log messages more frequently than at 5-minute intervals.



Caution

If you set the *number-of-matches* argument to 1, a log message is sent right away, rather than caching it; every packet that matches an access list causes a log message. A setting of 1 is not recommended because the volume of log messages could overwhelm the system.

Even if you use the **ip access-list log-update** command, the 5-minute timer remains in effect, so each cache is emptied at the end of 5 minutes, regardless of the count of messages in each cache. Regardless of when the log message is sent, the cache is flushed and the count reset to 0 for that message the same way it is when a threshold is not specified.



Note

The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.

Alternative to Access List Logging

Packets matching an entry in an ACL with a log option are process switched. It is not recommended to use the log option on ACLs, but rather use NetFlow export and match on a destination interface of Null0. This is done in the CEF path. The destination interface of Null0 is set for any packet that is dropped by the ACL.

Additional IP Access List Features

Beyond the basic steps to create a standard or extended access list, you can enhance your access lists as mentioned below. Each of these methods is described completely in the module entitled “[Refining an Access List](#).”

- You can impose dates and times when **permit** or **deny** statements in an extended access list are in effect, making your access list more granular and specific to an absolute or periodic time period.
- After you create a named access list, you might want to add entries or change the order of the entries, known as resequencing an access list.
- You can achieve finer granularity when filtering packets by filtering on noninitial fragments of packets.

Time-Based and Distributed Time-Based Access Lists

Time-based access lists implement access list entries based on particular times of the day or week. This is an advantage when you don't want access list entries always in effect or in effect as soon as they are applied. Use time-based access lists to make the enforcement of permit or deny conditions granular, based on time and date.

Distributed time-based access lists are those that are supported on line cards for the Cisco 7500 series routers. Packets destined for an interface configured with time-based access lists are distributed switched through the line card.

Types of IP Access Lists

There are several types of access lists that are distinct because of how they are triggered, their temporary nature, or how their behavior differs from an ordinary access list.

Authentication Proxy

Authentication proxy provides dynamic, per-user authentication and authorization, authenticating users against industry standard TACACS+ and RADIUS authentication protocols. Authenticating and authorizing connections by users provides more robust protection against network attacks.

Context-Based Access Control

Context-based access control (CBAC) examines not only network layer and transport layer information, but also the application-layer protocol information (such as FTP information) to learn about the state of TCP and UDP connections. CBAC maintains connection state information for individual connections. This state information is used to make intelligent decisions about whether packets should be permitted or denied, and dynamically creates and deletes temporary openings in the firewall.

Dynamic Access Lists with the Lock-and-Key Feature

Dynamic access lists provide temporary access to designated users who are using Telnet to reach designated hosts through a firewall. Dynamic access lists involve user authentication and authorization.

Reflexive Access Lists

Reflexive access lists provide filtering on upper-layer IP protocol sessions. They contain temporary entries that are automatically created when a new IP session begins. They are nested within extended, named IP access lists that are applied to an interface. Reflexive access lists are typically configured on border routers, which pass traffic between an internal and external network. These are often firewall routers. Reflexive access lists do not end with an implicit deny statement because they are nested within an access list and the subsequent statements need to be examined.

Where to Apply an Access List

If you are applying an access list to an interface, carefully consider whether to specify it as **in** (inbound) or **out** (outbound). Applying an access list to an incoming or outgoing interface controls the traffic that will enter or leave the router's interface or process level (in the case of filtering on TTL values).

- When an inbound access list is applied to an interface, after the software receives a packet, the software checks the packet against the access list statements. If the access list permits the packet, the software continues to process the packet. Therefore, filtering on incoming packets can save router resources because filtered packets will not go through the router.

- Access lists that apply to outbound packets are filtering packets that have already gone through the router. Packets that pass the access list are transmitted (sent) out the interface.
- The TCP ACL splitting feature of Rate-Based Satellite Control Protocol (RBSCP) is an example of a feature that can be used on an outgoing interface. The access list controls which packets are subject to TCP ACK splitting.

Access lists can be used in ways other than applying them to interfaces. The following are additional places to apply an access list.

- To restrict incoming and outgoing connections between a particular vty (into a Cisco device) and the network devices at addresses in an access list, apply an access list to a line. See the “[Controlling Access to a Virtual Terminal Line](#)” module.
- Referencing an access list from a **debug** command limits the amount of information displayed to only the information permitted by the access list, such as sources, destinations, or protocols, for example.
- Access lists can be used to control routing updates, to control dial-on-demand routing (DDR), and to control quality of service (QoS) features, for example. See the appropriate configuration chapters for using access lists with these features.

Where to Go Next

You must first decide what you want to restrict, and then select the type of access list that achieves your goal. Next, you will create an access list that permits or denies packets based on values in the fields you specify, and finally, you will apply the access list (which determines its placement).

Assuming you have decided what you want to restrict and what type of access list you need, your next step is to create an access list. Creating an access list based on source address, destination address, or protocol is described in the “[Creating an IP Access List and Applying It to an Interface](#)” module. You could create an access list that filters on other fields, as described in “[Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values](#).” If you want to control access to a virtual line, see “Controlling Access to a Virtual Terminal Line.” If the purpose of your access list is to control routing updates or QoS features, for example, see the appropriate technology chapter.

Additional References

The following sections provide references related to IP access lists.

Related Documents

Related Topic	Document Title
IP access list commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS IP Application Services Command Reference, Release 12.4
Filtering on source address, destination address, or protocol	“Creating an IP Access List and Applying It to an Interface”
Filtering on IP Options, TCP flags, noncontiguous ports, or TTL	“Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, and TTL Values”
Restricting access to a vty line.	“Controlling Access to a Virtual Terminal Line”

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Creating an IP Access List and Applying It to an Interface

First Published: August 18, 2006

Last Updated: August 18, 2006

IP access lists provide many benefits for securing a network and achieving nonsecurity goals, such as determining quality of service (QoS) factors or limiting **debug** command output. This module describes how to create standard, extended, named, and numbered IP access lists. An access list can be referenced by a name or a number. Standard access lists filter on only the source address in IP packets. Extended access lists can filter on source address, destination address, and other fields in an IP packet.

After you create an access list, you must apply it to something in order for it to have any effect. This module describes how to apply an access list to an interface. However, there are many other uses for an access list, which are referenced in this module and described in other modules and in other configuration guides for various technologies.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Creating IP Access Lists](#)” section on page 24.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Creating an IP Access List and Applying It to an Interface, page 2](#)
- [Information About Creating an IP Access List and Applying It to an Interface, page 2](#)
- [How to Create an IP Access List and Apply It to an Interface, page 4](#)
- [Configuration Examples for IP Access Lists, page 17](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Where to Go Next, page 21](#)
- [Additional References, page 22](#)

Prerequisites for Creating an IP Access List and Applying It to an Interface

Before you create or apply an IP access list, you should understand the concepts in the “IP Access List Overview” module. You should also have IP running in your network.

Information About Creating an IP Access List and Applying It to an Interface

You should understand the following concepts before creating an IP access list.

- [Helpful Hints for Creating IP Access Lists, page 2](#)
- [Access List Remarks, page 3](#)
- [Additional IP Access List Features, page 3](#)

Helpful Hints for Creating IP Access Lists

The following tips will help you avoid unintended consequences and help you create more efficient access lists.

- Create the access list before applying it to an interface (or elsewhere), because if you apply a nonexistent access list to an interface and then proceed to configure the access list, the first statement is put into effect, and the implicit **deny** statement that follows could cause you immediate access problems.
- Another reason to configure an access list before applying it is because an interface with an empty access list applied to it permits all traffic.
- All access lists need at least one **permit** statement; otherwise, all packets are denied and no traffic passes.
- Because the software stops testing conditions after it encounters the first match (to either a **permit** or **deny** statement), you will reduce processing time and resources if you put the statements that packets are most likely to match at the beginning of the access list. Place more frequently occurring conditions before less frequent conditions.
- Organize your access list so that more specific references in a network or subnet appear before more general ones.
- Use the statement **permit any any** if you want to allow all other packets not already denied. Using the statement **permit any any** in effect avoids denying all other packets with the implicit deny statement at the end of an access list. Do not make your first access list entry **permit any any** because all traffic will get through; no packets will reach the subsequent testing. In fact, once you specify **permit any any**, all traffic not already denied will get through.

- Although all access lists end with an implicit **deny** statement, we recommend use of an explicit **deny** statement (for example, **deny ip any any**). On most platforms, you can display the count of packets denied by issuing the **show access-list** command, thus finding out more information about who your access list is disallowing. Only packets denied by explicit **deny** statements are counted, which is why the explicit **deny** statement will yield more complete data for you.
- While you are creating an access list or after it is created, you might want to delete an entry.
 - You cannot delete an entry from a *numbered* access list; trying to do so will delete the entire access list. If you need to delete an entry, you need to delete the entire access list and start over.
 - You can delete an entry from a *named* access list. Use the **no permit** or **no deny** command to delete the appropriate entry.
- In order to make the purpose of individual statements more scannable and easily understood at a glance, you can write a helpful remark before or after any statement by using the **remark** command.
- If you want to deny access to a particular host or network and find out if someone from that network or host is attempting to gain access, include the **log** keyword with the corresponding **deny** statement so that the packets denied from that source are logged for you.
- This hint applies to the placement of your access list. When trying to save resources, remember that an inbound access list applies the filter conditions *before* the routing table lookup. An outbound access list applies the filter conditions *after* the routing table lookup.

Access List Remarks

You can include comments (remarks) about entries in a named IP access list. An access list remark is an optional comment before or after an access list entry that describes the entry for you at a glance, so you do not have to interpret the purpose of the entry by its command syntax. Each remark is limited to 100 characters.

The remark can go before or after a **permit** or **deny** statement. You should be consistent about where you put your remarks so that it is clear which remark describes which statement. It could be confusing to have some remarks before the associated **permit** or **deny** statements and some remarks after the associated statements.

The following example of a remark is a user-friendly description of what the subsequent **deny** statement does.

```
ip access-list extended telnetting
remark Do not allow host1 subnet to telnet out
deny tcp host 172.69.2.88 any eq telnet
```

Additional IP Access List Features

Beyond the basic steps to create a standard or extended access list, you can enhance your access lists as mentioned below. Each of these methods is described completely in the module entitled “[Refining an Access List](#).”

- You can impose dates and times when **permit** or **deny** statements in an extended access list are in effect, making your access list more granular and specific to an absolute or periodic time period.
- After you create a named or numbered access list, you might want to add entries or change the order of the entries, known as resequencing an access list.
- You can achieve finer granularity when filtering packets by filtering on noninitial fragments of packets.

How to Create an IP Access List and Apply It to an Interface

This section describes the general ways to create a standard or extended access list using either a name or a number. Access lists are very flexible; the tasks simply illustrate one **permit** command and one **deny** command to provide you the command syntax of each. Only you can determine how many **permit** and **deny** commands you need and their order.



Note

The first two tasks in this module create an access list; you must apply the access list in order for it to function. If you want to apply the access list to an interface, perform the task [“Applying the Access List to an Interface” section on page 16](#).

If you don’t intend to apply the access list to an interface, see the [“Where to Go Next” section on page 21](#) for pointers to modules that describe other ways to apply access lists.

- [Creating a Standard Access List to Filter on Source Address, page 4](#)
- [Creating an Extended Access List, page 10](#)
- [Applying the Access List to an Interface, page 16](#)

Creating a Standard Access List to Filter on Source Address

If you want to filter on source address only, a standard access list is simple and sufficient. There are two alternative types of standard access list: named and numbered. Named access lists allow you to identify your access lists with a more intuitive name rather than a number, and they also support more features than numbered access lists.

- [Creating a Named Access List to Filter on Source Address, page 4](#)
- [Creating a Numbered Access List to Filter on Source Address, page 7](#)

Creating a Named Access List to Filter on Source Address

Use a standard, named access list if you need to filter on source address only. This task illustrates one **permit** statement and one **deny** statement, but the actual statements you use and their order depend on what you want to filter or allow. Define your **permit** and **deny** statements in the order that achieves your filtering goals.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list standard** *name*
4. **remark** *remark*
5. **deny** {*source* [*source-wildcard*] | **any**} [**log**]
6. **remark** *remark*
7. **permit** {*source* [*source-wildcard*] | **any**} [**log**]
8. Repeat some combination of Steps 4 through 7 until you have specified the source networks and hosts on which you want to base your access list.

9. `end`
10. `show ip access-list`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip access-list standard name Example: Router(config)# ip access-list standard R&D	Defines a standard IP access list using a name and enters standard named access list configuration mode.
Step 4	remark remark Example: Router(config-std-nacl)# remark deny Sales network	(Optional) Adds a user-friendly comment about an access list entry. <ul style="list-style-type: none"> A remark can precede or follow an access list entry. In this example, the remark reminds the network administrator that the subsequent entry denies the Sales network access to the interface (assuming this access list is later applied to an interface).
Step 5	deny {source [source-wildcard] any} [log] Example: Router(config-std-nacl)# deny 172.16.0.0 0.0.255.255 log	(Optional) Denies the specified source based on a source address and wildcard mask. <ul style="list-style-type: none"> If the <i>source-wildcard</i> is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source address. Optionally use the keyword any as a substitute for the <i>source source-wildcard</i> to specify the source and source wildcard of 0.0.0.0 255.255.255.255. In this example, all hosts on network 172.16.0.0 are denied passing the access list. Because this example explicitly denies a source address and the log keyword is specified, any packets from that source are logged when they are denied. This is a way to be notified that someone on a network or host is trying to gain access.
Step 6	remark remark Example: Router(config-std-nacl)# remark Give access to Tester's host	(Optional) Adds a user-friendly comment about an access list entry. <ul style="list-style-type: none"> A remark can precede or follow an access list entry. This remark reminds the network administrator that the subsequent entry allows the Tester's host access to the interface.

	Command or Action	Purpose
Step 7	<p>permit {<i>source</i> [<i>source-wildcard</i>] any} [log]</p> <p>Example: Router(config-std-nacl)# permit 172.18.5.22 0.0.0.0</p>	<p>Permits the specified source based on a source address and wildcard mask.</p> <ul style="list-style-type: none"> Every access list needs at least one permit statement; it need not be the first entry. If the <i>source-wildcard</i> is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source address. Optionally use the keyword any as a substitute for the <i>source source-wildcard</i> to specify the source and source wildcard of 0.0.0.0 255.255.255.255. In this example, host 172.18.5.22 is allowed to pass the access list.
Step 8	Repeat some combination of Steps 4 through 7 until you have specified the sources on which you want to base your access list.	Remember that all sources not specifically permitted are denied by an implicit deny statement at the end of the access list.
Step 9	<p>end</p> <p>Example: Router(config-std-nacl)# end</p>	Ends configuration mode and brings the system to privileged EXEC mode.
Step 10	<p>show ip access-list</p> <p>Example: Router# show ip access-list</p>	(Optional) Displays the contents of all current IP access lists.

What to Do Next

The access list you created is not in effect until you apply it to an interface, a vty line, or reference it from a command that uses an access list. See the [“Applying the Access List to an Interface”](#) section on page 16 or the [“Where to Go Next”](#) section on page 21 for pointers to modules that describe other ways to use access lists.

Creating a Numbered Access List to Filter on Source Address

Configure a standard, numbered access list if you need to filter on source address only and you prefer not to use a named access list.

IP standard access lists are numbered 1 to 99 or 1300 to 1999. This task illustrates one **permit** statement and one **deny** statement, but the actual statements you use and their order depend on what you want to filter or allow. Define your **permit** and **deny** statements in the order that achieves your filtering goals.

SUMMARY STEPS

- enable**
- configure terminal**
- access-list** *access-list-number* **remark** *remark*
- access-list** *access-list-number* **permit** {*source* [*source-wildcard*] | **any**} [**log**]

5. **access-list** *access-list-number* **remark** *remark*
6. **access-list** *access-list-number* **deny** {*source* [*source-wildcard*] | **any**} [**log**]
7. Repeat some combination of Steps 3 through 6 until you have specified the sources on which you want to base your access list.
8. **end**
9. **show ip access-list**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	access-list access-list-number remark remark Example: Router(config)# access-list 1 remark Give access to Jones	(Optional) Adds a user-friendly comment about an access list entry. <ul style="list-style-type: none"> A remark of up to 100 characters can precede or follow an access list entry.
Step 4	access-list access-list-number permit {source [source-wildcard] any} [log] Example: Router(config)# access-list 1 permit 172.16.5.22 0.0.0.0	Permits the specified source based on a source address and wildcard mask. <ul style="list-style-type: none"> Every access list needs at least one permit statement; it need not be the first entry. Standard IP access lists are numbered 1 to 99 or 1300 to 1999. If the <i>source-wildcard</i> is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source address. Optionally use the keyword any as a substitute for the <i>source source-wildcard</i> to specify the source and source wildcard of 0.0.0.0 255.255.255.255. In this example, host 172.16.5.22 is allowed to pass the access list.
Step 5	access-list access-list-number remark remark Example: Router(config)# access-list 1 remark Don't give access to Johnson and log any attempts	(Optional) Adds a user-friendly comment about an access list entry. <ul style="list-style-type: none"> A remark of up to 100 characters can precede or follow an access list entry.
Step 6	access-list access-list-number deny {source [source-wildcard] any} [log] Example: Router(config)# access-list 1 deny 172.16.7.34 0.0.0.0	Denies the specified source based on a source address and wildcard mask. <ul style="list-style-type: none"> If the <i>source-wildcard</i> is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source address. Optionally use the abbreviation any as a substitute for the <i>source source-wildcard</i> to specify the source and source wildcard of 0.0.0.0 255.255.255.255. In this example, host 172.16.7.34 is denied passing the access list.

	Command or Action	Purpose
Step 7	Repeat some combination of Steps 3 through 6 until you have specified the sources on which you want to base your access list.	Remember that all sources not specifically permitted are denied by an implicit deny statement at the end of the access list.
Step 8	end Example: Router(config-std-nacl)# end	Ends configuration mode and brings the system to privileged EXEC mode.
Step 9	show ip access-list Example: Router# show ip access-list	(Optional) Displays the contents of all current IP access lists.

What to Do Next

The access list you created is not in effect until you apply it to an interface, a vty line, or reference it from a command that uses an access list. See the [“Applying the Access List to an Interface” section on page 16](#) or the [“Where to Go Next” section on page 21](#) for pointers to modules that describe other ways to use access lists.

Creating an Extended Access List

If you want to filter on anything other than source address, you need to create an extended access list. There are two alternative types of extended access list: named and numbered. Named access lists allow you to identify your access lists with a more intuitive name rather than a number, and they also support more features.

For details on how to filter something other than source or destination address, see the syntax descriptions in the command reference documentation.

- [Creating a Named Extended Access List, page 10](#)
- [Creating a Numbered Extended Access List, page 13](#)

Creating a Named Extended Access List

Create a named extended access list if you want to filter on source and destination address, or a combination of addresses and other IP fields.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list extended** *name*
4. **remark** *remark*
5. **deny** *protocol source [source-wildcard] destination [destination-wildcard] [option option-name] [precedence precedence] [tos tos] [established] [log | log-input] [time-range time-range-name] [fragments]*

6. **remark** *remark*
7. **permit** *protocol source [source-wildcard] destination [destination-wildcard]* [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]
8. Repeat some combination of Steps 4 through 7 until you have specified the fields and values on which you want to base your access list.
9. **end**
10. **show ip access-list**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip access-list extended name Example: Router(config)# ip access-list extended nomarketing	Defines an extended IP access list using a name and enters extended named access list configuration mode.
Step 4	remark remark Example: Router(config-ext-nacl)# remark protect server by denying access from the Marketing network	(Optional) Adds a user-friendly comment about an access list entry. <ul style="list-style-type: none"> A remark can precede or follow an access list entry. In this example, the remark reminds the network administrator that the subsequent entry denies the Sales network access to the interface.
Step 5	deny protocol source [source-wildcard] destination [destination-wildcard] [option option-name] [precedence precedence] [tos tos] [established] [log log-input] [time-range time-range-name] [fragments] Example: Router(config-ext-nacl)# deny ip 172.18.0.0 0.0.255.255 host 172.16.40.10 log	(Optional) Denies any packet that matches all of the conditions specified in the statement. <ul style="list-style-type: none"> If the <i>source-wildcard</i> or <i>destination-wildcard</i> is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source or destination address, respectively. Optionally use the keyword any as a substitute for the <i>source source-wildcard</i> or <i>destination destination-wildcard</i> to specify the address and wildcard of 0.0.0.0 255.255.255.255. Optionally use the keyword host source to indicate a source and source wildcard of <i>source</i> 0.0.0.0 or the abbreviation host destination to indicate a destination and destination wildcard of <i>destination</i> 0.0.0.0. In this example, packets from all sources are denied access to the destination network 172.18.0.0. Logging messages about packets permitted or denied by the access list are sent to the facility configured by the logging facility command (for example, console, terminal, or syslog). That is, any packet that matches the access list will cause an informational logging message about the packet to be sent to the configured facility. The level of messages logged to the console is controlled by the logging console command.

	Command or Action	Purpose
Step 6	remark <i>remark</i> Example: Router(config-ext-nacl)# remark allow TCP from any source to any destination	(Optional) Adds a user-friendly comment about an access list entry. <ul style="list-style-type: none"> A remark can precede or follow an access list entry.
Step 7	permit <i>protocol source [source-wildcard] destination [destination-wildcard] [option option-name] [precedence precedence] [tos tos] [established] [log log-input] [time-range time-range-name] [fragments]</i> Example: Router(config-ext-nacl)# permit tcp any any	Permits any packet that matches all of the conditions specified in the statement. <ul style="list-style-type: none"> Every access list needs at least one permit statement. If the <i>source-wildcard</i> or <i>destination-wildcard</i> is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source or destination address, respectively. Optionally use the keyword any as a substitute for the <i>source source-wildcard</i> or <i>destination destination-wildcard</i> to specify the address and wildcard of 0.0.0.0 255.255.255.255. In this example, TCP packets are allowed from any source to any destination. Use the log-input keyword to include input interface, source MAC address, or virtual circuit in the logging output.
Step 8	Repeat some combination of Steps 4 through 7 until you have specified the fields and values on which you want to base your access list.	Remember that all sources not specifically permitted are denied by an implicit deny statement at the end of the access list.
Step 9	end Example: Router(config-ext-nacl)# end	Ends configuration mode and brings the system to privileged EXEC mode.
Step 10	show ip access-list Example: Router# show ip access-list	(Optional) Displays the contents of all current IP access lists.

What to Do Next

The access list you created is not in effect until you apply it to an interface, a vty line, or reference it from a command that uses an access list. See the [“Applying the Access List to an Interface”](#) section on page 16 or the [“Where to Go Next”](#) section on page 21 for pointers to modules that describe other ways to use access lists.

Creating a Numbered Extended Access List

Create a numbered extended access list if you want to filter on source and destination address, or a combination of addresses and other IP fields, and you prefer not to use a name. Extended IP access lists are numbered 100 to 199 or 2000 to 2699.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* **remark** *remark*
4. **access-list** *access-list-number* **permit** *protocol* { *source* [*source-wildcard*] | **any** } { *destination* [*destination-wildcard*] | **any** } [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]
5. **access-list** *access-list-number* **remark** *remark*
6. **access-list** *access-list-number* **deny** *protocol* { *source* [*source-wildcard*] | **any** } { *destination* [*destination-wildcard*] | **any** } [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]
7. Repeat some combination of Steps 3 through 6 until you have specified the fields and values on which you want to base your access list.
8. **end**
9. **show ip access-list**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>access-list <i>access-list-number</i> remark <i>remark</i></p> <p>Example: Router(config)# access-list 107 remark allow Telnet packets from any source to network 173.69.0.0 (headquarters)</p>	<p>(Optional) Adds a user-friendly comment about an access list entry.</p> <ul style="list-style-type: none"> A remark of up to 100 characters can precede or follow an access list entry.
Step 4	<p>access-list <i>access-list-number</i> permit <i>protocol</i> [<i>source</i> [<i>source-wildcard</i>] any] [<i>destination</i> [<i>destination-wildcard</i>] any] [precedence <i>precedence</i>] [tos <i>tos</i>] [established] [log log-input] [time-range <i>time-range-name</i>] [fragments]</p> <p>Example: Router(config)# access-list 107 permit tcp any 173.69.0.0 0.0.255.255 eq telnet</p>	<p>Permits any packet that matches all of the conditions specified in the statement.</p> <ul style="list-style-type: none"> Every access list needs at least one permit statement; it need not be the first entry. Extended IP access lists are numbered 100 to 199 or 2000 to 2699. If the <i>source-wildcard</i> or <i>destination-wildcard</i> is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source or destination address, respectively. Optionally use the keyword any as a substitute for the <i>source source-wildcard</i> or <i>destination destination-wildcard</i> to specify the address and wildcard of 0.0.0.0 255.255.255.255. TCP and other protocols have additional syntax available. See the access-list command in the command reference for complete syntax.
Step 5	<p>access-list <i>access-list-number</i> remark <i>remark</i></p> <p>Example: Router(config)# access-list 107 remark deny all other TCP packets</p>	<p>(Optional) Adds a user-friendly comment about an access list entry.</p> <ul style="list-style-type: none"> A remark of up to 100 characters can precede or follow an access list entry.

	Command or Action	Purpose
Step 6	<p>access-list <i>access-list-number</i> deny <i>protocol</i> {<i>source</i> [<i>source-wildcard</i>] any} {<i>destination</i> [<i>destination-wildcard</i>] any} [precedence <i>precedence</i>] [tos <i>tos</i>] [established] [log log-input] [time-range <i>time-range-name</i>] [fragments]</p> <p>Example: Router(config)# access-list 107 deny tcp any any</p>	<p>Denies any packet that matches all of the conditions specified in the statement.</p> <ul style="list-style-type: none"> If the <i>source-wildcard</i> or <i>destination-wildcard</i> is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source or destination address, respectively. Optionally use the keyword any as a substitute for the <i>source source-wildcard</i> or <i>destination destination-wildcard</i> to specify the address and wildcard of 0.0.0.0 255.255.255.255.
Step 7	Repeat some combination of Steps 3 through 6 until you have specified the fields and values on which you want to base your access list.	Remember that all sources not specifically permitted are denied by an implicit deny statement at the end of the access list.
Step 8	<p>end</p> <p>Example: Router(config)# end</p>	Ends configuration mode and brings the system to privileged EXEC mode.
Step 9	<p>show ip access-list</p> <p>Example: Router# show ip access-list</p>	(Optional) Displays the contents of all current IP access lists.

Applying the Access List to an Interface

Perform this task to apply an access list to an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Router(config)# interface ethernet 0	Specifies an interface and enters interface configuration mode.
Step 4	ip access-group { <i>access-list-number</i> <i>access-list-name</i> } { in out } Example: Router(config-if)# ip access-group noncorp in	Applies the specified access list to the incoming or outgoing interface. <ul style="list-style-type: none"> When you are filtering on source addresses, you typically apply the access list to an incoming interface. Filtering on source addresses is most efficient when applied near the destination.

What to Do Next

The access list you created is not in effect until you apply it to an interface, a vty line, or reference it from a command that uses an access list. See the [“Applying the Access List to an Interface”](#) section on page 16 or the [“Where to Go Next”](#) section on page 21 for pointers to modules that describe other ways to use access lists.

Configuration Examples for IP Access Lists

This section contains the following examples of named and numbered, standard and extended IP access lists that are applied to an interface or referenced by a command:

- [Filtering on Source Address \(Hosts\): Example, page 18](#)
- [Filtering on Source Address \(Subnet\): Example, page 18](#)
- [Filtering on Source Address, Destination Address, and IP Protocols: Example, page 18](#)
- [Filtering on Source Address \(Host and Subnets\) Using a Numbered Access List: Example, page 19](#)
- [Preventing Telnet Access to a Subnet: Example, page 19](#)
- [Filtering on TCP and ICMP Using Port Numbers: Example, page 19](#)
- [Allowing SMTP \(E-mail\) and Established TCP Connections: Example, page 19](#)
- [Preventing Access to the Web By Filtering on Port Name: Example, page 20](#)
- [Filtering on Source Address and Logging the Packets Permitted and Denied: Example, page 20](#)
- [Limiting Debug Output: Example, page 21](#)

Filtering on Source Address (Hosts): Example

In the following example, the workstation belonging to Jones is allowed access to Ethernet interface 0 and the workstation belonging to Smith is not allowed access:

```
interface ethernet 0
 ip access-group workstations in
!
ip access-list standard workstations
 remark Permit only Jones workstation through
 permit 172.16.2.88
 remark Do not allow Smith workstation through
 deny 172.16.3.13
```

Filtering on Source Address (Subnet): Example

In the following example, the Jones subnet is not allowed access to Ethernet interface 0, but the Main subnet is allowed access:

```
interface ethernet 0
 ip access-group prevention in
!
ip access-list standard prevention
 remark Do not allow Jones subnet through
 deny 172.22.0.0 0.0.255.255
 remark Allow Main subnet
 permit 172.25.0.0 0.0.255.255
```

Filtering on Source Address, Destination Address, and IP Protocols: Example

The following configuration example shows an interface with two access lists, one applied to outgoing packets and one applied to incoming packets. The standard access list named Internet_filter filters outgoing packets on source address. The only packets allowed out the interface must be from source 172.16.3.4.

The extended access list named marketing_group filters incoming packets. The access list permits Telnet packets from any source to network 172.26.0.0 and denies all other TCP packets. It permits any ICMP packets. It denies UDP packets from any source to network 172.26.0.0 on port numbers less than 1024. Finally, the access list denies all other IP packets and performs logging of packets passed or denied by that entry.

```
interface Ethernet0/5
 ip address 172.20.5.1 255.255.255.0
 ip access-group Internet_filter out
 ip access-group marketing_group in
!
ip access-list standard Internet_filter
 permit 172.16.3.4
ip access-list extended marketing_group
 permit tcp any 172.26.0.0 0.0.255.255 eq telnet
 deny tcp any any
 permit icmp any any
 deny udp any 172.26.0.0 0.0.255.255 lt 1024
 deny ip any any
```

Filtering on Source Address (Host and Subnets) Using a Numbered Access List: Example

In the following example, network 10.0.0.0 is a Class A network whose second octet specifies a subnet; that is, its subnet mask is 255.255.0.0. The third and fourth octets of a network 10.0.0.0 address specify a particular host. Using access list 2, the Cisco IOS software would accept one address on subnet 48 and reject all others on that subnet. The last line of the list shows that the software would accept addresses on all other network 10.0.0.0 subnets.

```
interface ethernet 0
  ip access-group 2 in
!
access-list 2 permit 10.48.0.3
access-list 2 deny 10.48.0.0 0.0.255.255
access-list 2 permit 10.0.0.0 0.255.255.255
```

Preventing Telnet Access to a Subnet: Example

In the following example, the Jones subnet is not allowed to Telnet out Ethernet interface 0:

```
interface ethernet 0
  ip access-group telnetting out
!
ip access-list extended telnetting
  remark Do not allow Jones subnet to telnet out
  deny tcp 172.20.0.0 0.0.255.255 any eq telnet
  remark Allow Top subnet to telnet out
  permit tcp 172.33.0.0 0.0.255.255 any eq telnet
```

Filtering on TCP and ICMP Using Port Numbers: Example

In the following example, the first line of the extended access list named goodports permits any incoming TCP connections with destination ports greater than 1023. The second line permits incoming TCP connections to the Simple Mail Transfer Protocol (SMTP) port of host 172.28.1.2. The last line permits incoming ICMP messages for error feedback.

```
interface ethernet 0
  ip access-group goodports in
!
ip access-list extended goodports
  permit tcp any 172.28.0.0 0.0.255.255 gt 1023
  permit tcp any host 172.28.1.2 eq 25
  permit icmp any 172.28.0.0 255.255.255.255
```

Allowing SMTP (E-mail) and Established TCP Connections: Example

Suppose you have a network connected to the Internet, and you want any host on an Ethernet to be able to form TCP connections to any host on the Internet. However, you do not want IP hosts to be able to form TCP connections to hosts on the Ethernet except to the mail (SMTP) port of a dedicated mail host.

SMTP uses TCP port 25 on one end of the connection and a random port number on the other end. The same two port numbers are used throughout the life of the connection. Mail packets coming in from the Internet will have a destination port of 25. Outbound packets will have the port numbers reversed. The

fact that the secure system behind the router always will accept mail connections on port 25 is what makes possible separate control of incoming and outgoing services. The access list can be configured on either the outbound or inbound interface.

In the following example, the Ethernet network is a Class B network with the address 172.18.0.0, and the address of the mail host is 172.18.1.2. The **established** keyword is used only for the TCP protocol to indicate an established connection. A match occurs if the TCP datagram has the ACK or RST bits set, which indicate that the packet belongs to an existing connection.

```
interface ethernet 0
  ip access-group 102 in
!
access-list 102 permit tcp any 172.18.0.0 0.0.255.255 established
access-list 102 permit tcp any host 172.18.1.2 eq 25
```

Preventing Access to the Web By Filtering on Port Name: Example

In the following example, the Winter and Smith workstations are not allowed web access; other hosts on network 172.20.0.0 are allowed web access:

```
interface ethernet 0
  ip access-group no_web out
!
ip access-list extended no_web
  remark Do not allow Winter to browse the web
  deny host 172.20.3.85 any eq http
  remark Do not allow Smith to browse the web
  deny host 172.20.3.13 any eq http
  remark Allow others on our network to browse the web
  permit 172.20.0.0 0.0.255.255 any eq http
```

Filtering on Source Address and Logging the Packets Permitted and Denied: Example

The following example defines access lists 1 and 2, both of which have logging enabled:

```
interface ethernet 0
  ip address 172.16.1.1 255.0.0.0
  ip access-group 1 in
  ip access-group 2 out
!
access-list 1 permit 172.25.0.0 0.0.255.255 log
access-list 1 deny 172.30.0.0 0.0.255.255 log
!
access-list 2 permit 172.27.3.4 log
access-list 2 deny 172.17.0.0 0.0.255.255 log
```

If the interface receives 10 packets from 172.25.7.7 and 14 packets from 172.17.23.21, the first log will look like the following:

```
list 1 permit 172.25.7.7 1 packet
list 2 deny 172.17.23.21 1 packet
```

Five minutes later, the console will receive the following log:

```
list 1 permit 172.25.7.7 9 packets
list 2 deny 172.17.23.21 13 packets
```

Limiting Debug Output: Example

The following example configuration example uses an access list to limit the **debug** command output displayed. Limiting debug output narrows the volume of data to what you are interested in, saving you time and resources.

```
ip access-list idaho
  remark Displays only advertisements for LDP peer in idaho
  permit host 10.0.0.44

Router# debug mpls ldp advertisements peer-acl idaho

tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 172.17.0.33
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 172.16.0.31
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 172.22.0.33
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 192.168.0.1
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 192.168.0.3
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 192.168.1.33
```

Where to Go Next

This module describes how to create an access list that permits or denies packets based on source or destination address or protocol. However, there are other fields you could filter on, and other ways to use access lists. If you want to create an access list that filters on other fields or if you want to apply an access list to something other than an interface, you should decide what you want to restrict in your network and determine the type of access list that achieves your goal.

See the following table for references to other fields to filter and other ways to use an IP access list.

If you want to...	See
Filter based on IP Options, TCP flags, noncontiguous ports, or TTL value	“Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values” module
Reorder your access list entries	“Refining an IP Access List” module
Limit access list entries to a time of day or week	“Refining an IP Access List” module
Restrict packets with noninitial fragments	“Refining an IP Access List” module
Restrict access to virtual terminal lines	“Controlling Access to a Virtual Terminal Line”
Control routing updates	“Configuring Routing Protocol-Independent Features” module in the Cisco IOS IP Routing Protocols Configuration Guide , Release 12.4
Identify or classify traffic for features such as congestion avoidance, congestion management, and priority queuing	“Regulating Packet Flow on a Per-Interface Basis—Using Generic Traffic Shaping” module in the Quality of Service Solutions Configuration Guide , Release 12.4

If you want to...	See
Trigger dial-on-demand (DOD) calls	“Preparing to Configure DDR” module in the Cisco IOS Dial Technologies Configuration Guide , Release 12.4
Configure authentication proxy	“Configuring Authentication Proxy” module in the Cisco IOS Security Configuration Guide , Release 12.4
Configure reflexive access lists	“Configuring IP Session Filtering (Reflexive Access Lists)” module in the Cisco IOS Security Configuration Guide , Release 12.4
Configure Context-Based Access Control (CBAC)	“Configuring Lock-and-Key Security (Dynamic Access Lists)” module in the Cisco IOS Security Configuration Guide , Release 12.4
Configure dynamic access lists	“Configuring Context-Based Access Control” module in the Cisco IOS Security Configuration Guide , Release 12.4
Configure TCP Intercept	“Configuring TCP Intercept (Preventing Denial-of-Service Attacks)” module in the Cisco IOS Security Configuration Guide , Release 12.4

Additional References

The following sections provide references related to IP access lists.

Related Documents

Related Topic	Document Title
Order of access list entries	“Refining an IP Access List” module in the Cisco IOS Security Configuration Guide , Release 12.4
Access list entries based on time of day or week	“Refining an IP Access List” module in the Cisco IOS Security Configuration Guide , Release 12.4
Packets with noninitial fragments	“Refining an IP Access List” module in the Cisco IOS Security Configuration Guide , Release 12.4
Filtering on IP Options, TCP flags, noncontiguous ports, or TTL values	“Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values” module in the Cisco IOS Security Configuration Guide , Release 12.4
Access to virtual terminal lines	“Controlling Access to a Virtual Terminal Line” module in the Cisco IOS Security Configuration Guide , Release 12.4
Routing updates and policy routing	“Configuring Routing Protocol-Independent Features” modules in the Cisco IOS IP Routing Protocols Configuration Guide , Release 12.4
Traffic identification or classification for features such as congestion avoidance, congestion management, and priority queuing	“Regulating Packet Flow on a Per-Interface Basis—Using Generic Traffic Shaping” module in the Quality of Service Solutions Configuration Guide , Release 12.4
Dial-on-demand (DOD) calls	“Preparing to Configure DDR” module in the Cisco IOS Dial Technologies Configuration Guide , Release 12.4
Authentication proxy	“Configuring Authentication Proxy” module in the Cisco IOS Security Configuration Guide , Release 12.4
Reflexive access lists	“Configuring IP Session Filtering (Reflexive Access Lists)” module in the Cisco IOS Security Configuration Guide , Release 12.4
Context-Based Access Control (CBAC)	“Configuring Lock-and-Key Security (Dynamic Access Lists)” module in the Cisco IOS Security Configuration Guide , Release 12.4
Dynamic access lists	“Configuring Context-Based Access Control” module in the Cisco IOS Security Configuration Guide , Release 12.4
TCP Intercept	“Configuring TCP Intercept (Preventing Denial-of-Service Attacks)” module in the Cisco IOS Security Configuration Guide , Release 12.4

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Creating IP Access Lists

[Table 1](#) lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the IP Access List Roadmap.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

[Table 1](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 *Feature Information for Creating IP Access Lists*

Feature Name	Releases	Feature Configuration Information
—	Cisco IOS	For information about feature support in Cisco IOS software, use Cisco Feature Navigator.
Commented IP Access List Entries	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
Standard IP Access List Logging	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values

First Published: August 18, 2006
Last Updated: August 18, 2006

This module describes how to use an IP access list to filter IP packets that contain certain IP Options, TCP flags, noncontiguous ports, or time-to-live (TTL) values.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Using an IP Access List to Filter Packets](#)” section on page 21.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values, page 2](#)
- [How to Create an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values, page 2](#)
- [Configuration Examples for Filtering IP Options, TCP Flags, Noncontiguous Ports, and TTL Values, page 17](#)
- [Additional References, page 20](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values

Before you perform any of the tasks in this module, you should be familiar with the information in the following modules:

- “IP Access List Overview”
- “Creating an IP Access List and Applying It to an Interface”

How to Create an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values

This section includes the following optional tasks:

- [Filtering Packets That Contain IP Options, page 2](#)
- [Filtering Packets That Contain TCP Flags, page 5](#)
- [Configuring an Access Control Entry with Noncontiguous Ports, page 8](#)
- [Consolidating Access List Entries with Noncontiguous Ports into One Access List Entry, page 10](#)
- [Filtering Packets Based on TTL Value, page 12](#)
- [Enabling Control Plane Policing to Filter on TTL Values 0 and 1, page 15](#)

Filtering Packets That Contain IP Options

The task in this section configures an access list to filter packets that contain IP Options and verifies that the access list has been configured correctly.

IP Options

IP uses four key mechanisms in providing its service: Type of Service, Time to Live, Options, and Header Checksum.

The Options, commonly referred to as IP Options, provide for control functions that are required in some situations but unnecessary for the most common communications. IP Options include provisions for time stamps, security, and special routing.

IP Options may or may not appear in datagrams. They must be implemented by all IP modules (host and gateways). What is optional is their transmission in any particular datagram, not their implementation. In some environments the security option may be required in all datagrams.

The option field is variable in length. There may be zero or more options. IP Options can have one of two formats:

- Format 1: A single octet of option-type.
- Format 2: An option-type octet, an option-length octet, and the actual option-data octets.

The option-length octet counts the option-type octet, the option-length octet, and the option-data octets.

The option-type octet is viewed as having three fields: a 1-bit copied flag, a 2-bit option class, and a 5-bit option number. These fields form an 8-bit value for the option type field. IP Options are commonly referred to by their 8-bit value.

For a complete list and description of IP Options, refer to RFC 791, *Internet Protocol* at the following URL:

<http://www.faqs.org/rfcs/rfc791.html>

Benefits of Filtering IP Options

- Filtering of packets that contain IP Options from the network relieves downstream routers and hosts of the load from options packets.
- This feature also minimizes load to the Route Processor (RP) for packets with IP Options that require RP processing on distributed systems. Previously, the packets were always routed to or processed by the RP CPU. Filtering the packets prevents them from impacting the RP.

Restrictions

- The ACL Support for Filtering IP Options feature can be used only with named, extended ACLs.
- Resource Reservation Protocol (RSVP) Multiprotocol Label Switching Traffic Engineering (MPLS TE), Internet Group Management Protocol Version 2 (IGMPV2), and other protocols that use IP Options packets may not function in drop or ignore mode if this feature is configured.
- On most Cisco routers, a packet with IP Options is not switched in hardware, but requires control plane software processing (primarily because there is a need to process the options and rewrite the IP header), so all IP packets with IP Options will be filtered and switched in software.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list extended** *access-list-name*
4. [*sequence-number*] **deny** *protocol source source-wildcard destination destination-wildcard* [**option** *option-value*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]
5. [*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* [**option** *option-value*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]
6. Repeat Step 4 or Step 5 as necessary.
7. **end**
8. **show ip access-lists** *access-list-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip access-list extended access-list-name Example: Router(config)# ip access-list extended mylist1	Specifies the IP access list by name and enters named access list configuration mode. Note The ACL Support for Filtering IP Options feature works only with named, extended ACLs.
Step 4	<pre>[sequence-number] deny protocol source source-wildcard destination destination-wildcard [option option-value] [precedence precedence] [tos tos] [log] [time-range time-range-name] [fragments]</pre> Example: Router(config-ext-nacl)# deny ip any any option traceroute	(Optional) Specifies a deny statement in named IP access list mode. <ul style="list-style-type: none"> This access list happens to use a deny statement first, but a permit statement could appear first, depending on the order of statements you need. Use the option keyword and <i>option-value</i> argument to filter packets that contain a particular IP Option. In this example, any packet that contains the traceroute IP Option will be filtered out. Use the no sequence-number form of this command to delete an entry.
Step 5	<pre>[sequence-number] permit protocol source source-wildcard destination destination-wildcard [option option-value] [precedence precedence] [tos tos] [log] [time-range time-range-name] [fragments]</pre> Example: Router(config-ext-nacl)# permit ip any any option security	Specifies a permit statement in named IP access list mode. <ul style="list-style-type: none"> In this example, any packet (not already filtered) that contains the security IP Option will be permitted. Use the no sequence-number form of this command to delete an entry.
Step 6	Repeat Step 4 or Step 5 as necessary.	Allows you to revise the access list.
Step 7	end Example: Router(config-ext-nacl)# end	(Optional) Exits the configuration mode and returns to privileged EXEC mode.
Step 8	show ip access-lists access-list-name Example: Router# show ip access-lists mylist1	(Optional) Displays the contents of the IP access list. <ul style="list-style-type: none"> Review the output to verify that the access list includes the new entry.

What to Do Next

Apply the access list to an interface or reference it from a command that accepts an access list.



Note

To effectively eliminate all packets that contain IP Options, we recommend that you configure the global **ip options drop** command.

Filtering Packets That Contain TCP Flags

The task in this section configures an access list to filter packets that contain TCP flags and verifies that the access list has been configured correctly.

Benefits of Filtering on TCP Flags

The ACL TCP Flags Filtering feature provides a flexible mechanism for filtering on TCP flags. Before Cisco IOS Release 12.3(4)T, an incoming packet was matched as long as any TCP flag in the packet matched a flag specified in the access control entry (ACE). This behavior allows for a security loophole, because packets with all flags set could get past the access control list (ACL). The ACL TCP Flags Filtering feature allows you to select any combination of flags on which to filter. The ability to match on a flag set and on a flag not set gives you a greater degree of control for filtering on TCP flags, thus enhancing security.

Because TCP packets can be sent as false synchronization packets that can be accepted by a listening port, it is recommended that administrators of firewall devices set up some filtering rules to drop false TCP packets.

The ACEs that make up an access list can be configured to detect and drop unauthorized TCP packets by allowing only the packets that have a very specific group of TCP flags set or not set. The ACL TCP Flags Filtering feature gives users a greater degree of packet-filtering control in the following ways:

- Users can select any desired combination of TCP flags on which to filter TCP packets.
- Users can configure ACEs in order to allow matching on a flag that is set, as well as on a flag that is not set.

TCP Flags

[Table 1](#) lists the TCP flags, which are further described in RFC 793, *Transmission Control Protocol*.

Table 1 TCP Flags

TCP Flag	Purpose
ACK	Acknowledge flag—Indicates that the acknowledgment field of a segment specifies the next sequence number the sender of this segment is expecting to receive.
FIN	Finish flag—Used to clear connections.
PSH	Push flag— Indicates the data in the call should be immediately pushed through to the receiving user.
RST	Reset flag—Indicates that the receiver should delete the connection without further interaction.

Table 1 *TCP Flags (continued)*

TCP Flag	Purpose
SYN	Synchronize flag—Used to establish connections.
URG	Urgent flag—Indicates that the urgent field is meaningful and must be added to the segment sequence number.

Restrictions

- TCP flag filtering can be used only with named, extended ACLs.
- The ACL TCP Flags Filtering feature is supported only for Cisco IOS ACLs.
- Before Cisco IOS Release 12.3(4)T, the following command-line interface (CLI) format could be used to configure a TCP flag-checking mechanism:

permit tcp any any rst

The following format that represents the same ACE can be used with Cisco IOS Release 12.3(4)T and later releases:

permit tcp any any match-any +rst

Both the CLI formats are accepted; however, if the new keywords **match-all** or **match-any** are chosen, they must be followed by the new flags that are prefixed with “+” or “-”. It is advisable to use only the old format or the new format in a single ACL. You cannot mix and match the old and new CLI formats.



Caution

If a router having ACEs with the new syntax format is reloaded with an older version of Cisco IOS software that does not support the ACL TCP Flags Filtering feature, the ACEs will not be applied, leading to possible security loopholes.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list extended *access-list-name***
4. *[sequence-number] permit tcp source source-wildcard [operator [port]] destination destination-wildcard [operator [port]] [established | {match-any | match-all} {+ | -} flag-name] [precedence precedence] [tos tos] [log] [time-range time-range-name] [fragments]*
5. *[sequence-number] deny tcp source source-wildcard [operator [port]] destination destination-wildcard [operator [port]] [established | {match-any | match-all} {+ | -} flag-name] [precedence precedence] [tos tos] [log] [time-range time-range-name] [fragments]*
6. Repeat Step 4 or Step 5 as necessary, adding statements by sequence number where you planned. Use the **no sequence-number** command to delete an entry.
7. **end**
8. **show ip access-lists *access-list-name***

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>ip access-list extended access-list-name</p> <p>Example: Router(config)# ip access-list extended kmd1</p>	<p>Specifies the IP access list by name and enters named access list configuration mode.</p> <p>Note The ACL TCP Flags Filtering feature works only with named, extended ACLs.</p>
Step 4	<p>[sequence-number] permit tcp source source-wildcard [operator [port]] destination destination-wildcard [operator [port]] [established {match-any match-all} {+ -} flag-name] [precedence precedence] [tos tos] [log] [time-range time-range-name] [fragments]</p> <p>Example: Router(config-ext-nacl)# permit tcp any any match-any +rst</p>	<p>Specifies a permit statement in named IP access list mode.</p> <ul style="list-style-type: none"> This access list happens to use a permit statement first, but a deny statement could appear first, depending on the order of statements you need. Use the TCP command syntax of the permit command. Any packet with the RST TCP header flag set will be matched and allowed to pass the named access list kmd1 in Step 3.
Step 5	<p>[sequence-number] deny tcp source source-wildcard [operator [port]] destination destination-wildcard [operator [port]] [established {match-any match-all} {+ -} flag-name] [precedence precedence] [tos tos] [log] [time-range time-range-name] [fragments]</p> <p>Example: Router(config-ext-nacl)# deny tcp any any match-all -ack -fin</p>	<p>(Optional) Specifies a deny statement in named IP access list mode.</p> <ul style="list-style-type: none"> This access list happens to use a permit statement first, but a deny statement could appear first, depending on the order of statements you need. Use the TCP command syntax of the deny command. Any packet that does not have the ACK flag set, and also does not have the FIN flag set, will not be allowed to pass the named access list kmd1 in Step 3. See the deny (IP) command for additional command syntax to permit upper-layer protocols (ICMP, IGMP, TCP, and UDP).
Step 6	<p>Repeat Step 4 or Step 5 as necessary, adding statements by sequence number where you planned. Use the no sequence-number command to delete an entry.</p>	<p>Allows you to revise the access list.</p>

	Command or Action	Purpose
Step 7	end Example: Router(config-ext-nacl)# end	(Optional) Exits the configuration mode and returns to privileged EXEC mode.
Step 8	show ip access-lists <i>access-list-name</i> Example: Router# show ip access-lists kmd1	(Optional) Displays the contents of the IP access list. <ul style="list-style-type: none"> Review the output to confirm that the access list includes the new entry.

What to Do Next

Apply the access list to an interface or reference it from a command that accepts an access list.

Configuring an Access Control Entry with Noncontiguous Ports

Perform this task to create access list entries that use noncontiguous TCP or UDP port numbers. Although this task uses TCP ports, you could use the UDP syntax of the **permit** and **deny** commands to filter noncontiguous UDP ports.

Although this task uses a **permit** command first, use the **permit** and **deny** commands in the order that achieves your filtering goals.

Benefits of Using the ACL—Named ACL Support for Noncontiguous Ports on an Access Control Entry Feature

This feature greatly reduces the number of ACEs required in an access control list to handle multiple entries for the same source address, destination address, and protocol. If you maintain large numbers of ACEs, we recommend that you use this feature to consolidate existing groups of access list entries wherever it is possible and also when you create new access list entries. When you configure access list entries with noncontiguous ports, you will have fewer access list entries to maintain.

Restrictions

The ACL—Named ACL Support for Noncontiguous Ports on an Access Control Entry feature can be used only with named, extended ACLs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list extended** *access-list-name*
4. [*sequence-number*] **permit tcp** *source source-wildcard* [*operator port* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established** | {**match-any** | **match-all**} {+ | -} *flag-name*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

5. `[sequence-number] deny tcp source source-wildcard [operator port [port]] destination destination-wildcard [operator [port]] [established | {match-any | match-all} {+ | -} flag-name] [precedence precedence] [tos tos] [log] [time-range time-range-name] [fragments]`
6. Repeat Step 4 or Step 5 as necessary, adding statements by sequence number where you planned. Use the `no sequence-number` command to delete an entry.
7. `end`
8. `show ip access-lists access-list-name`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p><code>configure terminal</code></p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><code>ip access-list extended access-list-name</code></p> <p>Example: Router(config)# ip access-list extended kmd1</p>	<p>Specifies the IP access list by name and enters named access list configuration mode.</p>
Step 4	<p><code>[sequence-number] permit tcp source source-wildcard [operator port [port]] destination destination-wildcard [operator [port]] [established {match-any match-all} {+ -} flag-name] [precedence precedence] [tos tos] [log] [time-range time-range-name] [fragments]</code></p> <p>Example: Router(config-ext-nacl)# permit tcp any eq telnet ftp any eq 450 679</p>	<p>Specifies a permit statement in named IP access list configuration mode.</p> <ul style="list-style-type: none"> Operators include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range). If the operator is positioned after the source and source-wildcard arguments, it must match the source port. If the operator is positioned after the destination and destination-wildcard arguments, it must match the destination port. The range operator requires two port numbers. You can configure up to 10 ports after the eq and neq operators. All other operators require one port number. To filter UDP ports, use the UDP syntax of this command.

	Command or Action	Purpose
Step 5	<pre>[sequence-number] deny tcp source source-wildcard [operator port [port]] destination destination-wildcard [operator [port]] [established {match-any match-all} {+ -} flag-name] [precedence precedence] [tos tos] [log] [time-range time-range-name] [fragments]</pre> <p>Example: Router(config-ext-nacl)# deny tcp any neq 45 565 632</p>	<p>(Optional) Specifies a deny statement in named access list configuration mode.</p> <ul style="list-style-type: none"> Operators include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range). If the <i>operator</i> is positioned after the <i>source</i> and <i>source-wildcard</i> arguments, it must match the source port. If the <i>operator</i> is positioned after the <i>destination</i> and <i>destination-wildcard</i> arguments, it must match the destination port. The range operator requires two port numbers. You can configure up to 10 ports after the eq and neq operators. All other operators require one port number. To filter UDP ports, use the UDP syntax of this command.
Step 6	Repeat Step 4 or Step 5 as necessary, adding statements by sequence number where you planned. Use the no sequence-number command to delete an entry.	Allows you to revise the access list.
Step 7	<p>end</p> <p>Example: Router(config-ext-nacl)# end</p>	(Optional) Exits named access list configuration mode and returns to privileged EXEC mode.
Step 8	<pre>show ip access-lists access-list-name</pre> <p>Example: Router# show ip access-lists kmd1</p>	<p>(Optional) Displays the contents of the access list.</p> <ul style="list-style-type: none"> Review the output to verify that the access list displays the new entries that you created.

Consolidating Access List Entries with Noncontiguous Ports into One Access List Entry

Perform this task to consolidate a group of access list entries with noncontiguous ports into one access list entry.

Although this task uses TCP ports, you could use the UDP syntax of the **permit** and **deny** commands to filter noncontiguous UDP ports.

Although this task uses a **permit** command first, use the **permit** and **deny** commands in the order that achieves your filtering goals.

SUMMARY STEPS

1. **enable**
2. **show ip access-lists access-list-name**
3. **configure terminal**
4. **ip access-list extended access-list-name**

5. **no** *[sequence-number]* **permit** *protocol source source-wildcard destination destination-wildcard* **[option option-name]** **[precedence precedence]** **[tos tos]** **[log]** **[time-range time-range-name]** **[fragments]**
6. *[sequence-number]* **permit** *protocol source source-wildcard [operator port [port]] destination destination-wildcard [operator port [port]]* **[option option-name]** **[precedence precedence]** **[tos tos]** **[log]** **[time-range time-range-name]** **[fragments]**
7. Repeat Steps 5 and 6 as necessary, adding **permit** or **deny** statements to consolidate access list entries where possible. Use the **no sequence-number** command to delete an entry.
8. **end**
9. **show ip access-lists** *access-list-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show ip access-lists <i>access-list-name</i> Example: Router# show ip access-lists mylist1	(Optional) Displays the contents of the IP access list. <ul style="list-style-type: none"> Review the output to see if you can consolidate any access list entries.
Step 3	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 4	ip access-list extended <i>access-list-name</i> Example: Router(config)# ip access-list extended mylist1	Specifies the IP access list by name and enters named access list configuration mode.
Step 5	no <i>[sequence-number]</i> permit <i>protocol source source-wildcard destination destination-wildcard</i> [option option-name] [precedence precedence] [tos tos] [log] [time-range time-range-name] [fragments] Example: Router(config-ext-nacl)# no 10	Removes the redundant access list entry that can be consolidated. <ul style="list-style-type: none"> Repeat this step to remove entries to be consolidated because only the port numbers differ. After this step is repeated to remove the access list entries 20, 30, and 40, for example, those entries are removed because they will be consolidated into one permit statement. If a <i>sequence-number</i> is specified, the rest of the command syntax is optional.

	Command or Action	Purpose
Step 6	<pre>[sequence-number] permit protocol source source-wildcard [operator port [port]] destination destination-wildcard [operator port [port]] [option option-name] [precedence precedence] [tos tos] [log] [time-range time-range-name] [fragments]</pre> <p>Example: Router(config-ext-nacl)# permit tcp any neq 45 565 632 any eq 23 45 34 43</p>	<p>Specifies a permit statement in named access list configuration mode.</p> <ul style="list-style-type: none"> In this instance, a group of access list entries with noncontiguous ports was consolidated into one permit statement. You can configure up to 10 ports after the eq and neq operators.
Step 7	Repeat Steps 5 and 6 as necessary, adding permit or deny statements to consolidate access list entries where possible. Use the no sequence-number command to delete an entry.	Allows you to revise the access list.
Step 8	<p>end</p> <p>Example: Router(config-std-nacl)# end</p>	(Optional) Exits named access list configuration mode and returns to privileged EXEC mode.
Step 9	<p>show ip access-lists access-list-name</p> <p>Example: Router# show ip access-lists mylist1</p>	<p>(Optional) Displays the contents of the access list.</p> <ul style="list-style-type: none"> Review the output to verify that the redundant access list entries have been replaced with your new consolidated entries.

What To Do Next

Apply the access list to an interface or reference it from a command that accepts an access list.

Filtering Packets Based on TTL Value

Because access lists are very flexible, it is not possible to define only one combination of **permit** and **deny** commands to filter packets based on the TTL value. This task illustrates just one example that achieves TTL filtering. Configure the appropriate **permit** and **deny** statements that will accomplish your filtering plan.

How Filtering on TTL Works

IP extended named and numbered access lists may filter on the TTL value of packets arriving at or leaving an interface. Packets with any possible TTL values 0 through 255 may be permitted or denied (filtered). Like filtering on other fields, such as source or destination address, the **ip access-group** command specifies **in** or **out**, which makes the access list ingress or egress and applies it to incoming or outgoing packets, respectively. The TTL value is checked in conjunction with the specified protocol, application, and any other settings in the access list entry, and all conditions must be met.

Special Handling for Packets with TTL of 0 or 1 Arriving on Ingress Interface

The software switching paths—distributed Cisco Express Forwarding (dCEF), CEF, fast switching, and process switching—will usually permit or discard the packets based on the access list statements. However, when the TTL value of packets arriving on an *ingress* interface have a TTL of 0 or 1, special

handling is required. The packets with a TTL of 0 or 1 get sent to the process level before the ingress access list is checked in CEF, dCEF, or fast switching paths. The ingress access list is applied to packets with TTL values 2 through 255 and a permit or deny decision is made.

Packets with a TTL value of 0 or 1 are sent to the process level because they will never be forwarded out of the device; the process level must check whether each packet is destined for the router or not and whether an Internet Control Message Protocol (ICMP) TTL Expire message needs to be sent back or not. This means that even if an ACL with TTL value 0 or 1 filtering is configured on the ingress interface with the intention to drop packets with a TTL of 0 or 1, the dropping of the packets will not happen in the faster paths. It will instead happen in the process level when the process applies the ACL. This is also true for hardware switching platforms. Packets with TTL 0 or 1 are sent to the process level of the route processor (RP) or Multilayer Switch Feature Card (MSFC).

On egress interfaces, access list filtering on TTL work just like other access list features. The check will happen in the fastest switching path enabled in the device. This is because the faster switching paths handle all the TTL values (0-255) equally on the egress interface.

Control Plane Policing for Filtering TTL Values 0 and 1

The special behavior for packets with a TTL of 0 or 1 results in higher CPU usage for the device. If you are filtering on TTL value 0 or 1, you should use control plane policing (CPP) to protect the CPU from being overwhelmed. In order to leverage CPP, you must configure an access list especially for filtering TTL values 0 and 1 and apply the access list through CPP. This access list will be a separate access list from any interface access lists. Because CPP works for the entire system, not just on individual interfaces, you would need to configure only one such special access list for the entire device. This task is described in the section [“Enabling Control Plane Policing to Filter on TTL Values 0 and 1”](#) section on page 15.

Benefits of Filtering on TTL

- Filtering on TTL provides a way to control which packets are allowed to reach the router or prevented from reaching the router. By looking at your network layout, you can choose whether to accept or deny packets from a certain router based on how many hops away it is. For example, in a small network, you can deny packets from a location more than three hops away. Filtering on TTL allows you to validate if the traffic originated from a neighboring device, as follows. You can accept only packets that reach you in one hop, for example, by accepting only packets with a TTL of one less than the initial TTL value of a particular protocol.
- Many control plane protocols communicate only with their neighbors, but receive packets from everyone. By applying to receiving routers an access list that filters on TTL, you can block unwanted packets.
- The Cisco IOS software sends all packets with a TTL of 0 or 1 to the process level to be processed. The device must then send an ICMP TTL expire message to the source. By filtering packets that have a TTL of 0 through 2, you can reduce the load on the process level.

Restrictions

- When the access list specifies the operation EQ or NEQ, routers running Cisco IOS Release 12.2S can have that access list specify up to ten TTL values. However, for Release 12.0S, only one TTL value can be specified.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **ip access-list extended** *access-list-name*
4. [*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**log**] [**time-range** *time-range-name*] [**fragments**]
5. Continue to add **permit** or **deny** statements to achieve the filtering you want.
6. **exit**
7. **interface** *type number*
8. **ip access-group** *access-list-name* {**in** | **out**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip access-list extended <i>access-list-name</i> Example: Router(config)# ip access-list extended ttlfilter	Defines an IP access list by name. <ul style="list-style-type: none">An access list that filters on TTL value must be an extended access list.
Step 4	[<i>sequence-number</i>] permit <i>protocol source source-wildcard destination destination-wildcard</i> [option <i>option-name</i>] [precedence <i>precedence</i>] [tos <i>tos</i>] [ttl <i>operator value</i>] [log] [time-range <i>time-range-name</i>] [fragments] Example: Router(config-ext-nacl)# permit ip host 172.16.1.1 any ttl lt 2	Sets conditions to allow a packet to pass a named IP access list. <ul style="list-style-type: none">Every access list must have at least one permit statement.This example permits packets from source 172.16.1.1 to any destination with a TTL value less than 2.
Step 5	Continue to add permit or deny statements to achieve the filtering you want.	—
Step 6	exit Example: Router(config-ext-nacl)# exit	Exits any configuration mode to the next highest mode in the CLI mode hierarchy.

	Command or Action	Purpose
Step 7	<code>interface type number</code> Example: Router(config)# interface ethernet 0	Configures an interface type and enters interface configuration mode.
Step 8	<code>ip access-group access-list-name {in out}</code> Example: Router(config-if)# ip access-group ttlfilter in	Applies the access list to an interface.

Enabling Control Plane Policing to Filter on TTL Values 0 and 1

Perform this task if you want to filter IP packets based on a TTL value of 0 or 1 and you want to protect the CPU from being overwhelmed. This task configures an access list for classification on TTL 0 and 1, configures Modular QoS CLI (MQC), and applies the policy map to the control plane. Any packets that pass the access list are dropped. This special access list is separate from any interface access lists.

Because access lists are very flexible, it is not possible to define only one combination of **permit** and **deny** commands to filter packets based on the TTL value. This task illustrates just one example that achieves TTL filtering. Configure the appropriate **permit** and **deny** statements that will accomplish your filtering plan.

SUMMARY STEPS

- `enable`
- `configure terminal`
- `ip access-list extended access-list-name`
- `[sequence-number] permit protocol source source-wildcard destination destination-wildcard ttl operator value`
- Continue to add **permit** or **deny** statements to achieve the filtering you want.
- `exit`
- `class-map class-map-name [match-all | match-any]`
- `match access-group {access-group | name access-group-name}`
- `exit`
- `policy-map policy-map-name`
- `class {class-name | class-default}`
- `drop`
- `exit`
- `exit`
- `control-plane`
- `service-policy {input | output} policy-map-name`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip access-list extended <i>access-list-name</i> Example: Router(config)# ip access-list extended ttlfilter	Defines an IP access list by name. <ul style="list-style-type: none">An access list that filters on a TTL value must be an extended access list.
Step 4	[<i>sequence-number</i>] permit <i>protocol source source-wildcard destination destination-wildcard</i> ttl <i>operator value</i> Example: Router(config-ext-nacl)# permit ip host 172.16.1.1 any ttl lt 2	Sets conditions to allow a packet to pass a named IP access list. <ul style="list-style-type: none">Every access list must have at least one permit statement.This example permits packets from source 172.16.1.1 to any destination with a TTL value less than 2.
Step 5	Continue to add permit or deny statements to achieve the filtering you want.	The packets that pass the access list will be dropped.
Step 6	exit Example: Router(config-ext-nacl)# exit	Exits any configuration mode to the next highest mode in the CLI mode hierarchy.
Step 7	class-map <i>class-map-name</i> [match-all match-any] Example: Router(config)# class-map acl-filtering	Creates a class map to be used for matching packets to a specified class.
Step 8	match access-group { <i>access-group</i> name <i>access-group-name</i> } Example: Router(config-cmap)# match access-group name ttlfilter	Configures the match criteria for a class map on the basis of the specified access control list.
Step 9	exit Example: Router(config-cmap)# exit	Exits any configuration mode to the next highest mode in the CLI mode hierarchy.

	Command or Action	Purpose
Step 10	policy-map <i>policy-map-name</i> Example: Router(config)# policy-map acl-filter	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
Step 11	class { <i>class-name</i> class-default } Example: Router(config-pmap)# class acl-filter-class	Specifies the name of the class whose policy you want to create or change or to specify the default class (commonly known as the class-default class) before you configure its policy.
Step 12	drop Example: Router(config-pmap-c)# drop	Configures a traffic class to discard packets belonging to a specific class.
Step 13	exit Example: Router(config-pmap-c)# exit	Exits any configuration mode to the next highest mode in the CLI mode hierarchy.
Step 14	exit Example: Router(config-pmap)# exit	Exits any configuration mode to the next highest mode in the CLI mode hierarchy.
Step 15	control-plane Example: Router(config)# control-plane	Associates or modifies attributes or parameters that are associated with the control plane of the device.
Step 16	service-policy { input output } <i>policy-map-name</i> Example: Router(config-cp)# service-policy input acl-filter	Attaches a policy map to a control plane for aggregate control plane services.

Configuration Examples for Filtering IP Options, TCP Flags, Noncontiguous Ports, and TTL Values

This section provides the following configuration examples:

- [Filtering Packets That Contain IP Options: Example, page 18](#)
- [Filtering Packets That Contain TCP Flags: Example, page 18](#)
- [Creating an Access List Entry with Noncontiguous Ports: Example, page 18](#)
- [Consolidating Some Existing Access List Entries into One Access List Entry with Noncontiguous Ports: Example, page 19](#)
- [Filtering on TTL Value: Example, page 19](#)
- [Control Plane Policing to Filter on TTL Values 0 and 1: Example, page 20](#)

Filtering Packets That Contain IP Options: Example

The following example shows an extended access list named `mylist2` that contains access list entries (ACEs) that are configured to permit TCP packets only if they contain the IP Options that are specified in the ACEs:

```
ip access-list extended mylist2
 10 permit ip any any option eool
 20 permit ip any any option record-route
 30 permit ip any any option zsu
 40 permit ip any any option mtup
```

The **show access-list** command has been entered to show how many packets were matched and therefore permitted:

```
Router# show ip access-list mylist2

Extended IP access list test
10 permit ip any any option eool (1 match)
20 permit ip any any option record-route (1 match)
30 permit ip any any option zsu (1 match)
40 permit ip any any option mtup (1 match)
```

Filtering Packets That Contain TCP Flags: Example

The following access list allows TCP packets only if the TCP flags ACK and SYN are set and the FIN flag is not set:

```
ip access-list extended aaa
 permit tcp any any match-all +ack +syn -fin
end
```

The **show access-list** command has been entered to display the ACL:

```
Router# show access-list aaa

Extended IP access list aaa
 10 permit tcp any any match-all +ack +syn -fin
```

Creating an Access List Entry with Noncontiguous Ports: Example

The following access list entry can be created because up to ten ports can be entered after the **eq** and **neq** operators:

```
ip access-list extended aaa
 permit tcp any eq telnet ftp any eq 23 45 34
end
```

Enter the **show access-lists** command to display the newly created access list entry.

```
Router# show access-lists aaa

Extended IP access list aaa
 10 permit tcp any eq telnet ftp any eq 23 45 34
```

Consolidating Some Existing Access List Entries into One Access List Entry with Noncontiguous Ports: Example

The **show access-lists** command is used to display a group of access list entries for the access list named abc:

```
Router# show access-lists abc
```

```
Extended IP access list abc
 10 permit tcp any eq telnet any eq 450
 20 permit tcp any eq telnet any eq 679
 30 permit tcp any eq ftp any eq 450
 40 permit tcp any eq ftp any eq 679
```

Because the entries are all for the same **permit** statement and simply show different ports, they can be consolidated into one new access list entry. The following example shows the removal of the redundant access list entries and the creation of a new access list entry that consolidates the previously displayed group of access list entries:

```
ip access-list extended abc
 no 10
 no 20
 no 30
 no 40
 permit tcp any eq telnet ftp any eq 450 679
end
```

When the **show access-lists** command is reentered, the consolidated access list entry is displayed:

```
Router# show access-lists abc
```

```
Extended IP access list abc
 10 permit tcp any eq telnet ftp any eq 450 679
```

Filtering on TTL Value: Example

The following access list filters IP packets containing type of service (ToS) level 3 with TTL values 10 and 20. It also filters IP packets with a TTL greater than 154 and applies that rule to noninitial fragments. It permits IP packets with a precedence level of flash and a TTL not equal to 1, and it sends log messages about such packets to the console. All other packets are denied.

```
ip access-list extended incomingfilter
 deny ip any any tos 3 ttl eq 10 20
 deny ip any any ttl gt 154 fragments
 permit ip any any precedence flash ttl neq 1 log
!
interface ethernet 0
ip access-group incomingfilter in
```

Control Plane Policing to Filter on TTL Values 0 and 1: Example

The following example configures a traffic class called `acl-filter-class` for use in a policy map called `acl-filter`. An access list permits IP packets from any source having a TTL of 0 or 1. Any packets matching the access list are dropped. The policy map is attached to the control plane.

```
ip access-list extended ttlfilter
  permit ip any any ttl eq 0 1
class-map acl-filter-class
  match access-group name ttlfilter
policy-map acl-filter
  class acl-filter-class
    drop
control-plane
  service-policy input acl-filter
```

Additional References

The following sections provide references related to IP access list filtering described in this module.

Related Documents

Related Topic	Document Title
Configuring the router to drop or ignore packets containing IP Options by using the no ip options command.	“IP Options Selective Drop” module in <i>Cisco IOS IP Application Services</i> , Release 12.3(4)T.
QoS commands	<i>Cisco IOS Quality of Service Solutions Command Reference</i> , Release 12.4

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 791	Internet Protocol http://www.faqs.org/rfcs/rfc791.html
RFC 793	<i>Transmission Control Protocol</i>
RFC 1393	<i>Traceroute Using an IP Option</i>

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Using an IP Access List to Filter Packets

Table 2 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for a specific command was introduced, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 2 *Feature Information for Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values*

Feature Name	Releases	Feature Configuration Information
ACL Support for Filtering IP Options	12.3(4)T 12.2(25)S	This feature allows you to filter packets having IP Options, in order to prevent routers from becoming saturated with spurious packets. See the following sections: <ul style="list-style-type: none"> • Filtering Packets That Contain IP Options, page 2 • Filtering Packets That Contain IP Options: Example, page 18
ACL TCP Flags Filtering	12.3(4)T 12.2(25)S	This feature provides a flexible mechanism for filtering on TCP flags. Before Cisco IOS Release 12.3(4)T, an incoming packet was matched as long as any TCP flag in the packet matched a flag specified in the access control entry (ACE). This behavior allows for a security loophole, because packets with all flags set could get past the access control list (ACL). The ACL TCP Flags Filtering feature allows you to select any combination of flags on which to filter. The ability to match on a flag set and on a flag not set gives you a greater degree of control for filtering on TCP flags, thus enhancing security. See the following sections: <ul style="list-style-type: none"> • Filtering Packets That Contain TCP Flags, page 5 • Filtering Packets That Contain TCP Flags: Example, page 18
ACL—Named ACL Support for Noncontiguous Ports on an Access Control Entry	12.3(7)T 12.2(25)S	This feature allows you to specify noncontiguous ports in a single access control entry, which greatly reduces the number of entries required in an access control list when several entries have the same source address, destination address, and protocol, but differ only in the ports. See the following sections: <ul style="list-style-type: none"> • Configuring an Access Control Entry with Noncontiguous Ports, page 8 • Consolidating Access List Entries with Noncontiguous Ports into One Access List Entry, page 10 • Creating an Access List Entry with Noncontiguous Ports: Example, page 18 • Consolidating Some Existing Access List Entries into One Access List Entry with Noncontiguous Ports: Example, page 19

Table 2 **Feature Information for Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values (continued)**

Feature Name	Releases	Feature Configuration Information
ACL Support for Filtering on TTL Value	12.4(2)T	<p>Customers may use extended IP access lists (named or numbered) to filter packets based on their time-to-live (TTL) value, from 0 to 255. This filtering enhances a customer's control over which packets reach a router. See the following sections:</p> <ul style="list-style-type: none"> • Filtering Packets Based on TTL Value, page 12 • Enabling Control Plane Policing to Filter on TTL Values 0 and 1, page 15 • Filtering on TTL Value: Example, page 19 • Control Plane Policing to Filter on TTL Values 0 and 1: Example, page 20
ACL - Named ACL Support for Noncontiguous Ports on an Access Control Entry	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
ACL - TCP Flags Filtering	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
ACL Support for Filtering IP Options	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
Selective Drop/ Ignore of IP Options	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Refining an IP Access List

First Published: August 18, 2006
Last Updated: August 18, 2006

There are several ways to refine an access list while or after you create it. You can change the order of the entries in an access list or add entries to an access list. You can restrict access list entries to a certain time of day or week, or achieve finer granularity when filtering packets by filtering noninitial fragments of packets.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Refining an IP Access List”](#) section on page 19.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Refining an IP Access List, page 1](#)
- [Information About Refining an IP Access List, page 2](#)
- [How to Refine an IP Access List, page 2](#)
- [Configuration Examples for Refining an IP Access List, page 16](#)
- [Additional References, page 18](#)

Prerequisites for Refining an IP Access List

Before you perform any of the tasks in this module, you should be familiar with the concepts in the “IP Access List Overview” module.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Information About Refining an IP Access List

You should understand the following concept before configuring an IP access list with sequence numbers:

- [Access List Sequence Numbers, page 2](#)

Access List Sequence Numbers

The ability to apply sequence numbers to IP access list entries simplifies access list changes. Prior to the IP Access List Entry Sequence Numbering feature, there was no way to specify the position of an entry within an access list. If you wanted to insert an entry in the middle of an existing list, all of the entries after the desired position had to be removed, then the new entry was added, and then all the removed entries had to be reentered. This method was cumbersome and error prone.

Sequence numbers allow users to add access list entries and resequence them. When you add a new entry, you specify the sequence number so that it is in a desired position in the access list. If necessary, entries currently in the access list can be resequenced to create room to insert the new entry.

How to Refine an IP Access List

The tasks in this module provide you with various ways to refine an access list if you did not already do so while you were creating it. You can change the order of the entries in an access list, add entries to an access list, restrict access list entries to a certain time of day or week, or achieve finer granularity when filtering packets by filtering on noninitial fragments of packets.

This section includes the following tasks:

- [Revising an Access List Using Sequence Numbers, page 2](#) (optional)
- [Restricting an Access List Entry to a Time of Day or Week, page 6](#) (optional)
- [Filtering Noninitial Fragments of Packets, page 11](#) (optional)

Revising an Access List Using Sequence Numbers

Perform this task if you want to add entries to an existing access list, change the order of entries, or simply number the entries in an access list to accommodate future changes.



Note

Remember that if you want to delete an entry from an access list, you can simply use the **no deny** or **no permit** form of the command, or the **no sequence-number** command if the statement already has a sequence number.

Benefits of Access List Sequence Numbers

An access list sequence number is a number at the beginning of a **permit** or **deny** command in an access list. The sequence number determines the order that the entry appears in the access list. The ability to apply sequence numbers to IP access list entries simplifies access list changes.

Prior to having sequence numbers, users could only add access list entries to the end of an access list; therefore, needing to add statements anywhere except the end of the list required reconfiguring the entire access list. There was no way to specify the position of an entry within an access list. If a user wanted to insert an entry (statement) in the middle of an existing list, all of the entries after the desired position had to be removed, then the new entry was added, and then all the removed entries had to be reentered. This method was cumbersome and error prone.

This feature allows users to add sequence numbers to access list entries and resequence them. When a user adds a new entry, the user chooses the sequence number so that it is in a desired position in the access list. If necessary, entries currently in the access list can be resequenced to create room to insert the new entry. Sequence numbers make revising an access list much easier.

Sequence Numbering Behavior

- For backward compatibility with previous releases, if entries with no sequence numbers are applied, the first entry is assigned a sequence number of 10, and successive entries are incremented by 10. The maximum sequence number is 2147483647. If the generated sequence number exceeds this maximum number, the following message is displayed:

`Exceeded maximum sequence number.`

- If the user enters an entry without a sequence number, it is assigned a sequence number that is 10 greater than the last sequence number in that access list and is placed at the end of the list.
- If the user enters an entry that matches an already existing entry (except for the sequence number), then no changes are made.
- If the user enters a sequence number that is already present, the following error message is generated:
`Duplicate sequence number.`
- If a new access list is entered from global configuration mode, then sequence numbers for that access list are generated automatically.
- Distributed support is provided so that the sequence numbers of entries in the Route Processor (RP) and line card are in synchronization at all times.
- Sequence numbers are not nvgened. That is, the sequence numbers themselves are not saved. In the event that the system is reloaded, the configured sequence numbers revert to the default sequence starting number and increment. The function is provided for backward compatibility with software releases that do not support sequence numbering.
- This feature works with named and numbered, standard and extended IP access lists.

Restrictions

- Access list sequence numbers do not support dynamic, reflexive, or firewall access lists.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list resequence** *access-list-name starting-sequence-number increment*
4. **ip access-list {standard | extended}** *access-list-name*
5. *sequence-number permit source source-wildcard*

or

sequence-number **permit** *protocol source source-wildcard destination destination-wildcard*
[**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

6. *sequence-number* **deny** *source source-wildcard*

or

sequence-number **deny** *protocol source source-wildcard destination destination-wildcard*
[**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

7. Repeat Step 5 and Step 6 as necessary, adding statements by sequence number where you planned. Use the **no** *sequence-number* command to delete an entry.
8. **end**
9. **show ip access-lists** *access-list-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip access-list resequence <i>access-list-name</i> <i>starting-sequence-number</i> <i>increment</i> Example: Router(config)# ip access-list resequence kmd1 100 15	Resequences the specified IP access list using the starting sequence number and the increment of sequence numbers. <ul style="list-style-type: none"> This example resequences an access list named kmd1. The starting sequence number is 100 and the increment is 15.
Step 4	ip access-list { standard extended } <i>access-list-name</i> Example: Router(config)# ip access-list standard xyz123	Specifies the IP access list by name and enters named access list configuration mode. <ul style="list-style-type: none"> If you specify standard, make sure you specify subsequent permit and deny statements using the standard access list syntax. If you specify extended, make sure you specify subsequent permit and deny statements using the extended access list syntax.
Step 5	<i>sequence-number</i> permit <i>source</i> <i>source-wildcard</i> or <i>sequence-number</i> permit <i>protocol</i> <i>source</i> <i>source-wildcard</i> <i>destination</i> <i>destination-wildcard</i> [precedence <i>precedence</i>] [tos <i>tos</i>] [log] [time-range <i>time-range-name</i>] [fragments] Example: Router(config-std-nacl)# 105 permit 10.5.5.5 0.0.0.255	Specifies a permit statement in named IP access list mode. <ul style="list-style-type: none"> This access list happens to use a permit statement first, but a deny statement could appear first, depending on the order of statements you need. See the permit (IP) command for additional command syntax to permit upper layer protocols (ICMP, IGMP, TCP, and UDP). Use the no <i>sequence-number</i> command to delete an entry. As the prompt indicates, this access list was a standard access list. If you had specified extended in Step 4, the prompt for this step would be Router(config-ext-nacl)# and you would use the extended permit command syntax.

	Command or Action	Purpose
Step 6	<p><code>sequence-number deny source source-wildcard</code></p> <p>or</p> <p><code>sequence-number deny protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [log] [time-range time-range-name] [fragments]</code></p> <p>Example: Router(config-std-nacl)# 110 deny 10.6.6.7 0.0.0.255</p>	<p>(Optional) Specifies a deny statement in named IP access list mode.</p> <ul style="list-style-type: none"> This access list happens to use a permit statement first, but a deny statement could appear first, depending on the order of statements you need. See the deny (IP) command for additional command syntax to permit upper layer protocols (ICMP, IGMP, TCP, and UDP). Use the no sequence-number command to delete an entry. As the prompt indicates, this access list was a standard access list. If you had specified extended in Step 4, the prompt for this step would be Router(config-ext-nacl)# and you would use the extended deny command syntax.
Step 7	Repeat Step 5 and Step 6 as necessary, adding statements by sequence number where you planned. Use the no sequence-number command to delete an entry.	Allows you to revise the access list.
Step 8	<p>end</p> <p>Example: Router(config-std-nacl)# end</p>	(Optional) Exits the configuration mode and returns to privileged EXEC mode.
Step 9	<p>show ip access-lists access-list-name</p> <p>Example: Router# show ip access-lists xyz123</p>	<p>(Optional) Displays the contents of the IP access list.</p> <ul style="list-style-type: none"> Review the output to see that the access list includes the new entry.

Examples

The following is sample output from the **show ip access-lists** command when the **xyz123** access list is specified.

```
Router# show ip access-lists xyz123

Standard IP access list xyz123
100 permit 10.4.4.0, wildcard bits 0.0.0.255
105 permit 10.5.5.5, wildcard bits 0.0.0.255
115 permit 10.0.0.0, wildcard bits 0.0.0.255
130 permit 10.5.5.0, wildcard bits 0.0.0.255
145 permit 10.0.0.0, wildcard bits 0.0.0.255
```

Restricting an Access List Entry to a Time of Day or Week

By default, access list statements are always in effect once they are applied. However, you can define the times of the day or week that **permit** or **deny** statements are in effect by defining a time range, and then referencing the time range by name in an individual access list statement. IP and Internetwork Packet Exchange (IPX) named or numbered extended access lists can use time ranges.

Benefits of Time Ranges

Benefits and possible uses of time ranges include the following:

- The network administrator has more control over permitting or denying a user access to resources. These resources could be an application (identified by an IP address/mask pair and a port number), policy routing, or an on-demand link (identified as interesting traffic to the dialer).
- Network administrators can set time-based security policy, including the following:
 - Perimeter security using the Cisco IOS Firewall feature set or access lists
 - Data confidentiality with Cisco Encryption Technology or IP Security Protocol (IPSec)
- Policy-based routing (PBR) and queueing functions are enhanced.
- When provider access rates vary by time of day, it is possible to automatically reroute traffic cost effectively.
- Service providers can dynamically change a committed access rate (CAR) configuration to support the quality of service (QoS) service level agreements (SLAs) that are negotiated for certain times of day.
- Network administrators can control logging messages. Access list entries can log traffic at certain times of the day, but not constantly. Therefore, administrators can simply deny access without needing to analyze many logs generated during peak hours.

Distributed Time-Based Access Lists

Before the introduction of the Distributed Time-Based Access Lists feature, time-based access lists were not supported on line cards for the Cisco 7500 series routers. If time-based access lists were configured, they behaved as normal access lists. If an interface on a line card were configured with a time-based access list, the packets switched into the interface were not distributed switched through the line card, but were forwarded to the Route Processor for processing.

The Distributed Time-Based Access Lists feature allows packets destined for an interface configured with a time-based access list to be distributed switched through the line card.

For this functionality to work, the software clock must remain synchronized between the Route Processor and the line card. This synchronization occurs through an exchange of interprocess communications (IPC) messages from the Route Processor to the line card. When a time range or a time-range entry is changed, added, or deleted, an IPC message is sent by the Route Processor to the line card.

There is no difference between how the user configures a time-based access list and a distributed time-based access list.

Prerequisites

The time range relies on the software clock of the routing device. For the time range feature to work the way you intend, you need a reliable clock source. We recommend that you use Network Time Protocol (NTP) to synchronize the software clock of the routing device.

Restrictions

The Distributed Time-Based Access Lists feature is supported on Cisco 7500 series routers with a Versatile Interface Processor (VIP) enabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **time-range** *time-range-name*
4. **periodic** *days-of-the-week hh:mm to [days-of-the-week] hh:mm*
5. Repeat Step 4 if you want more than one period of time applied to an access list statement.
6. **absolute** [*start time date*] [*end time date*]
7. **exit**
8. Repeat Steps 3 through 7 if you want different time ranges to apply to **permit** or **deny** statements.
9. **ip access-list extended** *name*
10. **deny** *protocol source [source-wildcard] destination [destination-wildcard] [option option-name] [precedence precedence] [tos tos] [established] [log | log-input] time-range time-range-name*
11. **permit** *protocol source [source-wildcard] destination [destination-wildcard] [option option-name] [precedence precedence] [tos tos] [established] [log | log-input] time-range time-range-name*
12. Optionally repeat some combination of Steps 10 and 11 until you have specified the values on which you want to base your access list.
13. **end**
14. **show ip access-list**
15. **show time-range**
16. **show time-range ipc**
17. **clear time-range ipc**
18. **debug time-range ipc**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	time-range <i>time-range-name</i> Example: Router(config)# time-range limit_http	Defines a time range and enters time-range configuration mode. <ul style="list-style-type: none"> The name cannot contain a space or quotation mark, and must begin with a letter. Multiple time ranges can occur in a single access list.
Step 4	periodic <i>days-of-the-week hh:mm to [days-of-the-week] hh:mm</i> Example: Router(config-time-range)# periodic Monday 6:00 to Wednesday 19:00	(Optional) Specifies a recurring (weekly) time range. <ul style="list-style-type: none"> The first occurrence of <i>days-of-the-week</i> is the starting day or day of the week that the associated time range is in effect. The second occurrence is the ending day or day of the week the associated statement is in effect. The <i>days-of-the-week</i> argument can be any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. Other possible values are: <ul style="list-style-type: none"> daily—Monday through Sunday weekdays—Monday through Friday weekend—Saturday and Sunday If the ending days of the week are the same as the starting days of the week, they can be omitted. The first occurrence of <i>hh:mm</i> is the starting hours:minutes that the associated time range is in effect. The second occurrence is the ending hours:minutes the associated statement is in effect. The hours:minutes are expressed in a 24-hour clock. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.
Step 5	Repeat Step 4 if you want more than one period of time applied to an access list statement.	(Optional) Multiple periodic commands are allowed in a time range.

	Command or Action	Purpose
Step 6	<p>absolute [start <i>time date</i>] [end <i>time date</i>]</p> <p>Example: Router(config-time-range)# absolute start 6:00 1 August 2005 end 18:00 31 October 2005</p>	<p>(Optional) Specifies an absolute time when a time range is in effect.</p> <ul style="list-style-type: none"> Only one absolute command is allowed in a time range. The time is expressed in 24-hour notation, in the form of hours:minutes. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m. The date is expressed in the format <i>day month year</i>. The minimum start is 00:00 1 January 1993. If no start time and date are specified, the permit or deny statement is in effect immediately. Absolute time and date that the permit or deny statement of the associated access list is no longer in effect. Same time and date format as described for the start keyword. The end time and date must be after the start time and date. The maximum end time is 23:59 31 December 2035. If no end time and date are specified, the associated permit or deny statement is in effect indefinitely.
Step 7	<p>exit</p> <p>Example: Router(config-time-range)# exit</p>	Exits to the next highest mode.
Step 8	Repeat Steps 3 through 7 if you want different time ranges to apply to permit or deny statements.	—
Step 9	<p>ip access-list extended <i>name</i></p> <p>Example: Router(config)# ip access-list extended autumn</p>	Defines an extended IP access list using a name and enters extended named access list configuration mode.
Step 10	<p>deny <i>protocol source</i> [<i>source-wildcard</i>] [<i>destination</i> [<i>destination-wildcard</i>] [option <i>option-name</i>] [precedence <i>precedence</i>] [tos <i>tos</i>] [established] [log log-input] time-range <i>time-range-name</i></p> <p>Example: Router(config-ext-nacl)# deny tcp 172.16.22.23 any eq http time-range limit_http</p>	<p>(Optional) Denies any packet that matches all of the conditions specified in the statement.</p> <ul style="list-style-type: none"> Specify the time range you created in Step 3. In this example, one host is denied HTTP access during the time defined by the time range called “limit_http.”
Step 11	<p>permit <i>protocol source</i> [<i>source-wildcard</i>] [<i>destination</i> [<i>destination-wildcard</i>] [option <i>option-name</i>] [precedence <i>precedence</i>] [tos <i>tos</i>] [established] [log log-input] time-range <i>time-range-name</i></p> <p>Example: Router(config-ext-nacl)# permit tcp any any eq http time-range limit_http</p>	<p>Permits any packet that matches all of the conditions specified in the statement.</p> <ul style="list-style-type: none"> You can specify the time range you created in Step 3 or in a different instance of Step 3, depending on whether you want the time ranges for your statements to be the same or different. In this example, all other sources are given access to HTTP during the time defined by the time range called “limit_http.”

	Command or Action	Purpose
Step 12	Optionally repeat some combination of Steps 10 and 11 until you have specified the values on which you want to base your access list.	—
Step 13	end Example: Router(config-ext-nacl)# end	Ends configuration mode and returns the system to privileged EXEC mode.
Step 14	show ip access-list Example: Router# show ip access-list	(Optional) Displays the contents of all current IP access lists.
Step 15	show time-range Example: Router# show time-range	(Optional) Displays the time ranges that are set.
Step 16	show time-range ipc Example: Router# show time-range ipc	(Optional) Displays the statistics about the time-range IPC messages between the Route Processor and line card on the Cisco 7500 series router.
Step 17	clear time-range ipc Example: Router# clear time-range ipc	(Optional) Clears the time-range IPC message statistics and counters between the Route Processor and line card on the Cisco 7500 series router.
Step 18	debug time-range ipc Example: Router# debug time-range ipc	(Optional) Enables debugging output for monitoring the time-range IPC messages between the Route Processor and line card on the Cisco 7500 series router.

What to Do Next

Apply the access list to an interface or reference it from a command that accepts an access list.

Filtering Noninitial Fragments of Packets

Filter noninitial fragments of packets with an extended access list if you want to block more of the traffic you intended to block, not just the initial fragment of such packets. You should first understand the following concepts.

Benefits of Filtering Noninitial Fragments of Packets

If the **fragments** keyword is used in additional IP access list entries that deny fragments, the fragment control feature provides the following benefits:

Additional Security

You are able to block more of the traffic you intended to block, not just the initial fragment of such packets. The unwanted fragments no longer linger at the receiver until the reassembly timeout is reached because they are blocked before being sent to the receiver. Blocking a greater portion of unwanted traffic improves security and reduces the risk from potential hackers.

Reduced Cost

By blocking unwanted noninitial fragments of packets, you are not paying for traffic you intended to block.

Reduced Storage

By blocking unwanted noninitial fragments of packets from ever reaching the receiver, that destination does not have to store the fragments until the reassembly timeout period is reached.

Expected Behavior Is Achieved

The noninitial fragments will be handled in the same way as the initial fragment, which is what you would expect. There are fewer unexpected policy routing results and fewer fragments of packets being routed when they should not be.

Access List Processing of Fragments

The behavior of access list entries regarding the use or lack of use of the **fragments** keyword can be summarized as follows:

If the Access-List Entry Has...	Then...
...no fragments keyword (the default), and assuming all of the access-list entry information matches,	<p>For an access list entry that contains only Layer 3 information:</p> <ul style="list-style-type: none"> The entry is applied to nonfragmented packets, initial fragments, and noninitial fragments. <p>For an access list entry that contains Layer 3 and Layer 4 information:</p> <ul style="list-style-type: none"> The entry is applied to nonfragmented packets and initial fragments. <ul style="list-style-type: none"> If the entry is a permit statement, then the packet or fragment is permitted. If the entry is a deny statement, then the packet or fragment is denied. The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access list entry can be applied. If the Layer 3 portion of the access list entry matches, and <ul style="list-style-type: none"> If the entry is a permit statement, then the noninitial fragment is permitted. If the entry is a deny statement, then the next access list entry is processed. <p>Note The deny statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.</p>
...the fragments keyword, and assuming all of the access-list entry information matches,	<p>The access list entry is applied only to noninitial fragments.</p> <p>The fragments keyword cannot be configured for an access list entry that contains any Layer 4 information.</p>

Be aware that you should not add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments** keyword. The packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases in which there are multiple **deny** entries for the same host but with different Layer 4 ports, a single **deny** access list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets, and each counts individually as a packet in access list accounting and access list violation counts.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list extended** *name*
4. *[sequence-number] deny protocol source [source-wildcard] [operator port [port]] destination [destination-wildcard][operator port [port]]*
5. *[sequence-number] deny protocol source [source-wildcard] [operator port [port]] destination [destination-wildcard] [operator port [port]] [fragments]*
6. *[sequence-number] permit protocol source [source-wildcard] [operator port [port]] destination [destination-wildcard] [operator port [port]]*
7. Repeat some combination of Steps 4 through 6 until you have specified the values on which you want to base your access list.
8. **end**
9. **show ip access-list**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip access-list extended name Example: Router(config)# ip access-list extended rstrct4	Defines an extended IP access list using a name and enters extended named access list configuration mode.
Step 4	[sequence-number] deny protocol source [source-wildcard] [operator port [port]] destination [destination-wildcard] [operator port [port]] Example: Router(config-ext-nacl)# deny ip any 172.20.1.1	(Optional) Denies any packet that matches all of the conditions specified in the statement. <ul style="list-style-type: none"> This statement will apply to nonfragmented packets and initial fragments.
Step 5	[sequence-number] deny protocol source [source-wildcard] [operator port [port]] destination [destination-wildcard] [operator port [port]] fragments Example: Router(config-ext-nacl)# deny ip any 172.20.1.1 fragments	(Optional) Denies any packet that matches all of the conditions specified in the statement <ul style="list-style-type: none"> This statement will apply to noninitial fragments.
Step 6	[sequence-number] permit protocol source [source-wildcard] [operator port [port]] destination [destination-wildcard] [operator port [port]] Example: Router(config-ext-nacl)# permit tcp any any	Permits any packet that matches all of the conditions specified in the statement. <ul style="list-style-type: none"> Every access list needs at least one permit statement. If the <i>source-wildcard</i> or <i>destination-wildcard</i> is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source or destination address, respectively. Optionally use the keyword any as a substitute for the <i>source source-wildcard</i> or <i>destination destination-wildcard</i> to specify the address and wildcard of 0.0.0.0 255.255.255.255.
Step 7	Repeat some combination of Steps 4 through 6 until you have specified the values on which you want to base your access list.	Remember that all sources not specifically permitted are denied by an implicit deny statement at the end of the access list.

	Command or Action	Purpose
Step 8	end Example: Router(config-ext-nacl)# end	Ends configuration mode and returns the system to privileged EXEC mode.
Step 9	show ip access-list Example: Router# show ip access-list	(Optional) Displays the contents of all current IP access lists.

What to Do Next

Apply the access list to an interface or reference it from a command that accepts an access list.

Configuration Examples for Refining an IP Access List

This section provides the following configuration examples:

- [Resequencing Entries in an Access List: Example, page 16](#)
- [Adding an Entry with a Sequence Number: Example, page 17](#)
- [Adding an Entry with No Sequence Number: Example, page 17](#)
- [Time Ranges Applied to IP Access List Entries: Example, page 18](#)
- [Filtering IP Packet Fragments: Example, page 18](#)

Resequencing Entries in an Access List: Example

The following example shows an access list before and after resequencing. The starting value is 1, and increment value is 2. The subsequent entries are ordered based on the increment values that users provide, and the range is from 1 to 2147483647.

When an entry with no sequence number is entered, by default it has a sequence number of 10 more than the last entry in the access list.

```
Router# show access-list carls
```

```
Extended IP access list carls
 10 permit ip host 10.3.3.3 host 172.16.5.34
 20 permit icmp any any
 30 permit tcp any host 10.3.3.3
 40 permit ip host 10.4.4.4 any
 50 Dynamic test permit ip any any
 60 permit ip host 172.16.2.2 host 10.3.3.12
 70 permit ip host 10.3.3.3 any log
 80 permit tcp host 10.3.3.3 host 10.1.2.2
 90 permit ip host 10.3.3.3 any
100 permit ip any any
```

```
Router(config)# ip access-list extended carls
Router(config)# ip access-list resequence carls 1 2
Router(config)# end
```

```
Router# show access-list carls

Extended IP access list carls
 1 permit ip host 10.3.3.3 host 172.16.5.34
 3 permit icmp any any
 5 permit tcp any host 10.3.3.3
 7 permit ip host 10.4.4.4 any
 9 Dynamic test permit ip any any
11 permit ip host 172.16.2.2 host 10.3.3.12
13 permit ip host 10.3.3.3 any log
15 permit tcp host 10.3.3.3 host 10.1.2.2
17 permit ip host 10.3.3.3 any
19 permit ip any any
```

Adding an Entry with a Sequence Number: Example

In the following example, a new entry (sequence number 15) is added to an access list:

```
Router# show ip access-list

Standard IP access list tryon
 2 permit 10.4.4.2, wildcard bits 0.0.255.255
 5 permit 10.0.0.44, wildcard bits 0.0.0.255
10 permit 10.0.0.1, wildcard bits 0.0.0.255
20 permit 10.0.0.2, wildcard bits 0.0.0.255

Router(config)# ip access-list standard tryon

Router(config-std-nacl)# 15 permit 10.5.5.5 0.0.0.255

Router# show ip access-list

Standard IP access list tryon
 2 permit 10.4.0.0, wildcard bits 0.0.255.255
 5 permit 10.0.0.0, wildcard bits 0.0.0.255
10 permit 10.0.0.0, wildcard bits 0.0.0.255
15 permit 10.5.5.0, wildcard bits 0.0.0.255
20 permit 10.0.0.0, wildcard bits 0.0.0.255
```

Adding an Entry with No Sequence Number: Example

The following example shows how an entry with no specified sequence number is added to the end of an access list. When an entry is added without a sequence number, it is automatically given a sequence number that puts it at the end of the access list. Because the default increment is 10, the entry will have a sequence number 10 higher than the last entry in the existing access list.

```
Router(config)# ip access-list standard resources

Router(config-std-nacl)# permit 10.1.1.1 0.0.0.255
Router(config-std-nacl)# permit 10.2.2.2 0.0.0.255
Router(config-std-nacl)# permit 10.3.3.3 0.0.0.255

Router# show access-list

Standard IP access list resources
10 permit 10.1.1.1, wildcard bits 0.0.0.255
20 permit 10.2.2.2, wildcard bits 0.0.0.255
30 permit 10.3.3.3, wildcard bits 0.0.0.255

Router(config)# ip access-list standard resources
```

```
Router(config-std-nacl)# permit 10.4.4.4 0.0.0.255
Router(config-std-nacl)# end

Router# show access-list

Standard IP access list resources
10 permit 10.1.1.1, wildcard bits 0.0.0.255
20 permit 10.2.2.2, wildcard bits 0.0.0.255
30 permit 10.3.3.3, wildcard bits 0.0.0.255
40 permit 10.4.4.4, wildcard bits 0.0.0.255
```

Time Ranges Applied to IP Access List Entries: Example

The following example creates a time range called no-http, which extends from Monday to Friday from 8:00 a.m. to 6:00 p.m. That time range is applied to the **deny** statement, thereby denying HTTP traffic on Monday through Friday from 8:00 a.m. to 6:00 p.m.

The time range called udp-yes defines weekends from noon to 8:00 p.m. That time range is applied to the **permit** statement, thereby allowing UDP traffic on Saturday and Sunday from noon to 8:00 p.m. only. The access list containing both statements is applied to inbound packets on Ethernet interface 0.

```
time-range no-http
  periodic weekdays 8:00 to 18:00
!
time-range udp-yes
  periodic weekend 12:00 to 20:00
!
ip access-list extended strict
  deny tcp any any eq http time-range no-http
  permit udp any any time-range udp-yes
!
interface ethernet 0
  ip access-group strict in
```

Filtering IP Packet Fragments: Example

In the following access list, the first statement will deny only noninitial fragments destined for host 172.16.1.1. The second statement will permit only the remaining nonfragmented and initial fragments that are destined for host 172.16.1.1 TCP port 80. The third statement will deny all other traffic. In order to block noninitial fragments for any TCP port, we must block noninitial fragments for all TCP ports, including port 80 for host 172.16.1.1. That is, non-initial fragments will not contain Layer 4 port information, so, in order to block such traffic for a given port, we have to block fragments for all ports.

```
access-list 101 deny ip any host 172.16.1.1 fragments
access-list 101 permit tcp any host 172.16.1.1 eq 80
access-list 101 deny ip any any
```

Additional References

The following sections provide references related to access list entry resequencing, time-based access lists, or IP fragment filtering.

Related Documents

Related Topic	Document Title
Using the time-range command to establish time ranges	“Performing Basic System Management” chapter in the <i>Cisco IOS Configuration Fundamentals Configuration Guide</i>

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Refining an IP Access List

[Table 1](#) lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for a specific command was introduced, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

[Table 1](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 *Feature Information for Refining an IP Access List*

Feature Name	Releases	Feature Configuration Information
Distributed Time-Based Access Lists	12.2(2)T	<p>Before the introduction of this feature, time-based access lists were not supported on line cards for the Cisco 7500 series routers. If time-based access lists were configured, they behaved as normal access lists. If an interface on a line card were configured with a time-based access list, the packets switched into the interface were not distributed switched through the line card, but were forwarded to the Route Processor for processing.</p> <p>The Distributed Time-Based Access Lists feature allows packets destined for an interface configured with a time-based access list to be distributed switched through the line card. See the following section:</p> <ul style="list-style-type: none"> • Distributed Time-Based Access Lists, page 7
Time-Based Access Lists	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Object Groups for ACLs

First Published: July 11, 2008

Last Updated: July 11, 2008

The Object Groups for ACLs feature lets you classify users, devices, or protocols into groups and apply them to access control lists (ACLs) to create access control policies for those groups. This feature lets you use object groups instead of individual IP addresses, protocols, and ports, which are used in conventional ACLs. This feature allows multiple access control entries (ACEs), but now you can use each ACE to allow an entire group of users to access a group of servers or services or to deny them from doing so.

In large networks, the number of ACLs can be large (hundreds of lines) and difficult to configure and manage, especially if the ACLs frequently change. Object group-based ACLs are smaller, more readable, and easier to configure and manage than conventional ACLs, which simplifies static and dynamic ACL deployments for large user access environments on Cisco IOS routers.

Cisco IOS Firewall benefits from object groups, because they simplify policy creation (for example, group A has access to group A services).

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Object Groups for ACLs”](#) section on page 18.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008 Cisco Systems, Inc. All rights reserved.

Contents

- [Restrictions for Object Groups for ACLs, page 2](#)
- [Information About Object Groups for ACLs, page 2](#)
- [How to Configure Object Group-Based ACLs, page 4](#)
- [Configuration Examples for Object Groups for ACLs, page 13](#)
- [Additional References, page 16](#)
- [Feature Information for Object Groups for ACLs, page 18](#)

Restrictions for Object Groups for ACLs

- You can use object groups only in extended and named (not numbered) ACLs.
- Object group-based ACLs support only IPv4 addresses.
- Object group-based ACLs support only Layer 3 interfaces (such as routed interfaces and VLAN interfaces). Object group-based ACLs do not support Layer 2 features such as VLAN ACLs (VACLs) or port ACLs (PACLs).

Information About Object Groups for ACLs

You can configure conventional ACEs and ACEs that refer to object groups in the same ACL.

You can use object group-based ACLs with QoS match criteria, Cisco IOS Firewall, IPSec, DHCP, and any other features that use extended ACLs. In addition, you can use object group-based ACLs with multicast traffic.

When there are many inbound and outbound packets, using object group-based ACLs increases performance when compared to conventional ACLs. Also, in large configurations, this feature reduces the storage needed in NVRAM, because using object groups in ACEs means that you do not need to define an individual ACE for every address and protocol pairing.

To configure the Object Groups for ACLs feature, you should understand the following concepts:

- [Object Groups, page 2](#)
- [ACLs Based on Object Groups, page 3](#)

Object Groups

An object group can contain a single object (such as a single IP address, network, or subnet) or multiple objects (such as a combination of multiple IP addresses, networks, or subnets)

A typical ACE could allow a group of users to have access only to a specific group of servers. In an object group-based ACL, you can create a single ACE that uses an object group name instead of creating many ACEs (which would require each one to have a different IP address). A similar object group (such as a protocol port group) can be extended to provide access only to a set of applications for a user group to a server group. ACEs can have object groups for the source only, destination only, none, or both.

You can use object groups to separate the ownership of the components of an ACE. For example, each department in an organization could control its group membership, and the administrator could own the ACE itself to control which departments can contact each other.

You can use object groups as members (children) of other object groups. For example, you can create an ENG-ALL address group that contains the ENG-EAST and ENG-WEST address groups. You can use an unlimited number of levels of nested (child) object groups (however, a maximum of two levels is recommended).

You can use object groups in features that use Cisco Policy Language (CPL) class maps.

This feature supports two types of object group for grouping ACL parameters: network object groups and service object groups. These object groups can be used to group IP addresses, protocols, protocol services (ports), and ICMP types.

Objects Allowed in Network Object Groups

A network object group is a group of any of the following objects:

- Hostnames
- Host IP addresses
- Subnets
- Ranges of IP addresses
- Other network object groups

Objects Allowed in Service Object Groups

A service object group is a group of any of the following objects:

- Source and destination protocol ports (such as Telnet or SNMP)
- ICMP types (such as echo, echo-reply, or host-unreachable)
- Top-level protocols (such as TCP, UDP, or ESP)
- Other service object groups

ACLs Based on Object Groups

All features that use or reference conventional ACLs are compatible with object group-based ACLs, and feature interactions for conventional ACLs are the same with object group-based ACLs. This feature extends the conventional ACL syntax to support object group-based ACLs and also adds new keywords along with the source and destination addresses and ports.

You can apply object group-based ACLs to interfaces that are configured in a VPN routing/forwarding (VRF) instance or features that are used within a VRF context.

How to Configure Object Group-Based ACLs

You can add to, delete from, or change objects in an object group membership list dynamically (meaning without deleting and redefining the object group). Also, you can add to, delete from, or change objects in an object group membership list without redefining the ACL ACE that is using the object group (meaning without deleting the ACE before changing the object group and then redefining the ACE after the change). You can add objects to groups and delete them from groups and then ensure that the changes are properly functioning within the object group-based ACL without re-applying it to the interface.

You can configure an object group-based ACL multiple times with source group only, destination group only, or source and destination groups.

You cannot delete an object group that is being used within an ACL or a CPL policy.

To configure the Object Groups for ACLs feature, you first create one or more object groups. These can be any combination of network object groups (containing objects such as host addresses and network addresses) or service object groups (which use operators such as **lt**, **eq**, **gt**, **neq**, and **range** with port numbers). Then, you create ACEs that apply a policy (such as **permit** or **deny**) to those object groups.

This section contains the following procedures:

- [Creating a Network Object Group, page 5](#) (optional)
- [Creating a Service Object Group, page 7](#) (optional)
- [Creating an Object Group-Based ACL, page 8](#) (required)
- [Applying an Object Group-Based ACL to an Interface, page 12](#) (required)
- [Verifying Object Groups for ACLs, page 13](#) (optional)

Creating a Network Object Group

To create a network object group, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **object-group network** *object-group-name*
4. **description** *description-text*
5. **host** {*host-address* | *host-name*}
6. *network-address* [*network-mask*]
7. **range** *host-address1* *host-address2*
8. **group-object** *nested-object-group-name*
9. Repeat some combination of Steps 5. through 8. until you have specified the objects on which you want to base your object group.
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# object-group network <i>object-group-name</i> Example: Router(config)# object-group network my_network_object_group	Defines the object group name and enters network object-group configuration mode.
Step 4	Router(config-network-group)# description <i>description-text</i> Example: Router(config-network-group)# description San Jose engineers	(Optional) Specifies a description of the object group. You can use up to 200 characters.
Step 5	Router(config-network-group)# host { <i>host-address</i> <i>host-name</i> } Example: Router(config-network-group)# host 10.20.20.1	(Optional) Specifies the IP address or name of a host. If you specify a host address, you must use an IPv4 address.

	Command or Action	Purpose
Step 6	<pre>Router(config-network-group)# <i>network-address</i> [<i>network-mask</i>]</pre> <p>Example:</p> <pre>Router(config-network-group)# 10.30.0.0 255.255.0.0</pre>	(Optional) Specifies a subnet object. You must specify an IPv4 address for the network address. The default network mask is 255.255.255.255.
Step 7	<pre>Router(config-network-group)# range <i>host-address1</i> <i>host-address2</i></pre> <p>Example:</p> <pre>Router(config-network-group)# range 172.23.56.195 172.23.56.196</pre>	(Optional) Specifies a range of host IP addresses. A mask of 255.255.255.0 is implicit.
Step 8	<pre>Router(config-network-group)# group-object <i>nested-object-group-name</i></pre> <p>Example:</p> <pre>Router(config-network-group)# group-object my_nested_object_group</pre>	<p>(Optional) Specifies a nested (child) object group to be included in the current (parent) object group.</p> <p>The type of child object group must match that of the parent (for example, if you are creating a network object group, you must specify another network object group as the child).</p> <p>You can use duplicated objects in an object group if it is because of the inclusion of group objects. For example, if object 1 is in both group A and group B, you can define a group C that includes both A and B. However, you cannot include a group object that causes the group hierarchy to become circular (for example, you cannot include group A in group B and then also include group B in group A).</p> <p>You can use an unlimited number of levels of nested object groups (however, a maximum of two levels is recommended).</p>
Step 9	Repeat some combination of Steps 5 through 8 until you have specified the objects on which you want to base your object group.	
Step 10	<pre>Router(config-network-group)# end</pre> <p>Example:</p> <pre>Router(config-network-group)# end</pre>	Returns to privileged EXEC mode.

Creating a Service Object Group

To create a service object group, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **object-group service** *object-group-name*
4. **description** *description-text*
5. *protocol*
6. **[tcp | udp | tcp-udp]** **[source** { **[eq | lt | gt]** *port1* | **range** *port1 port2* } } **[{ [eq | lt | gt]** *port1* | **range** *port1 port2* }]
7. **icmp** *icmp-type*
8. **group-object** *nested-object-group-name*
9. Repeat some combination of Steps 5. through 8. until you have specified the objects on which you want to base your object group.
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# object-group service <i>object-group-name</i> Example: Router(config)# object-group service my_service_object_group	Defines the object group name and enters service object-group configuration mode.
Step 4	Router(config-service-group)# description <i>description-text</i> Example: Router(config-service-group)# description Milpitas engineers	(Optional) Specifies a description of the object group. You can use up to 200 characters.
Step 5	Router(config-service-group)# <i>protocol</i> Example: Router(config-service-group)# ahp	(Optional) Specifies an IP protocol number or name.

	Command or Action	Purpose
Step 6	<pre>Router(config-service-group)# tcp udp tcp-udp [source {[eq] lt gt} <i>port1</i> range <i>port1 port2</i>]} [{[eq] lt gt} <i>port1</i> range <i>port1 port2</i>}]</pre> <p>Example:</p> <pre>Router(config-service-group)# tcp-udp range 2000 2005</pre>	(Optional) Specifies TCP, UDP, or both.
Step 7	<pre>Router(config-service-group)# icmp <i>icmp-type</i></pre> <p>Example:</p> <pre>Router(config-service-group)# conversion-error</pre>	(Optional) Specifies the decimal number or name of an ICMP type.
Step 8	<pre>Router(config-service-group)# group-object <i>nested-object-group-name</i></pre> <p>Example:</p> <pre>Router(config-service-group)# group-object my_nested_object_group</pre>	<p>(Optional) Specifies a nested (child) object group to be included in the current (parent) object group.</p> <p>The type of child object group must match that of the parent (for example, if you are creating a network object group, you must specify another network object group as the child).</p> <p>You can use duplicated objects in an object group if it is because of the inclusion of group objects. For example, if object 1 is in both group A and group B, you can define a group C that includes both A and B. However, you cannot include a group object that causes the group hierarchy to become circular (for example, you cannot include group A in group B and then also include group B in group A).</p> <p>You can use an unlimited number of levels of nested object groups (however, a maximum of two levels is recommended).</p>
Step 9	Repeat some combination of Steps 5 through 8 until you have specified the objects on which you want to base your object group.	
Step 10	<pre>Router(config-service-group)# end</pre> <p>Example:</p> <pre>Router(config-service-group)# end</pre>	Returns to privileged EXEC mode.

Creating an Object Group-Based ACL

When creating an object group-based ACL, you configure an ACL that references one or more object groups. As with regular ACLs, you can associate the same access policy with one or more interfaces.

You can define multiple ACEs that reference object groups within the same object group-based ACL. Also, you can reuse a specific object group in multiple ACEs.

To create an object group-based ACL, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list extended** *access-list-name*
4. **remark** *remark*
5. **deny protocol source** [*source-wildcard*] *destination* [*destination-wildcard*] [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]
6. **remark** *remark*
7. **permit protocol source** [*source-wildcard*] *destination* [*destination-wildcard*] [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]
8. Repeat some combination of Steps 4. through 7. until you have specified the fields and values on which you want to base your access list.
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip access-list extended <i>access-list-name</i> Example: Router(config)# ip access-list extended nomarketing	Defines an extended IP access list using a name and enters extended named access list configuration mode.
Step 4	remark <i>remark</i> Example: Router(config-ext-nacl)# remark protect server by denying access from the Marketing network	(Optional) Adds a user-friendly comment about an access list entry. <ul style="list-style-type: none">• A remark can precede or follow an access list entry.• In this example, the remark reminds the network administrator that the subsequent entry denies the Sales network access to the interface.

	Command or Action	Purpose
Step 5	<p>deny <i>protocol</i> <i>source</i> [<i>source-wildcard</i>] <i>destination</i> [<i>destination-wildcard</i>] [option <i>option-name</i>] [precedence <i>precedence</i>] [tos <i>tos</i>] [established] [log log-input] [time-range <i>time-range-name</i>] [fragments]</p> <p>Example: Router(config-ext-nacl)# deny ip 172.18.0.0 0.0.255.255 host 172.16.40.10 log</p>	<p>(Optional) Denies any packet that matches all of the conditions specified in the statement.</p> <ul style="list-style-type: none"> Optionally use the keyword and argument object-group <i>service-object-group-name</i> as a substitute for the <i>protocol</i>. Optionally use the keyword and argument object-group <i>source-network-object-group-name</i> as a substitute for the <i>source source-wildcard</i>. Optionally use the keyword and argument object-group <i>destination-network-object-group-name</i> as a substitute for the <i>destination destination-wildcard</i>. If the <i>source-wildcard</i> or <i>destination-wildcard</i> is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source or destination address, respectively. Optionally use the keyword any as a substitute for the <i>source source-wildcard</i> or <i>destination destination-wildcard</i> to specify the address and wildcard of 0.0.0.0 255.255.255.255. Optionally use the keyword host <i>source</i> to indicate a source and source wildcard of <i>source</i> 0.0.0.0 or the abbreviation host <i>destination</i> to indicate a destination and destination wildcard of <i>destination</i> 0.0.0.0. In this example, packets from all sources are denied access to the destination network 172.18.0.0. Logging messages about packets permitted or denied by the access list are sent to the facility configured by the logging facility command (for example, console, terminal, or syslog). That is, any packet that matches the access list will cause an informational logging message about the packet to be sent to the configured facility. The level of messages logged to the console is controlled by the logging console command.
Step 6	<p>remark <i>remark</i></p> <p>Example: Router(config-ext-nacl)# remark allow TCP from any source to any destination</p>	<p>(Optional) Adds a user-friendly comment about an access list entry.</p> <ul style="list-style-type: none"> A remark can precede or follow an access list entry.

	Command or Action	Purpose
Step 7	<p>permit <i>protocol source [source-wildcard] destination [destination-wildcard] [option option-name] [precedence precedence] [tos tos] [established] [log log-input] [time-range time-range-name] [fragments]</i></p> <p>Example: Router(config-ext-nacl)# permit tcp any any</p>	<p>Permits any packet that matches all of the conditions specified in the statement.</p> <ul style="list-style-type: none"> • Every access list needs at least one permit statement. • Optionally use the keyword and argument object-group <i>service-object-group-name</i> as a substitute for the <i>protocol</i>. • Optionally use the keyword and argument object-group <i>source-network-object-group-name</i> as a substitute for the <i>source source-wildcard</i>. • Optionally use the keyword and argument object-group <i>destination-network-object-group-name</i> as a substitute for the <i>destination destination-wildcard</i>. • If the <i>source-wildcard</i> or <i>destination-wildcard</i> is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source or destination address, respectively. • Optionally use the keyword any as a substitute for the <i>source source-wildcard</i> or <i>destination destination-wildcard</i> to specify the address and wildcard of 0.0.0.0 255.255.255.255. • In this example, TCP packets are allowed from any source to any destination. • Use the log-input keyword to include input interface, source MAC address, or virtual circuit in the logging output.
Step 8	Repeat some combination of Steps 4 through 7 until you have specified the fields and values on which you want to base your access list.	Remember that all sources not specifically permitted are denied by an implicit deny statement at the end of the access list.
Step 9	<p>end</p> <p>Example: Router(config-ext-nacl)# end</p>	Returns to privileged EXEC mode.

Applying an Object Group-Based ACL to an Interface

You use the **ip access-group** command to apply an object group-based ACL to an interface. The command syntax and usage are the same as for conventional ACLs.

To apply an object group-based ACL to an interface, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip access-group** {*access-list-name* | *access-list-number*} {**in** | **out**}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Router(config-if# interface vlan 100	Specifies the interface type and number and enters interface configuration mode.
Step 4	ip access-group { <i>access-list-name</i> <i>access-list-number</i> } { in out } Example: Router(config-if)# ip access-group my_ogacl_policy in	Applies the ACL to the interface and specifies whether to filter inbound or outbound packets.
Step 5	Router(config-if)# end Example: Router(config-if)# end	Returns to privileged EXEC mode.

Verifying Object Groups for ACLs

To verify object groups for ACLs, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **show object-group** [*object-group-name*]
3. **show ip access-list** [*access-list-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	Router# show object-group [<i>object-group-name</i>]	Displays the configuration in the named object group (or in all object groups if no name is entered).
Step 3	Router# show ip access-list [<i>access-list-name</i>]	Displays the contents of the named access list or object group-based ACL (or for all access lists and object group-based ACLs if no name is entered).

Configuration Examples for Object Groups for ACLs

This section provides the following configuration examples:

- [Creating a Network Object Group: Example, page 13](#)
- [Creating a Service Object Group: Example, page 14](#)
- [Creating an Object Group-Based ACL: Example, page 14](#)
- [Applying an Object Group-Based ACL to an Interface: Example, page 14](#)
- [Verifying Object Groups for ACLs: Example, page 15](#)

Creating a Network Object Group: Example

The following example shows how to create a network object group named `my_network_object_group`, which contains two hosts, a range of IP addresses, and a subnet as objects.

```
Router> enable
Router# configure terminal
Router(config)# object-group network my_network_object_group
Router(config-network-group)# host 10.20.20.1
Router(config-network-group)# host 10.20.20.5
Router(config-network-group)# range 10.50.1.23 10.50.1.45
Router(config-network-group)# 10.30.0.0 255.255.0.0
```

The following example shows how to create a network object group named `sjc_ftp_servers`, which contains two hosts, a subnet, and an existing object group (child) named `sjc_eng_ftp_servers` as objects.

```
Router> enable
Router# configure terminal
Router(config)# object-group network sjc_ftp_servers
Router(config-network-group)# host sjc.eng.ftp
Router(config-network-group)# host 172.23.56.195
Router(config-network-group)# 193.1.1.0 255.255.255.224
Router(config-network-group)# group-object sjc_eng_ftp_servers
```

Creating a Service Object Group: Example

The following example shows how to create a service object group named `my_service_object_group`, which contains several ICMP, TCP, UDP, and TCP-UDP protocols and an existing object group (child) named `sjc_eng_svcs` as objects.

```
Router> enable
Router# configure terminal
Router(config)# object-group service my_service_object_group
(config-service-group)# icmp echo
(config-service-group)# tcp smtp
(config-service-group)# tcp telnet
(config-service-group)# tcp source range 1 65535 snmp
(config-service-group)# udp domain
(config-service-group)# tcp-udp range 2000 2005
(config-service-group)# group-object sjc_eng_svcs
```

Creating an Object Group-Based ACL: Example

The following example shows how to create an object group-based ACL that permits packets from the users in `my_network_object_group` if the protocol ports match the ports specified in `my_service_object_group`.

```
Router> enable
Router# configure terminal
Router(config)# ip access-list extended my_ogacl_policy
Router(config-ext-nacl)# permit tcp object-group my_network_object_group object-group
my_service_object_group any
Router(config-ext-nacl)# deny tcp any any
Router(config-ext-nacl)# exit
Router(config)# exit
```

Applying an Object Group-Based ACL to an Interface: Example

The following example shows how to apply an object group-based ACL to an interface. In this example, an object group-based ACL named `my_ogacl_policy` is applied to VLAN interface 100:

```
Router> enable
Router# configure terminal
Router(config)# interface vlan 100
Router(config-if)# ip access-group my_ogacl_policy in
Router(config-if)# end
```

Verifying Object Groups for ACLs: Example

The following example shows how to display all object groups.

```
Router> enable
Router#
Network object group auth_proxy_acl_deny_dest
  host 171.68.225.134

Service object group auth_proxy_acl_deny_services
  tcp eq www
  tcp eq 443

Network object group auth_proxy_acl_permit_dest
  10.34.250.96 255.255.255.224
  171.68.0.0 255.252.0.0
  172.16.0.0 255.240.0.0
  128.107.0.0 255.255.0.0
  10.0.0.0 255.0.0.0
  64.100.0.0 255.253.0.0
  64.104.0.0 255.255.0.0
  144.254.0.0 255.255.0.0
  161.44.0.0 255.255.0.0
  192.168.0.0 255.255.0.0

Service object group auth_proxy_acl_permit_services
  tcp eq www
  tcp eq 443
```

The following example shows how to display information about specific object group-based ACLs.

```
Router# show ip access-list my_ogacl_policy
Extended IP access list my_ogacl_policy
10 permit object-group eng_service any any
```

Additional References

The following sections provide references related to the Object Groups for ACLs feature.

Related Documents

Related Topic	Document Title
General information about ACLs	“IP Access List Overview” module in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4T
Security commands	<i>Cisco IOS Security Command Reference</i>

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Feature Information for Object Groups for ACLs

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Releases 12.2(1), 12.0(3)S, 12.2(33)SRA, 12.2(33)SXH, or later releases appear in the table.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Object Groups for ACLs

Feature Name	Releases	Feature Information
Object Groups for ACLs	12.4(20)T	<p>The Object Groups for ACLs feature lets you classify users, devices, or protocols into groups and apply them to access control lists (ACLs) to create access control policies for those groups. This feature lets you use object groups instead of individual IP addresses, protocols, and ports, which are used in conventional ACLs. This feature allows multiple access control entries (ACEs), but now you can use each ACE to allow an entire group of users to access a group of servers or services or to deny them from doing so.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • ACLs Based on Object Groups, page 3 • Object Groups, page 2 • Creating a Network Object Group, page 5 • Creating a Service Object Group, page 7 • Creating an Object Group-Based ACL, page 8 • Applying an Object Group-Based ACL to an Interface, page 12 • Verifying Object Groups for ACLs, page 13 <p>The following commands were introduced or modified: deny, ip access-group, ip access-list, object-group network, object-group service, permit, show ip access-list, show object-group.</p>

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.



Displaying and Clearing IP Access List Data Using ACL Manageability

First Published: August 18, 2006

Last Updated: August 18, 2006

This module describes how to display the entries in an IP access list and the number of packets that have matched each entry. Users can get these statistics globally, or per interface and per incoming or outgoing traffic direction, by using the ACL Manageability feature. Viewing details of incoming and outgoing traffic patterns on various interfaces of a network device can help secure devices against attacks coming in on a particular interface. This module also describes how to clear counters so that the count of packets matching an access list entry will restart from zero.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module.

[“Feature Information for Displaying IP Access List Information and Clearing Counters” section on page 8.](#)

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Introduction, page 2](#)
- [How to Display and Clear IP Access List Data, page 2](#)
 - [Display and Clear IP ACL Data Examples, page 4](#)
 - [Additional References, page 6](#)
 - [Feature Information for Displaying IP Access List Information and Clearing Counters, page 8](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Information About IP Access List Data

Before displaying or clearing IP access list data, you should understand the following concepts:

- [Benefits of ACL Manageability, page 2](#)
- [Support for Interface-Level ACL Statistics, page 2](#)

Benefits of ACL Manageability

Prior to Cisco IOS Release 12.4(6)T, the ACL infrastructure in Cisco IOS software maintained only global statistics for each ACE in an ACL. With this method, if an ACL is applied to multiple interfaces, the maintained ACE statistics are the sum of incoming and outgoing packet matches (hits) on all the interfaces on which that ACL is applied.

However, if ACE statistics are maintained per interface and per incoming or outgoing traffic direction, users can view specific details of incoming and outgoing traffic patterns and the effectiveness of ACEs on the various interfaces of a network device. This type of information is useful for securing devices against attacks coming in on a particular interface.

Support for Interface-Level ACL Statistics



Note

How to Display and Clear IP Access List Data



Note

log

deny

[Displaying Global IP ACL Statistics, page 3](#)

[Displaying Interface-Level IP ACL Statistics, page 3](#)

[Clearing the Access List Counters, page 4](#)

Displaying Global IP ACL Statistics

SUMMARY STEPS

1. `enable`
`show ip access-list [access-list-number | access-list-name]`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
	Example: Router> <code>enable</code>	
	<code>show ip access-list [access-list-number access-list-name]</code> Router# <code>show ip access-list limited</code>	

This section describes how to display IP ACE statistics per interface and per incoming or outgoing traffic direction for ACLs. This feature is known as ACL Manageability.

Restrictions for ACL Manageability

-

–

–

–

–

interface

in out

	Enables privileged EXEC mode. Enter your password if prompted.
<pre>in out interface interface-name Router# show ip access-list interface FastEthernet 0/0 in</pre>	

Clearing the Access List Counters

The system counts how many packets match (hit) each line of an access list; the counters are displayed by the EXEC command. Perform this task to clear the counters of an access list. You might do this if you are trying to determine a more recent count of packets that match an access list, starting from zero.

{ | }

Router> enable	
{ access-list-name}	
Router# clear access-list counters corpmark	

Display and Clear IP ACL Data Examples

Displaying Global IP ACL Statistics: Example

The following example displays global statistics for ACL 150:

```
show ip access-list 150
```

```
Extended IP access list 150
 10 permit ip host 10.1.1.1 any (3 matches)
 30 permit ip host 10.2.2.2 any (27 matches)
```

```
Router# show ip access-list interface FastEthernet 0/1 in
```

Displaying Output Statistics: Example

```
show ip access-list interface FastEthernet 0/0 out
```

```
10 permit udp any any eq snmp (6 matches)
```

Displaying Input and Output Statistics: Example



Note

```
Router#

Extended IP access list 150 in
 10 permit ip host 10.1.1.1 any
 30 permit ip host 10.2.2.2 any (15 matches)
Extended IP access list myacl out
 5 deny ip any 10.1.0.0 0.0.255.255
```

Additional References

Related Documents

Related Topic	Document Title
	, Release 12.4T
	, Release 12.4T
	, Release 12.4T “Access List Logging” section in the “IP Access List Overview” module

Standards

Standard	Title
	—

MIBs

MIB	MIBs Link

RFCs

RFC	Title

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Displaying IP Access List Information and Clearing Counters



Note

Table 1 Feature Information for Displaying and Clearing IP Access List Data Using ACL Manageability

Feature Name	Releases	Feature Information
		<ul style="list-style-type: none"> • • • •

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





Controlling Access to a Virtual Terminal Line

First Published: August 18, 2006

Last Updated: August 18, 2006

You can control who can access the virtual terminal lines (vty) to a router by applying an access list to inbound vtys. You can also control the destinations that the vtys from a router can reach by applying an access list to outbound vtys.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Controlling Access to a Virtual Terminal Line”](#) section on page 9.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Restrictions for Controlling Access to a Virtual Terminal Line, page 2](#)
- [Information About Controlling Access to a Virtual Terminal Line, page 2](#)
- [How to Control Access to a Virtual Terminal Line, page 2](#)
- [Configuration Examples for Controlling Access to a Virtual Terminal Line, page 7](#)
- [Where to Go Next, page 8](#)
- [Additional References, page 8](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Restrictions for Controlling Access to a Virtual Terminal Line

When you apply an access list to a vty (by using the **access-class** command), the access list must be a numbered access list, not a named access list.

Information About Controlling Access to a Virtual Terminal Line

Before you control access to a vty, you should understand the following concepts:

- [Benefits of Controlling Access to a Virtual Terminal Line, page 2](#)

Benefits of Controlling Access to a Virtual Terminal Line

By applying an access list to an inbound vty, you can control who can access the lines to a router. By applying an access list to an outbound vty, you can control the destinations that the lines from a router can reach.

How to Control Access to a Virtual Terminal Line

This section contains the following procedures:

- [Controlling Inbound Access to a vty, page 2](#)
- [Controlling Outbound Access to a vty, page 4](#)

Controlling Inbound Access to a vty

Perform this task when you want to control access to a vty coming into the router by using an access list. Access lists are very flexible; this task illustrates one **access-list deny** command and one **access-list permit** command. You will decide how many of each command you should use and their order to achieve the restrictions you want.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* **deny** {*source* [*source-wildcard*] | **any**} [**log**]
4. **access-list** *access-list-number* **permit** {*source* [*source-wildcard*] | **any**} [**log**]
5. **line vty** *line-number* [*ending-line-number*]
6. **access-class** *access-list-number* **in** [**vrf-also**]
7. **exit**
8. Repeat Steps 5 and 6 for each line to set identical restrictions on all the virtual terminal lines because a user can connect to any of them.
9. **end**
10. **show line** [*line-number* | **summary**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	access-list access-list-number deny {source [source-wildcard] any} [log] Example: Router(config)# access-list 1 deny 172.16.7.34	(Optional) Denies the specified source based on a source address and wildcard mask. <ul style="list-style-type: none"> If the <i>source-wildcard</i> is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source address. Optionally use the keyword any as a substitute for the <i>source source-wildcard</i> to specify the source and source wildcard of 0.0.0.0 255.255.255.255. In this example, host 172.16.7.34 is denied passing the access list.
Step 4	access-list access-list-number permit {source [source-wildcard] any} [log] Example: Router(config)# access-list 1 permit 172.16.0.0 0.0.255.255	Permits the specified source based on a source address and wildcard mask. <ul style="list-style-type: none"> If the <i>source-wildcard</i> is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source address. Optionally use the keyword any as a substitute for the <i>source source-wildcard</i> to specify the source and source wildcard of 0.0.0.0 255.255.255.255. In this example, hosts on network 172.16.0.0 (other than the host denied in the prior step) pass the access list, meaning they can access the vtys identified in the line command.
Step 5	line vty line-number [ending-line-number] Example: Router(config)# line vty 5 10	Identifies a specific line for configuration and enters line configuration mode. <ul style="list-style-type: none"> Entering the line command with the optional line type vtty designates the line number as a relative line number. You also can use the line command without specifying a line type. In this case, the line number is treated as an absolute line number.

	Command or Action	Purpose
Step 6	access-class <i>access-list-number</i> in [vrf-also] Example: Router(config-line)# access-class 1 in vrf-also	Restricts incoming connections between a particular vty (into a Cisco device) and the networking devices associated with addresses in the access list. <ul style="list-style-type: none"> If you do not specify the vrf-also keyword, incoming Telnet connections from interfaces that are part of a VPN routing and forwarding (VRF) instance are rejected.
Step 7	exit Example: Router(config-line)# exit	Returns the user to the next highest configuration mode.
Step 8	Repeat Steps 5 and 6 for each line to set identical restrictions on all the vtys because a user can connect to any of them.	If you indicated the full range of vty lines in Step 5 with the line command, you do not need to repeat Steps 5 and 6.
Step 9	end Example: Router(config-line)# end	Returns the user to privileged EXEC mode.
Step 10	show line [<i>line-number</i> summary] Example: Router# show line 5	Displays parameters of a terminal line.

Controlling Outbound Access to a vty

Perform this task when you want to control access from a vty to a destination. Access lists are very flexible; this task illustrates one **access-list deny** command and one **access-list permit** command. You will decide how many of each command you should use and their order to achieve the restrictions you want.

Outbound Access List on a Line Specifies a Destination Address

When a standard access list is applied to a line with the **access-class out** command, the address specified in the access list is not a source address (as it is in an access list applied to an interface), but a destination address.

SUMMARY STEPS

- enable**
- configure terminal**
- access-list** *access-list-number* **deny** {*destination* [*destination-wildcard*] | **any**} [**log**]
- access-list** *access-list-number* **permit** {*destination* [*destination-wildcard*] | **any**} [**log**]
- line vty** *line-number* [*ending-line-number*]
- access-class** *access-list-number* **out**

7. **exit**
8. Repeat Steps 5 and 6 for each line to set identical restrictions on all the virtual terminal lines because a user can connect to any of them.
9. **end**
10. **show line** [*line-number* | **summary**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	access-list access-list-number deny {destination [destination-wildcard] any} [log] Example: Router(config)# access-list 2 deny 172.16.7.34	Denies line access to the specified destination based on a destination address and wildcard mask. <ul style="list-style-type: none"> If the <i>destination-wildcard</i> is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source address. Optionally use the keyword any as a substitute for the <i>destination destination-wildcard</i> to specify the source and source wildcard of 0.0.0.0 255.255.255.255. In this example, host 172.16.7.34 is denied passing the access list, meaning the line cannot connect to it.
Step 4	access-list access-list-number permit {source [source-wildcard] any} [log] Example: Router(config)# access-list 2 permit 172.16.0.0 0.0.255.255	Permits the specified source based on a source address and wildcard mask. <ul style="list-style-type: none"> If the <i>source-wildcard</i> is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source address. Optionally use the keyword any as a substitute for the <i>source source-wildcard</i> to specify the source and source wildcard of 0.0.0.0 255.255.255.255. In this example, hosts on network 172.16.0.0 (other than the host denied in the prior step) pass the access list, meaning they can be connected to by the vty identified in the line command.
Step 5	line vty line-number [ending-line-number] Example: Router(config)# line vty 5 10	Identifies a specific line for configuration and enter line configuration mode. <ul style="list-style-type: none"> Entering the line command with the optional line type vty designates the line number as a relative line number. You also can use the line command without specifying a line type. In this case, the line number is treated as an absolute line number.
Step 6	access-class access-list-number out Example: Router(config-line)# access-class 2 out	Restricts connections between a particular vty (into a Cisco device) out to the networking devices associated with addresses in the access list.

	Command or Action	Purpose
Step 7	exit Example: Router(config-line)# exit	Returns the user to the next highest configuration mode.
Step 8	Repeat Steps 5 and 6 for each line to set identical restrictions on all the vtys because a user can connect to any of them.	If you indicated the full range of vtys in Step 5 with the line command, you do not need to repeat Steps 5 and 6.
Step 9	end Example: Router(config-line)# end	Returns the user to privileged EXEC mode.
Step 10	show line [<i>line-number</i> summary] Example: Router# show line 5	Displays parameters of a terminal line.

Configuration Examples for Controlling Access to a Virtual Terminal Line

This section provides the following configuration examples:

- [Controlling Inbound Access on vtys: Example, page 7](#)
- [Controlling Outbound Access on vtys: Example, page 7](#)

Controlling Inbound Access on vtys: Example

The following example defines an access list that permits only hosts on network 172.19.5.0 to connect to the virtual terminal lines 1 through 5 on the router. Because the **vty** keyword is omitted from the **line** command, the line numbers 1 through 5 are absolute line numbers.

```
access-list 12 permit 172.19.5.0 0.0.0.255
line 1 5
access-class 12 in
```

Controlling Outbound Access on vtys: Example

The following example defines an access list that denies connections to networks other than network 171.20.0.0 on terminal lines 1 through 5. Because the **vty** keyword is omitted from the **line** command, the line numbers 1 through 5 are absolute line numbers.

```
access-list 10 permit 172.20.0.0 0.0.255.255
line 1 5
access-class 10 out
```

Where to Go Next

You can further secure a vty by configuring a password with the **password** line configuration command. See the **password** (line configuration) command in the [Cisco IOS Security Command Reference](#), Release 12.4.

Additional References

The following sections provide references related to Controlling Access to a Virtual Terminal Line.

Related Documents

Related Topic	Document Title
Configuring a password on a line	Cisco IOS Security Command Reference , Release 12.4

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Controlling Access to a Virtual Terminal Line

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for a specific command was introduced, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 **Feature Information for Controlling Access to a Virtual Terminal Line**

Feature Name	Releases	Feature Configuration Information
This table is intentionally left blank because no features were introduced or modified in Cisco IOS Release 12.2(1) or a later release. This table will be updated when feature information is added to this module.	—	—

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Cisco IOS Firewall Overview

This chapter describes how you can configure your Cisco networking device to function as a firewall, using Cisco IOS Firewall security features.

This chapter has the following sections:

- [About Firewalls](#)
- [The Cisco IOS Firewall Solution](#)
- [Creating a Customized Firewall](#)
[Other Guidelines for Configuring Your Firewall](#)

About Firewalls

Firewalls are networking devices that control access to your organization's network assets. Firewalls are positioned at the entrance points into your network. If your network has multiple entrance points, you must position a firewall at each point to provide effective network access control.

Firewalls are often placed in between the internal network and an external network such as the Internet. With a firewall between your network and the Internet, all traffic coming from the Internet must pass through the firewall before entering your network.

Firewalls can also be used to control access to a specific part of your network. For example, you can position firewalls at all the entry points into a research and development network to prevent unauthorized access to proprietary information.

The most basic function of a firewall is to monitor and filter traffic. Firewalls can be simple or elaborate, depending on your network requirements. Simple firewalls are usually easier to configure and manage. However, you might require the flexibility of a more elaborate firewall.

The Cisco IOS Firewall Solution

firewall functionality are listed in the [“Creating a Customized Firewall”](#) section.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

The Cisco IOS Firewall Feature Set

The Cisco IOS Firewall feature set combines existing Cisco IOS firewall technology and Context-based Access Control (CBAC). When you configure the Cisco IOS Firewall on your Cisco router, you turn your router into an effective, robust firewall.

The Cisco IOS Firewall features are designed to prevent unauthorized external individuals from gaining access to your internal network and to block attacks on your network, while at the same time allowing authorized users to access network resources.

You can use the Cisco IOS Firewall features to configure your Cisco IOS router as one of the following:

- An Internet firewall or part of an Internet firewall
- A firewall between groups in your internal network
- A firewall providing secure connections to or from branch offices
- A firewall between your company's network and your company's partners' networks

The Cisco IOS Firewall features provide the following benefits:

- Protection of internal networks from intrusion
- Monitoring of traffic through network perimeters
- Enabling of network commerce via the World Wide Web

Creating a Customized Firewall

- Standard Access Lists and Static Extended Access Lists
- Reflexive Access Lists
- Lock-and-Key (Dynamic Access Lists)
- TCP Intercept
- Context-based Access Control
- Intrusion Prevention System (IPS) (formerly known as Cisco IOS Firewall Intrusion Detection System)
- Authentication Proxy
- Port to Application Mapping
- Security Server Support
- Network Address Translation
- IPSec Network Security
- Neighbor Router Authentication

User Authentication and Authorization

In addition to configuring these features, you should follow the guidelines listed in the “[Other Guidelines for Configuring Your Firewall](#)” section. This section outlines important security practices to protect your firewall and network. [Table 23](#) describes Cisco IOS security features.

Table 23 *Cisco IOS Features for a Robust Firewall*

Feature	Chapter	Comments
		through your firewall, such as IP, IPX, AppleTalk, and so forth.
Lock-and-Key (Dynamic Access Lists)	“Configuring Lock-and-Key Security (Dynamic Access Lists)”	Lock-and-Key provides traffic filtering with the ability to allow temporary access through the firewall for certain individuals. These individuals must first be authenticated (by a username/password mechanism) before the firewall allows their traffic through the firewall. Afterwards, the firewall closes the temporary opening. This provides tighter control over traffic at the firewall than with standard or static extended access lists.
Reflexive Access Lists	“Configuring IP Session Filtering (Reflexive Access Lists)”	Reflexive access lists filter IP traffic so that TCP or UDP “session” traffic is only permitted through the firewall if the session originated from within the internal network. You would only configure Reflexive Access Lists when not using Context-based Access Control.
TCP Intercept	“Configuring TCP Intercept (Preventing Denial-of-Service Attacks)”	TCP Intercept protects TCP servers within your network from TCP SYN-flooding attacks, a type of denial-of-service attack. You would only configure TCP Intercept when not using Context-based Access Control.

	<p>“Configuring TACACS+,” “Configuring RADIUS,” and “Configuring Kerberos”</p>	<p>The Cisco IOS Firewall feature set can be configured as a client of the following supported security servers:</p> <p style="padding-left: 40px;">TACACS+ (including CiscoSecure)</p> <p style="padding-left: 40px;">RADIUS</p> <p style="padding-left: 40px;">Kerberos</p> <p>You can use any of these security servers to store a database of user profiles. To gain access into your firewall or to gain access through the firewall into another network, users must enter authentication information (such as a username and password), which is matched against the information on the security server. When users pass authentication, they are granted access according to their specified privileges.</p>
Network Address Translation	<p>“Configuring NAT for IP Address Conservation”</p>	<p>You can use Network Address Translation (NAT) to hide internal IP network addresses from the world outside the firewall.</p> <p>NAT was designed to provide IP address conservation and for internal IP networks that have unregistered (not globally unique) IP addresses: NAT translates these unregistered IP addresses into legal addresses at the firewall. NAT can also be configured to advertise only one address for the entire internal network to the outside world. This provides security by effectively hiding the entire internal network from the world.</p> <p>NAT gives you limited spoof protection because internal addresses are hidden. Additionally, NAT removes all your internal services from the external name space.</p> <p>NAT does not work with the application-layer protocols RPC, VDOLive, or SQL*Net “Redirected.” (NAT does work with SQL*Net “Bequeathed.”) Do not configure NAT with networks that will carry traffic for these incompatible protocols.</p>

	Cisco IOS Network Management Configuration Guide	

Other Guidelines for Configuring Your Firewall

- enable password enable secret login password password before break

disable **no cdp run** **ntp**

no ip source-route

all

no service tcp-small-servers **no**

service udp-small-servers

no ip directed-broadcast

networks do require directed broadcasts; if this is the case, do not disable directed broadcasts.

Directed broadcasts can be misused to multiply the power of denial-of-service attacks, because every denial-of-service packet sent is broadcast to every host on a subnet. Furthermore, some hosts have other intrinsic security risks present when handling broadcasts.

Configure the **no ip proxy-arp**

coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Configuring Lock-and-Key Security (Dynamic Access Lists)

Feature History

Release	Modification
Cisco IOS	For information about feature support in Cisco IOS software, use Cisco Feature Navigator.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

This chapter describes how to configure lock-and-key security at your router. Lock-and-key is a traffic filtering security feature available for the IP protocol.

For a complete description of lock-and-key commands, refer to the “Lock-and-Key Commands” chapter of the *Cisco IOS Security Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the chapter “Identifying Supported Platforms” section in the “Using Cisco IOS Software.”

In This Chapter

This chapter has the following sections:

- [About Lock-and-Key](#)
- [Compatibility with Releases Before Cisco IOS Release 11.1](#)
- [Risk of Spoofing with Lock-and-Key](#)
- [Router Performance Impacts with Lock-and-Key](#)
- [Prerequisites to Configuring Lock-and-Key](#)
- [Configuring Lock-and-Key](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Verifying Lock-and-Key Configuration](#)
- [Maintaining Lock-and-Key](#)
- [Lock-and-Key Configuration Examples](#)

About Lock-and-Key

Lock-and-key is a traffic filtering security feature that dynamically filters IP protocol traffic. Lock-and-key is configured using IP dynamic extended access lists. Lock-and-key can be used in conjunction with other standard access lists and static extended access lists.

When lock-and-key is configured, designated users whose IP traffic is normally blocked at a router can gain temporary access through the router. When triggered, lock-and-key reconfigures the interface's existing IP access list to permit designated users to reach their designated host(s). Afterwards, lock-and-key reconfigures the interface back to its original state.

For a user to gain access to a host through a router with lock-and-key configured, the user must first open a Telnet session to the router. When a user initiates a standard Telnet session to the router, lock-and-key automatically attempts to authenticate the user. If the user is authenticated, they will then gain temporary access through the router and be able to reach their destination host.

This section has the following sections:

- [Benefits of Lock-and-Key](#)
- [When to Use Lock-and-Key](#)
- [How Lock-and-Key Works](#)

Benefits of Lock-and-Key

Lock-and-key provides the same benefits as standard and static extended access lists (these benefits are discussed in the chapter "Access Control Lists: Overview and Guidelines"). However, lock-and-key also has the following security benefits over standard and static extended access lists:

- Lock-and-key uses a challenge mechanism to authenticate individual users.
- Lock-and-key provides simpler management in large internetworks.
- In many cases, lock-and-key reduces the amount of router processing required for access lists.
- Lock-and-key reduces the opportunity for network break-ins by network hackers.

With lock-and-key, you can specify which users are permitted access to which source and destination hosts. These users must pass a user authentication process before they are permitted access to their designated hosts. Lock-and-key creates dynamic user access through a firewall, without compromising other configured security restrictions.

When to Use Lock-and-Key

Two examples of when you might use lock-and-key follow:

- When you want a specific remote user (or group of remote users) to be able to access a host within your network, connecting from their remote hosts via the Internet. Lock-and-key authenticates the user, then permits limited access through your firewall router for the individual's host or subnet, for a finite period of time.

- When you want a subset of hosts on a local network to access a host on a remote network protected by a firewall. With lock-and-key, you can enable access to the remote host only for the desired set of local user's hosts. Lock-and-key require the users to authenticate through a TACACS+ server, or other security server, before allowing their hosts to access the remote hosts.

How Lock-and-Key Works

The following process describes the lock-and-key access operation:

1. A user opens a Telnet session to a border (firewall) router configured for lock-and-key. The user connects via the virtual terminal port on the router.
2. The Cisco IOS software receives the Telnet packet, opens a Telnet session, prompts for a password, and performs a user authentication process. The user must pass authentication before access through the router is allowed. The authentication process can be done by the router or by a central access security server such as a TACACS+ or RADIUS server.
3. When the user passes authentication, they are logged out of the Telnet session, and the software creates a temporary entry in the dynamic access list. (Per your configuration, this temporary entry can limit the range of networks to which the user is given temporary access.)
4. The user exchanges data through the firewall.
5. The software deletes the temporary access list entry when a configured timeout is reached, or when the system administrator manually clears it. The configured timeout can either be an idle timeout or an absolute timeout.



Note

The temporary access list entry is not automatically deleted when the user terminates a session. The temporary access list entry remains until a configured timeout is reached or until it is cleared by the system administrator.

Compatibility with Releases Before Cisco IOS Release 11.1

Enhancements to the **access-list** command are used for lock-and-key. These enhancements are backward compatible—if you migrate from a release before Cisco IOS Release 11.1 to a newer release, your access lists will be automatically converted to reflect the enhancements. However, if you try to use lock-and-key with a release before Cisco IOS Release 11.1, you might encounter problems as described in the following caution paragraph:



Caution

Cisco IOS releases before Release 11.1 are not upwardly compatible with the lock-and-key access list enhancements. Therefore, if you save an access list with software older than Release 11.1, and then use this software, the resulting access list will not be interpreted correctly. *This could cause you severe security problems.* You must save your old configuration files with Cisco IOS Release 11.1 or later software before booting an image with these files.

Risk of Spoofing with Lock-and-Key

**Caution**

Lock-and-key access allows an external event (a Telnet session) to place an opening in the firewall. While this opening exists, the router is susceptible to source address spoofing.

When lock-and-key is triggered, it creates a dynamic opening in the firewall by temporarily reconfiguring an interface to allow user access. While this opening exists, another host might spoof the authenticated user's address to gain access behind the firewall. Lock-and-key does not cause the address spoofing problem; the problem is only identified here as a concern to the user. Spoofing is a problem inherent to all access lists, and lock-and-key does not specifically address this problem.

To prevent spoofing, configure encryption so that traffic from the remote host is encrypted at a secured remote router, and decrypted locally at the router interface providing lock-and-key. You want to ensure that all traffic using lock-and-key will be encrypted when entering the router; this way no hackers can spoof the source address, because they will be unable to duplicate the encryption or to be authenticated as is a required part of the encryption setup process.

Router Performance Impacts with Lock-and-Key

When lock-and-key is configured, router performance can be affected in the following ways:

- When lock-and-key is triggered, the dynamic access list forces an access list rebuild on the silicon switching engine (SSE). This causes the SSE switching path to slow down momentarily.
- Dynamic access lists require the idle timeout facility (even if the timeout is left to default) and therefore cannot be SSE switched. These entries must be handled in the protocol fast-switching path.
- When remote users trigger lock-and-key at a border router, additional access list entries are created on the border router interface. The interface's access list will grow and shrink dynamically. Entries are dynamically removed from the list after either the idle-timeout or max-timeout period expires. Large access lists can degrade packet switching performance, so if you notice performance problems, you should look at the border router configuration to see if you should remove temporary access list entries generated by lock-and-key.

Prerequisites to Configuring Lock-and-Key

Lock-and-key uses IP extended access lists. You must have a solid understanding of how access lists are used to filter traffic, before you attempt to configure lock-and-key. Access lists are described in the chapter "Access Control Lists: Overview and Guidelines."

Lock-and-key employs user authentication and authorization as implemented in Cisco's authentication, authorization, and accounting (AAA) paradigm. You must understand how to configure AAA user authentication and authorization before you configure lock-and-key. User authentication and authorization is explained in the "Authentication, Authorization, and Accounting (AAA)" part of this document.

Lock-and-key uses the **autocommand** command, which you should understand. This command is described in the "Modem Support and Asynchronous Device Commands" chapter of the *Cisco IOS Dial Technologies Command Reference*.

Configuring Lock-and-Key

To configure lock-and-key, use the following commands beginning in global configuration mode. While completing these steps, be sure to follow the guidelines listed in the “[Lock-and-Key Configuration Guidelines](#)” section of this chapter.

	Command	Purpose
Step 1	Router(config)# access-list <i>access-list-number</i> [dynamic <i>dynamic-name</i> [timeout <i>minutes</i>]] { deny permit } telnet <i>source source-wildcard destination destination-wildcard</i> [precedence <i>precedence</i>] [tos <i>tos</i>] [established] [log]	Configures a dynamic access list, which serves as a template and placeholder for temporary access list entries.
Step 2	Router(config)# access-list dynamic-extend	(Optional) Extends the absolute timer of the dynamic ACL by six minutes when you open another Telnet session into the router to re-authenticate yourself using lock-and-key. Use this command if your job will run past the ACL’s absolute timer.
Step 3	Router(config)# interface <i>type number</i>	Configures an interface and enters interface configuration mode.
Step 4	Router(config-if)# ip access-group <i>access-list-number</i>	Applies the access list to the interface.
Step 5	Router(config-if)# exit	Exits interface configuration mode and enters global configuration mode.
Step 6	Router(config)# line vty <i>line-number</i> [<i>ending-line-number</i>]	Defines one or more virtual terminal (VTY) ports and enters line configuration mode. If you specify multiple VTY ports, they must all be configured identically because the software hunts for available VTY ports on a round-robin basis. If you do not want to configure all your VTY ports for lock-and-key access, you can specify a group of VTY ports for lock-and-key support only.
Step 7	Router(config-line)# login tacacs or Router(config-line)# password <i>password</i> or Router(config-line)# login local or Router(config-line)# exit then Router(config)# username <i>name</i> password <i>secret</i>	Configures user authentication in line or global configuration mode.
Step 8	Router(config-line)# autocommand access-enable [host] [timeout <i>minutes</i>] or Router(config)# autocommand access-enable [host] [timeout <i>minutes</i>]	Enables the creation of temporary access list entries in line or global configuration mode. If the optional host keyword is <i>not</i> specified, all hosts on the entire network are allowed to set up a temporary access list entry. The dynamic access list contains the network mask to enable the new network connection.

For an example of a lock-and-key configuration, see the section “[Lock-and-Key Configuration Examples](#)” later in this chapter.

Lock-and-Key Configuration Guidelines

Before you configure lock-and-key, you should understand the guidelines discussed in the following sections:

- [Dynamic Access Lists](#)
- [Lock-and-Key Authentication](#)
- [The autocommand Command](#)

Dynamic Access Lists

Use the following guidelines for configuring dynamic access lists:

- Do *not* create more than one dynamic access list for any one access list. The software only refers to the first dynamic access list defined.
- Do *not* assign the same *dynamic-name* to another access list. Doing so instructs the software to reuse the existing list. All named entries must be globally unique within the configuration.
- Assign attributes to the dynamic access list in the same way you assign attributes for a static access list. The temporary access list entries inherit the attributes assigned to this list.
- Configure Telnet as the protocol so that users must open a Telnet session into the router to be authenticated before they can gain access through the router.
- Either define an idle timeout now with the **timeout** keyword in the **access-enable** command in the **autocommand** command, or define an absolute timeout value later with the **access-list** command. You must define either an idle timeout or an absolute timeout—otherwise, the temporary access list entry will remain configured indefinitely on the interface (even after the user has terminated their session) until the entry is removed manually by an administrator. (You could configure both idle and absolute timeouts if you wish.)
- If you configure an idle timeout, the idle timeout value should be equal to the WAN idle timeout value.
- If you configure both idle and absolute timeouts, the idle timeout value must be less than the absolute timeout value.
- If you realize that a job will run past the ACL's absolute timer, use the **access-list dynamic-extend** command to extend the absolute timer of the dynamic ACL by six minutes. This command allows you to open a new Telnet session into the router to re-authentication yourself using lock-and-key.
- The only values replaced in the temporary entry are the source or destination address, depending whether the access list was in the input access list or output access list. All other attributes, such as port, are inherited from the main dynamic access list.
- Each addition to the dynamic list is always put at the beginning of the dynamic list. You cannot specify the order of temporary access list entries.
- Temporary access list entries are never written to NVRAM.
- To manually clear or to display dynamic access lists, refer to the section "[Maintaining Lock-and-Key](#)" later in this chapter.

Lock-and-Key Authentication

There are three possible methods to configure an authentication query process. These three methods are described in this section.

**Note**

Cisco recommends that you use the TACACS+ server for your authentication query process. TACACS+ provides authentication, authorization, and accounting services. It also provides protocol support, protocol specification, and a centralized security database. Using a TACACS+ server is described in the next section, “[Method 1—Configuring a Security Server](#).”

Method 1—Configuring a Security Server

Use a network access security server such as TACACS+ server. This method requires additional configuration steps on the TACACS+ server but allows for stricter authentication queries and more sophisticated tracking capabilities.

```
Router(config-line)# login tacacs
```

Method 2—Configuring the username Command

Use the **username** command. This method is more effective because authentication is determined on a user basis.

```
Router(config)# username name {nopassword | password {mutual-password | encryption-type encryption-password}}
```

Method 3—Configuring the password and login Commands

Use the **password** and **login** commands. This method is less effective because the password is configured for the port, not for the user. Therefore, any user who knows the password can authenticate successfully.

```
Router(config-line)# password password
Router(config-line)# login local
```

The autocommand Command

Use the following guidelines for configuring the **autocommand** command:

- If you use a TACACS+ server to authenticate the user, you should configure the **autocommand** command on the TACACS+ server as a per-user autocommand. If you use local authentication, use the **autocommand** command on the line.
- Configure all virtual terminal (VTY) ports with the same **autocommand** command. Omitting an **autocommand** command on a VTY port allows a random host to gain EXEC mode access to the router and does not create a temporary access list entry in the dynamic access list.
- If you did not previously define an idle timeout with the **autocommand access-enable** command, you must define an absolute timeout now with the **access-list** command. You must define either an idle timeout or an absolute timeout—otherwise, the temporary access list entry will remain configured indefinitely on the interface (even after the user has terminated their session) until the entry is removed manually by an administrator. (You could configure both idle and absolute timeouts if you wish.)
- If you configure both idle and absolute timeouts, the absolute timeout value must be greater than the idle timeout value.

Verifying Lock-and-Key Configuration

You can verify that lock-and-key is successfully configured on the router by asking a user to test the connection. The user should be at a host that is permitted in the dynamic access list, and the user should have AAA authentication and authorization configured.

To test the connection, the user should Telnet to the router, allow the Telnet session to close, and then attempt to access a host on the other side of the router. This host must be one that is permitted by the dynamic access list. The user should access the host with an application that uses the IP protocol.

The following sample display illustrates what end-users might see if they are successfully authenticated. Notice that the Telnet connection is closed immediately after the password is entered and authenticated. The temporary access list entry is then created, and the host that initiated the Telnet session now has access inside the firewall.

```
Router% telnet corporate
Trying 172.21.52.1 ...
Connected to corporate.example.com.
Escape character is '^]'.
User Access Verification
Password:Connection closed by foreign host.
```

You can then use the **show access-lists** command at the router to view the dynamic access lists, which should include an additional entry permitting the user access through the router.

Maintaining Lock-and-Key

When lock-and-key is in use, dynamic access lists will dynamically grow and shrink as entries are added and deleted. You need to make sure that entries are being deleted in a timely way, because while entries exist, the risk of a spoofing attack is present. Also, the more entries there are, the bigger the router performance impact will be.

If you do not have an idle or absolute timeout configured, entries will remain in the dynamic access list until you manually remove them. If this is the case, make sure that you are extremely vigilant about removing entries.

Displaying Dynamic Access List Entries

You can display temporary access list entries when they are in use. After a temporary access list entry is cleared by you or by the absolute or idle timeout parameter, it can no longer be displayed. The number of matches displayed indicates the number of times the access list entry was hit.

To view dynamic access lists and any temporary access list entries that are currently established, use the following command in privileged EXEC mode:

Command	Purpose
Router# show access-lists [<i>access-list-number</i>]	Displays dynamic access lists and temporary access list entries.

Manually Deleting Dynamic Access List Entries

To manually delete a temporary access list entry, use the following command in privileged EXEC mode:

Command	Purpose
Router# clear access-template [<i>access-list-number</i> <i>name</i>] [<i>dynamic-name</i>] [<i>source</i>] [<i>destination</i>]	Deletes a dynamic access list.

Lock-and-Key Configuration Examples

The following sections provide lock-and-key configuration examples:

- [Lock-and-Key with Local Authentication Example](#)
- [Lock-and-Key with TACACS+ Authentication Example](#)

Cisco recommends that you use a TACACS+ server for authentication, as shown in the second example.

Lock-and-Key with Local Authentication Example

This example shows how to configure lock-and-key access, with authentication occurring locally at the router. Lock-and-key is configured on the Ethernet 0 interface.

```
interface ethernet0
 ip address 172.18.23.9 255.255.255.0
 ip access-group 101 in

access-list 101 permit tcp any host 172.18.21.2 eq telnet
access-list 101 dynamic mytestlist timeout 120 permit ip any any

line vty 0
 login local
 autocommand access-enable timeout 5
```

The first access-list entry allows only Telnet into the router. The second access-list entry is always ignored until lock-and-key is triggered.

In the **access-list** command, the timeout is the absolute timeout. In this example, the lifetime of the mytestlist ACL is 120 minutes; that is, when a user logs in and enable the **access-enable** command, a dynamic ACL is created for 120 minutes (the maximum absolute time). The session is closed after 120 minutes, whether or not anyone is using it.

In the **autocommand** command, the timeout is the idle timeout. In this example, each time the user logs in or authenticates there is a 5-minute session. If there is no activity, the session closes in 5 minutes and the user has to reauthenticate. If the user uses the connection, the absolute time takes affect and the session closes in 120 minutes.

After a user opens a Telnet session into the router, the router will attempt to authenticate the user. If authentication is successful, the **autocommand** executes and the Telnet session terminates. The **autocommand** creates a temporary inbound access list entry at the Ethernet 0 interface, based on the second access-list entry (mytestlist). This temporary entry will expire after 5 minutes, as specified by the timeout.

Lock-and-Key with TACACS+ Authentication Example

The following example shows how to configure lock-and-key access, with authentication on a TACACS+ server. Lock-and-key access is configured on the BRI0 interface. Four VTY ports are defined with the password “cisco”.

```

aaa authentication login default group tacacs+ enable
aaa accounting exec stop-only group tacacs+
aaa accounting network stop-only group tacacs+
enable password ciscotac
!
isdn switch-type basic-dms100
!
interface ethernet0
ip address 172.18.23.9 255.255.255.0
!
interface BRI0
ip address 172.18.21.1 255.255.255.0
encapsulation ppp
dialer idle-timeout 3600
dialer wait-for-carrier-time 100
dialer map ip 172.18.21.2 name diana
dialer-group 1
isdn spid1 2036333715291
isdn spid2 2036339371566
ppp authentication chap
ip access-group 102 in
!
access-list 102 permit tcp any host 172.18.21.2 eq telnet
access-list 102 dynamic testlist timeout 5 permit ip any any
!
!
ip route 172.18.250.0 255.255.255.0 172.18.21.2
priority-list 1 interface BRI0 high
tacacs-server host 172.18.23.21
tacacs-server host 172.18.23.14
tacacs-server key test1
tftp-server rom alias all
!
dialer-list 1 protocol ip permit
!
line con 0
password cisco
line aux 0
line VTY 0 4
autocommand access-enable timeout 5
password cisco
!

```



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Configuring IP Session Filtering (Reflexive Access Lists)

This chapter describes how to configure reflexive access lists on your router. Reflexive access lists provide the ability to filter network traffic at a router, based on IP upper-layer protocol “session” information.

For a complete description of reflexive access list commands, refer to the “Reflexive Access List Commands” chapter of the *Cisco IOS Security Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the chapter “Identifying Supported Platforms” section in the “Using Cisco IOS Software.”

In This Chapter

This chapter has the following sections:

- [About Reflexive Access Lists](#)
- [Pework: Before You Configure Reflexive Access Lists](#)
- [Reflexive Access Lists Configuration Task List](#)
- [Reflexive Access List Configuration Examples](#)

About Reflexive Access Lists

Reflexive access lists allow IP packets to be filtered based on upper-layer session information. You can use reflexive access lists to permit IP traffic for sessions originating from within your network but to deny IP traffic for sessions originating from outside your network. This is accomplished by reflexive filtering, a kind of session filtering.

Reflexive access lists can be defined with extended named IP access lists only. You cannot define reflexive access lists with numbered or standard named IP access lists or with other protocol access lists.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

You can use reflexive access lists in conjunction with other standard access lists and static extended access lists.

This section has the following sections:

- [Benefits of Reflexive Access Lists](#)
- [What Is a Reflexive Access List?](#)
- [How Reflexive Access Lists Implement Session Filtering](#)
- [Where to Configure Reflexive Access Lists](#)
- [How Reflexive Access Lists Work](#)
- [Restrictions on Using Reflexive Access Lists](#)

Benefits of Reflexive Access Lists

Reflexive access lists are an important part of securing your network against network hackers, and can be included in a firewall defense. Reflexive access lists provide a level of security against spoofing and certain denial-of-service attacks. Reflexive access lists are simple to use, and, compared to basic access lists, provide greater control over which packets enter your network.

What Is a Reflexive Access List?

Reflexive access lists are similar in many ways to other access lists. Reflexive access lists contain condition statements (entries) that define criteria for permitting IP packets. These entries are evaluated in order, and when a match occurs, no more entries are evaluated.

However, reflexive access lists have significant differences from other types of access lists. Reflexive access lists contain only temporary entries; these entries are automatically created when a new IP session begins (for example, with an outbound packet), and the entries are removed when the session ends. Reflexive access lists are not themselves applied directly to an interface, but are “nested” within an extended named IP access list that is applied to the interface. (For more information about this, see the section “[Reflexive Access Lists Configuration Task List](#)” later in this chapter.) Also, reflexive access lists do not have the usual implicit “deny all traffic” statement at the end of the list, because of the nesting.

How Reflexive Access Lists Implement Session Filtering

This section compares session filtering with basic access lists to session filtering with reflexive access lists. This section contains the following sections:

- [With Basic Access Lists](#)
- [With Reflexive Access Lists](#)

With Basic Access Lists

With basic standard and static extended access lists, you can approximate session filtering by using the **established** keyword with the **permit** command. The **established** keyword filters TCP packets based on whether the ACK or RST bits are set. (Set ACK or RST bits indicate that the packet is not the first in the session, and therefore, that the packet belongs to an established session.) This filter criterion would be part of an access list applied permanently to an interface.

With Reflexive Access Lists

Reflexive access lists, however, provide a truer form of session filtering, which is much harder to spoof because more filter criteria must be matched before a packet is permitted through. (For example, source and destination addresses and port numbers are checked, not just ACK and RST bits.) Also, session filtering uses temporary filters which are removed when a session is over. This limits the hacker's attack opportunity to a smaller time window.

Moreover, the previous method of using the **established** keyword was available only for the TCP upper-layer protocol. So, for the other upper-layer protocols (such as UDP, ICMP, and so forth), you would have to either permit all incoming traffic or define all possible permissible source/destination host/port address pairs for each protocol. (Besides being an unmanageable task, this could exhaust NVRAM space.)

Where to Configure Reflexive Access Lists

Configure reflexive access lists on border routers—routers that pass traffic between an internal and external network. Often, these are firewall routers.



Note

In this chapter, the words “within your network” and “internal network” refer to a network that is controlled (secured), such as your organization's intranet, or to a part of your organization's internal network that has higher security requirements than another part. “Outside your network” and “external network” refer to a network that is uncontrolled (unsecured) such as the Internet or to a part of your organization's network that is not as highly secured.

How Reflexive Access Lists Work

A reflexive access list is triggered when a new IP upper-layer session (such as TCP or UDP) is initiated from inside your network, with a packet traveling to the external network. When triggered, the reflexive access list generates a new, temporary entry. This entry will permit traffic to enter your network if the traffic is part of the session, but will not permit traffic to enter your network if the traffic is not part of the session.

For example, if an outbound TCP packet is forwarded to outside of your network, and this packet is the first packet of a TCP session, then a new, temporary reflexive access list entry will be created. This entry is added to the reflexive access list, which applies to inbound traffic. The temporary entry has characteristics as described next.

This section contains the following sections:

- [Temporary Access List Entry Characteristics](#)
- [When the Session Ends](#)

Temporary Access List Entry Characteristics

- The entry is always a **permit** entry.
- The entry specifies the same protocol (TCP) as the original outbound TCP packet.
- The entry specifies the same source and destination addresses as the original outbound TCP packet, except the addresses are swapped.
- The entry specifies the same source and destination port numbers as the original outbound TCP packet, except the port numbers are swapped.
(This entry characteristic applies only for TCP and UDP packets. Other protocols, such as ICMP and IGMP, do not have port numbers, and other criteria are specified. For example, for ICMP, type numbers are used instead.)
- Inbound TCP traffic will be evaluated against the entry, until the entry expires. If an inbound TCP packet matches the entry, the inbound packet will be forwarded into your network.
- The entry will expire (be removed) after the last packet of the session passes through the interface.
- If no packets belonging to the session are detected for a configurable length of time (the timeout period), the entry will expire.

When the Session Ends

Temporary reflexive access list entries are removed at the end of the session. For TCP sessions, the entry is removed 5 seconds after two set FIN bits are detected, or immediately after matching a TCP packet with the RST bit set. (Two set FIN bits in a session indicate that the session is about to end; the 5-second window allows the session to close gracefully. A set RST bit indicates an abrupt session close.) Or, the temporary entry is removed after no packets of the session have been detected for a configurable length of time (the timeout period).

For UDP and other protocols, the end of the session is determined differently than for TCP. Because other protocols are considered to be connectionless (sessionless) services, there is no session tracking information embedded in packets. Therefore, the end of a session is considered to be when no packets of the session have been detected for a configurable length of time (the timeout period).

Restrictions on Using Reflexive Access Lists

Reflexive access lists do not work with some applications that use port numbers that change during a session. For example, if the port numbers for a return packet are different from the originating packet, the return packet will be denied, even if the packet is actually part of the same session.

The TCP application of FTP is an example of an application with changing port numbers. With reflexive access lists, if you start an FTP request from within your network, the request will not complete. Instead, you must use Passive FTP when originating requests from within your network.

Prework: Before You Configure Reflexive Access Lists

Before you configure reflexive access lists, you must decide whether to configure reflexive access lists on an internal or external interface, as described in the next section, “[Choosing an Interface: Internal or External](#).”

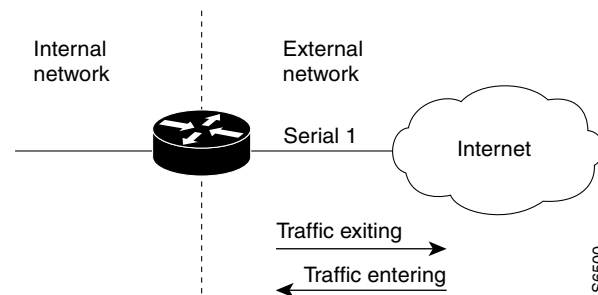
You should also be sure that you have a basic understanding of the IP protocol and of access lists; specifically, you should know how to configure extended named IP access lists. To learn about configuring IP extended access lists, refer to the “Configuring IP Services” chapter of the *Cisco IOS IP Configuration Guide*.

Choosing an Interface: Internal or External

Reflexive access lists are most commonly used with one of two basic network topologies. Determining which of these topologies is most like your own can help you decide whether to use reflexive access lists with an internal interface or with an external interface (the interface connecting to an internal network, or the interface connecting to an external network).

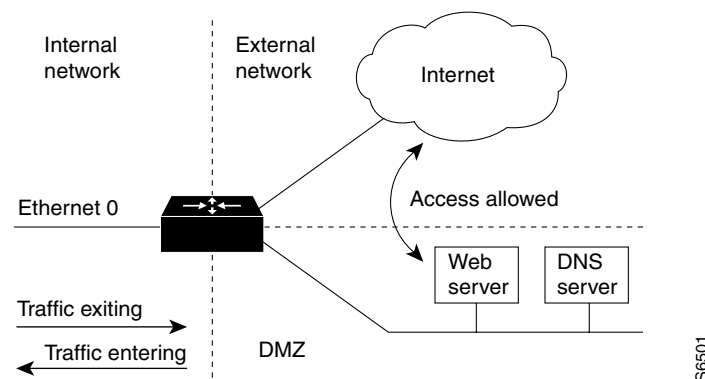
The first topology is shown in [Figure 18](#). In this simple topology, reflexive access lists are configured for the *external* interface Serial 1. This prevents IP traffic from entering the router and the internal network, unless the traffic is part of a session already established from within the internal network.

Figure 18 Simple Topology—Reflexive Access Lists Configured at the External Interface



The second topology is shown in [Figure 19](#). In this topology, reflexive access lists are configured for the *internal* interface Ethernet 0. This allows external traffic to access the services in the Demilitarized Zone (DMZ), such as DNS services, but prevents IP traffic from entering your internal network—unless the traffic is part of a session already established from within the internal network.

Figure 19 DMZ Topology—Reflexive Access Lists Configured at the Internal Interface



Use these two example topologies to help you decide whether to configure reflexive access lists for an internal or external interface.

Reflexive Access Lists Configuration Task List

In the previous section, “[Prework: Before You Configure Reflexive Access Lists](#),” you decided whether to configure reflexive access lists for an internal or external interface.

Now, complete the tasks in one of the following configuration task lists:

- [External Interface Configuration Task List](#)
- [Internal Interface Configuration Task List](#)

For configuration examples, refer to the “[Reflexive Access List Configuration Examples](#)” section at the end of this chapter.

External Interface Configuration Task List

To configure reflexive access lists for an external interface, perform the following tasks:

1. Defining the reflexive access list(s) in an *outbound* IP extended named access list
2. Nesting the reflexive access list(s) in an *inbound* IP extended named access list
3. Setting a global timeout value

These tasks are described in the sections following the “[Internal Interface Configuration Task List](#)” section.

**Note**

The defined (outbound) reflexive access list evaluates traffic traveling out of your network: if the defined reflexive access list is matched, temporary entries are created in the nested (inbound) reflexive access list. These temporary entries will then be applied to traffic traveling into your network.

Internal Interface Configuration Task List

To configure reflexive access lists for an internal interface, perform the following tasks:

1. Defining the reflexive access list(s) in an *inbound* IP extended named access list
2. Nesting the reflexive access list(s) in an *outbound* IP extended named access list
3. Setting a global timeout value

These tasks are described in the next sections.

**Note**

The defined (inbound) reflexive access list is used to evaluate traffic traveling out of your network: if the defined reflexive access list is matched, temporary entries are created in the nested (outbound) reflexive access list. These temporary entries will then be applied to traffic traveling into your network.

Defining the Reflexive Access List(s)

To define a reflexive access list, you use an entry in an extended named IP access list. This entry must use the **reflect** keyword.

- If you are configuring reflexive access lists for an external interface, the extended named IP access list should be one that is applied to outbound traffic.

- If you are configuring reflexive access lists for an internal interface, the extended named IP access list should be one that is applied to inbound traffic.

To define reflexive access lists, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# ip access-list extended <i>name</i>	External interface: Specifies the outbound access list. or Internal interface: Specifies the inbound access list. (This command enters access-list configuration mode.)
Step 2	Router(config-ext-nacl)# permit <i>protocol any any</i> reflect <i>name [timeout seconds]</i>	Defines the reflexive access list using the reflexive permit entry. Repeat this step for each IP upper-layer protocol; for example, you can define reflexive filtering for TCP sessions and also for UDP sessions. You can use the same <i>name</i> for multiple protocols. For additional guidelines for this task, see the following section, “ Mixing Reflexive Access List Statements with Other Permit and Deny Entries .”

If the extended named IP access list you just specified has never been applied to the interface, you must also apply the extended named IP access list to the interface.

To apply the extended named IP access list to the interface, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# ip access-group <i>name out</i>	External interface: Applies the extended access list to the interface’s outbound traffic.
or	
Router(config-if)# ip access-group <i>name in</i>	Internal interface: Applies the extended access list to the interface’s inbound traffic.

Mixing Reflexive Access List Statements with Other Permit and Deny Entries

The extended IP access list that contains the reflexive access list **permit** statement can also contain other normal **permit** and **deny** statements (entries). However, as with all access lists, the order of entries is important, as explained in the next few paragraphs.

If you configure reflexive access lists for an external interface, when an outbound IP packet reaches the interface, the packet will be evaluated sequentially by each entry in the outbound access list until a match occurs.

If the packet matches an entry prior to the reflexive **permit** entry, the packet will not be evaluated by the reflexive **permit** entry, and no temporary entry will be created for the reflexive access list (reflexive filtering will not be triggered).

The outbound packet will be evaluated by the reflexive **permit** entry only if no other match occurs first. Then, if the packet matches the protocol specified in the reflexive **permit** entry, the packet is forwarded out of the interface and a corresponding temporary entry is created in the inbound reflexive access list (unless the corresponding entry already exists, indicating the outbound packet belongs to a session in progress). The temporary entry specifies criteria that permits inbound traffic only for the same session.

Nesting the Reflexive Access List(s)

After you define a reflexive access list in one IP extended access list, you must “nest” the reflexive access list within a different extended named IP access list.

- If you are configuring reflexive access lists for an external interface, nest the reflexive access list within an extended named IP access list applied to inbound traffic.
- If you are configuring reflexive access lists for an internal interface, nest the reflexive access list within an extended named IP access list applied to outbound traffic.

After you nest a reflexive access list, packets heading into your internal network can be evaluated against any reflexive access list temporary entries, along with the other entries in the extended named IP access list.

To nest reflexive access lists, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# ip access-list extended <i>name</i>	External interface: Specifies the inbound access list. or Internal interface: Specifies the outbound access list. (This command enters access-list configuration mode.)
Step 2	Router(config-ext-nacl)# evaluate <i>name</i>	Adds an entry that “points” to the reflexive access list. Adds an entry for each reflexive access list <i>name</i> previously defined.

Again, the order of entries is important. Normally, when a packet is evaluated against entries in an access list, the entries are evaluated in sequential order, and when a match occurs, no more entries are evaluated. With a reflexive access list nested in an extended access list, the extended access list entries are evaluated sequentially up to the nested entry, then the reflexive access list entries are evaluated sequentially, and then the remaining entries in the extended access list are evaluated sequentially. As usual, after a packet matches *any* of these entries, no more entries will be evaluated.

If the extended named IP access list you just specified has never been applied to the interface, you must also apply the extended named IP access list to the interface.

To apply the extended named IP access list to the interface, use one of the following commands in interface configuration mode:

Command	Purpose
Router(config-if)# ip access-group <i>name</i> in	External interface: Applies the extended access list to the interface's inbound traffic.
OR	
Router(config-if)# ip access-group <i>name</i> out	Internal interface: Applies the extended access list to the interface's outbound traffic.

Setting a Global Timeout Value

Reflexive access list entries expire after no packets in the session have been detected for a certain length of time (the “timeout” period). You can specify the timeout for a particular reflexive access list when you define the reflexive access list. But if you do not specify the timeout for a given reflexive access list, the list will use the global timeout value instead.

The global timeout value is 300 seconds by default. But, you can change the global timeout to a different value at any time.

To change the global timeout value, use the following command in global configuration mode:

Command	Purpose
Router(config)# ip reflexive-list timeout <i>seconds</i>	Changes the global timeout value for temporary reflexive access list entries. Use a positive integer from 0 to 2,147,483.

Reflexive Access List Configuration Examples

The following sections provide reflexive access list configuration examples:

- [External Interface Configuration Example](#)
- [Internal Interface Configuration Example](#)

External Interface Configuration Example

This example shows reflexive access lists configured for an external interface, for a topology similar to the one in [Figure 18](#) (shown earlier in this chapter).

This configuration example permits both inbound and outbound TCP traffic at interface Serial 1, but only if the first packet (in a given session) originated from inside your network. The interface Serial 1 connects to the Internet.

Define the interface where the session-filtering configuration is to be applied:

```
interface serial 1
description Access to the Internet via this interface
```

Apply access lists to the interface, for inbound traffic and for outbound traffic:

```
ip access-group inboundfilters in
ip access-group outboundfilters out
```

Define the outbound access list. This is the access list that evaluates all outbound traffic on interface Serial 1.

```
ip access-list extended outboundfilters
```

Define the reflexive access list *tcptraffic*. This entry permits *all* outbound TCP traffic and creates a new access list named *tcptraffic*. Also, when an outbound TCP packet is the first in a new session, a corresponding temporary entry will be automatically created in the reflexive access list *tcptraffic*.

```
permit tcp any any reflect tcptraffic
```

Define the inbound access list. This is the access list that evaluates all inbound traffic on interface Serial 1.

```
ip access-list extended inboundfilters
```

Define the inbound access list entries. This example shows Enhanced IGRP permitted on the interface. Also, no ICMP traffic is permitted. The last entry points to the reflexive access list. If a packet does not match the first two entries, the packet will be evaluated against all the entries in the reflexive access list *tcptraffic*.

```
permit eigrp any any
deny icmp any any
evaluate tcptraffic
```

Define the global idle timeout value for all reflexive access lists. In this example, when the reflexive access list *tcptraffic* was defined, no timeout was specified, so *tcptraffic* uses the global timeout. Therefore, if for 120 seconds there is no TCP traffic that is part of an established session, the corresponding reflexive access list entry will be removed.

```
ip reflexive-list timeout 120
```

The example configuration looks as follows:

```
interface Serial 1
description Access to the Internet via this interface
ip access-group inboundfilters in
ip access-group outboundfilters out
!
ip reflexive-list timeout 120
!
ip access-list extended outboundfilters
permit tcp any any reflect tcptraffic
!
ip access-list extended inboundfilters
permit eigrp any any
deny icmp any any
evaluate tcptraffic
```

With this configuration, before any TCP sessions have been initiated the **show access-list EXEC** command displays the following:

```
Extended IP access list inboundfilters
permit eigrp any any
deny icmp any any
evaluate tcptraffic
Extended IP access list outboundfilters
permit tcp any any reflect tcptraffic
```

Notice that the reflexive access list does not appear in this output. This is because before any TCP sessions have been initiated, no traffic has triggered the reflexive access list, and the list is empty (has no entries). When empty, reflexive access lists do not show up in **show access-list** output.

After a Telnet connection is initiated from within your network to a destination outside of your network, the **show access-list EXEC** command displays the following:

```
Extended IP access list inboundfilters
  permit eigrp any any
  deny icmp any any
  evaluate tcptraffic
Extended IP access list outboundfilters
  permit tcp any any reflect tcptraffic
Reflexive IP access list tcptraffic
  permit tcp host 172.19.99.67 eq telnet host 192.168.60.185 eq 11005 (5 matches) (time
left 115 seconds)
```

Notice that the reflexive access list *tcptraffic* now appears and displays the temporary entry generated when the Telnet session initiated with an outbound packet.

Internal Interface Configuration Example

This is an example configuration for reflexive access lists configured for an internal interface. This example has a topology similar to the one in [Figure 19](#) (shown earlier in this chapter).

This example is similar to the previous example; the only difference between this example and the previous example is that the entries for the outbound and inbound access lists are swapped. Please refer to the previous example for more details and descriptions.

```
interface Ethernet 0
  description Access from the I-net to our Internal Network via this interface
  ip access-group inboundfilters in
  ip access-group outboundfilters out
  !
ip reflexive-list timeout 120
!
ip access-list extended outboundfilters
  permit eigrp any any
  deny icmp any any
  evaluate tcptraffic
!
ip access-list extended inboundfilters
  permit tcp any any reflect tcptraffic
```

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Configuring TCP Intercept (Preventing Denial-of-Service Attacks)

Feature History

Release	Modification
Cisco IOS	For information about feature support in Cisco IOS software, use Cisco Feature Navigator.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

This chapter describes how to configure your router to protect TCP servers from TCP SYN-flooding attacks, a type of denial-of-service attack. This is accomplished by configuring the Cisco IOS feature known as TCP Intercept.

For a complete description of TCP Intercept commands, refer to the “TCP Intercept Commands” chapter of the *Cisco IOS Security Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the chapter “Identifying Supported Platforms” section in the “Using Cisco IOS Software.”

In This Chapter

This chapter has the following sections:

- [About TCP Intercept](#)
- [TCP Intercept Configuration Task List](#)
- [TCP Intercept Configuration Example](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

About TCP Intercept

The TCP intercept feature implements software to protect TCP servers from TCP SYN-flooding attacks, which are a type of denial-of-service attack.

A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection. Because these messages have unreachable return addresses, the connections cannot be established. The resulting volume of unresolved open connections eventually overwhelms the server and can cause it to deny service to valid requests, thereby preventing legitimate users from connecting to a web site, accessing e-mail, using FTP service, and so on.

The TCP intercept feature helps prevent SYN-flooding attacks by intercepting and validating TCP connection requests. In intercept mode, the TCP intercept software intercepts TCP synchronization (SYN) packets from clients to servers that match an extended access list. The software establishes a connection with the client on behalf of the destination server, and if successful, establishes the connection with the server on behalf of the client and knits the two half-connections together transparently. Thus, connection attempts from unreachable hosts will never reach the server. The software continues to intercept and forward packets throughout the duration of the connection. The number of SYNs per second and the number of concurrent connections proxied depends on the platform, memory, processor, and other factors.

In the case of illegitimate requests, the software's aggressive timeouts on half-open connections and its thresholds on TCP connection requests protect destination servers while still allowing valid requests.

When establishing your security policy using TCP intercept, you can choose to intercept all requests or only those coming from specific networks or destined for specific servers. You can also configure the connection rate and threshold of outstanding connections.

You can choose to operate TCP intercept in watch mode, as opposed to intercept mode. In watch mode, the software passively watches the connection requests flowing through the router. If a connection fails to get established in a configurable interval, the software intervenes and terminates the connection attempt.

TCP options that are negotiated on handshake (such as RFC 1323 on window scaling) will not be negotiated because the TCP intercept software does not know what the server can do or will negotiate.

TCP Intercept Configuration Task List

To configure TCP intercept, perform the tasks in the following sections. The first task is required; the rest are optional.

- [Enabling TCP Intercept](#) (Required)
- [Setting the TCP Intercept Mode](#) (Optional)
- [Setting the TCP Intercept Drop Mode](#) (Optional)
- [Changing the TCP Intercept Timers](#) (Optional)
- [Changing the TCP Intercept Aggressive Thresholds](#) (Optional)
- [Monitoring and Maintaining TCP Intercept](#) (Optional)

For TCP intercept configuration examples using the commands in this chapter, refer to the “[TCP Intercept Configuration Example](#)” section at the end of this chapter.

Enabling TCP Intercept

To enable TCP intercept, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# access-list <i>access-list-number</i> { deny permit } tcp any <i>destination destination-wildcard</i>	Defines an IP extended access list.
Step 2	Router(config)# ip tcp intercept list <i>access-list-number</i>	Enables TCP intercept.

You can define an access list to intercept all requests or only those coming from specific networks or destined for specific servers. Typically the access list will define the source as **any** and define specific destination networks or servers. That is, you do not attempt to filter on the source addresses because you do not necessarily know who to intercept packets from. You identify the destination in order to protect destination servers.

If no access list match is found, the router allows the request to pass with no further action.

Setting the TCP Intercept Mode

The TCP intercept can operate in either active intercept mode or passive watch mode. The default is intercept mode.

In intercept mode, the software actively intercepts each incoming connection request (SYN) and responds on behalf of the server with an SYN-ACK, then waits for an ACK from the client. When that ACK is received, the original SYN is sent to the server and the software performs a three-way handshake with the server. When this is complete, the two half-connections are joined.

In watch mode, connection requests are allowed to pass through the router to the server but are watched until they become established. If they fail to become established within 30 seconds (configurable with the **ip tcp intercept watch-timeout** command), the software sends a Reset to the server to clear up its state.

To set the TCP intercept mode, use the following command in global configuration mode:

Command	Purpose
Router(config)# ip tcp intercept mode { intercept watch }	Sets the TCP intercept mode.

Setting the TCP Intercept Drop Mode

When under attack, the TCP intercept feature becomes more aggressive in its protective behavior. If the number of incomplete connections exceeds 1100 or the number of connections arriving in the last one minute exceeds 1100, each new arriving connection causes the oldest partial connection to be deleted. Also, the initial retransmission timeout is reduced by half to 0.5 seconds (so the total time trying to establish a connection is cut in half).

By default, the software drops the oldest partial connection. Alternatively, you can configure the software to drop a random connection. To set the drop mode, use the following command in global configuration mode:

Command	Purpose
Router(config)# ip tcp intercept drop-mode {oldest random}	Sets the drop mode.

Changing the TCP Intercept Timers

By default, the software waits for 30 seconds for a watched connection to reach established state before sending a Reset to the server. To change this value, use the following command in global configuration mode:

Command	Purpose
Router(config)# ip tcp intercept watch-timeout <i>seconds</i>	Changes the time allowed to reach established state.

By default, the software waits for 5 seconds from receipt of a reset or FIN-exchange before it ceases to manage the connection. To change this value, use the following command in global configuration mode:

Command	Purpose
Router(config)# ip tcp intercept finrst-timeout <i>seconds</i>	Changes the time between receipt of a reset or FIN-exchange and dropping the connection.

By default, the software still manages a connection for 24 hours after no activity. To change this value, use the following command in global configuration mode:

Command	Purpose
Router(config)# ip tcp intercept connection-timeout <i>seconds</i>	Changes the time the software will manage a connection after no activity.

Changing the TCP Intercept Aggressive Thresholds

Two factors determine when aggressive behavior begins and ends: total incomplete connections and connection requests during the last one-minute sample period. Both thresholds have default values that can be redefined.

When a threshold is exceeded, the TCP intercept assumes the server is under attack and goes into aggressive mode. When in aggressive mode, the following occurs:

- Each new arriving connection causes the oldest partial connection to be deleted. (You can change to a random drop mode.)
- The initial retransmission timeout is reduced by half to 0.5 seconds, and so the total time trying to establish the connection is cut in half. (When not in aggressive mode, the code does exponential back-off on its retransmissions of SYN segments. The initial retransmission timeout is 1 second. The subsequent timeouts are 2 seconds, 4 seconds, 8 seconds, and 16 seconds. The code retransmits 4 times before giving up, so it gives up after 31 seconds of no acknowledgment.)
- If in watch mode, the watch timeout is reduced by half. (If the default is in place, the watch timeout becomes 15 seconds.)

The drop strategy can be changed from the oldest connection to a random connection with the **ip tcp intercept drop-mode** command.

**Note**

The two factors that determine aggressive behavior are related and work together. When *either* of the **high** values is exceeded, aggressive behavior begins. When *both* quantities fall below the **low** value, aggressive behavior ends.

You can change the threshold for triggering aggressive mode based on the total number of incomplete connections. The default values for **low** and **high** are 900 and 1100 incomplete connections, respectively. To change these values, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# ip tcp intercept max-incomplete low number	Sets the threshold for stopping aggressive mode.
Step 2	Router(config)# ip tcp intercept max-incomplete high number	Sets the threshold for triggering aggressive mode.

You can also change the threshold for triggering aggressive mode based on the number of connection requests received in the last 1-minute sample period. The default values for **low** and **high** are 900 and 1100 connection requests, respectively. To change these values, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# ip tcp intercept one-minute low number	Sets the threshold for stopping aggressive mode.
Step 2	Router(config)# ip tcp intercept one-minute high number	Sets the threshold for triggering aggressive mode.

Monitoring and Maintaining TCP Intercept

To display TCP intercept information, use either of the following commands in EXEC mode:

Command	Purpose
Router# show tcp intercept connections	Displays incomplete connections and established connections.
Router# show tcp intercept statistics	Displays TCP intercept statistics.

TCP Intercept Configuration Example

The following configuration defines extended IP access list 101, causing the software to intercept packets for all TCP servers on the 192.168.1.0/24 subnet:

```
ip tcp intercept list 101
!
access-list 101 permit tcp any 192.168.1.0 0.0.0.255
```



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Context-Based Access Control



Configuring Context-Based Access Control

This chapter describes how to configure Context-based Access Control (CBAC). CBAC provides advanced traffic filtering functionality and can be used as an integral part of your network's firewall. For more information regarding firewalls, refer to the chapter "Cisco IOS Firewall Overview."

For a complete description of the CBAC commands used in this chapter, refer to the "Context-Based Access Control Commands" chapter in the *Cisco IOS Security Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the chapter "Identifying Supported Platforms" section in the "Using Cisco IOS Software."

In This Chapter

This chapter has the following sections:

- [About Context-Based Access Control](#)
- [CBAC Configuration Task List](#)
- [Monitoring and Maintaining CBAC](#)
- [CBAC Configuration Examples](#)

About Context-Based Access Control

This section describes CBAC features and functions:

- [What CBAC Does](#)
- [What CBAC Does Not Do](#)
- [How CBAC Works](#)
- [When and Where to Configure CBAC](#)
- [The CBAC Process](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Supported Protocols](#)
- [Restrictions](#)
- [Memory and Performance Impact](#)

What CBAC Does

CBAC works to provide network protection on multiple levels using the following functions:

- [Traffic Filtering](#)
- [Traffic Inspection](#)
- [Alerts and Audit Trails](#)
- [Intrusion Prevention](#)

Traffic Filtering

CBAC intelligently filters TCP and UDP packets based on application-layer protocol session information. You can configure CBAC to permit specified TCP and UDP traffic through a firewall only when the connection is initiated from within the network you want to protect. CBAC can inspect traffic for sessions that originate from either side of the firewall, and CBAC can be used for intranet, extranet, and Internet perimeters of your network.

Without CBAC, traffic filtering is limited to access list implementations that examine packets at the network layer, or at most, the transport layer. However, CBAC examines not only network layer and transport layer information but also examines the application-layer protocol information (such as FTP connection information) to learn about the state of the session. This allows support of protocols that involve multiple channels created as a result of negotiations in the control channel. Most of the multimedia protocols as well as some other protocols (such as FTP, RPC, and SQL*Net) involve multiple channels.

Using CBAC, Java blocking can be configured to filter HTTP traffic based on the server address or to completely deny access to Java applets that are not embedded in an archived or compressed file. With Java, you must protect against the risk of users inadvertently downloading destructive applets into your network. To protect against this risk, you could require all users to disable Java in their browser. If this is not an acceptable solution, you can create a CBAC inspection rule to filter Java applets at the firewall, which allows users to download only applets residing within the firewall and trusted applets from outside the firewall. For extensive content filtering of Java, Active-X, or virus scanning, you might want to consider purchasing a dedicated content filtering product.

Traffic Inspection

CBAC inspects traffic that travels through the firewall to discover and manage state information for TCP and UDP sessions. This state information is used to create temporary openings in the firewall's access lists to allow return traffic and additional data connections for permissible sessions.

Inspecting packets at the application layer, and maintaining TCP and UDP session information, provides CBAC with the ability to detect and prevent certain types of network attacks such as SYN-flooding. A SYN-flood attack occurs when a network attacker floods a server with a barrage of requests for connection and does not complete the connection. The resulting volume of half-open connections can overwhelm the server, causing it to deny service to valid requests. Network attacks that deny access to a network device are called denial-of-service (DoS) attacks.

CBAC helps to protect against DoS attacks in other ways. CBAC inspects packet sequence numbers in TCP connections to see if they are within expected ranges—CBAC drops any suspicious packets. You can also configure CBAC to drop half-open connections, which require firewall processing and memory resources to maintain. Additionally, CBAC can detect unusually high rates of new connections and issue alert messages.

CBAC can help by protecting against certain DoS attacks involving fragmented IP packets. Even though the firewall prevents an attacker from making actual connections to a given host, the attacker can disrupt services provided by that host. This is done by sending many non-initial IP fragments or by sending complete fragmented packets through a router with an ACL that filters the first fragment of a fragmented packet. These fragments can tie up resources on the target host as it tries to reassemble the incomplete packets.

Alerts and Audit Trails

CBAC also generates real-time alerts and audit trails. Enhanced audit trail features use SYSLOG to track all network transactions; recording time stamps, source host, destination host, ports used, and the total number of transmitted bytes, for advanced, session-based reporting. Real-time alerts send SYSLOG error messages to central management consoles upon detecting suspicious activity. Using CBAC inspection rules, you can configure alerts and audit trail information on a per-application protocol basis. For example, if you want to generate audit trail information for HTTP traffic, you can specify that in the CBAC rule covering HTTP inspection.

Intrusion Prevention

CBAC provides a limited amount of intrusion detection to protect against specific SMTP attacks. With intrusion detection, SYSLOG messages are reviewed and monitored for specific “attack signatures.” Certain types of network attacks have specific characteristics, or signatures. When CBAC detects an attacks, it resets the offending connections and sends SYSLOG information to the SYSLOG server. Refer to the section [“Interpreting Syslog and Console Messages Generated by CBAC”](#) later in this chapter for a list of supported signatures.

In addition to the limited intrusion detection offered by CBAC, the Cisco IOS Firewall feature set offers intrusion detection technology for mid-range and high-end router platforms using the Cisco IOS Intrusion Prevention System (IPS). Cisco IOS IPS restructures and replaces the existing Cisco IOS Intrusion Detection System (IDS). It is ideal for any network perimeter, and especially for locations in which a router is being deployed and additional security between network segments is required. It also can protect intranet and extranet connections where additional security is mandated, and branch-office sites connecting to the corporate office or Internet.

The Cisco IOS IPS acts as an in-line intrusion detection sensor, watching packets and sessions as they flow through the router and scanning each packet to match any of the Cisco IOS IPS signatures. When Cisco IOS IPS detects suspicious activity, it responds before network security can be compromised and logs the event through Cisco IOS syslog messages or Security Device Event Exchange (SDEE).

For more information about Cisco IOS IPS, refer to the module “Configuring Cisco IOS Intrusion Prevention System (IPS).”

What CBAC Does Not Do

CBAC does not provide intelligent filtering for all protocols; it only works for the protocols that you specify. If you do not specify a certain protocol for CBAC, the existing access lists will determine how that protocol is filtered. No temporary openings will be created for protocols not specified for CBAC inspection.

CBAC does not protect against attacks originating from within the protected network unless that traffic travels through a router that has the Cisco IOS Firewall feature set deployed on it. CBAC only detects and protects against attacks that travel through the firewall. This is a scenario in which you might want to deploy CBAC on an intranet-based router.

CBAC protects against certain types of attacks, but not every type of attack. CBAC should not be considered a perfect, impenetrable defense. Determined, skilled attackers might be able to launch effective attacks. While there is no such thing as a perfect defense, CBAC detects and prevents most of the popular attacks on your network.

How CBAC Works

You should understand the material in this section before you configure CBAC. If you do not understand how CBAC works, you might inadvertently introduce security risks by configuring CBAC inappropriately. This section contains the following sections:

- [How CBAC Works—Overview](#)
- [How CBAC Works—Details](#)

How CBAC Works—Overview

CBAC creates temporary openings in access lists at firewall interfaces. These openings are created when specified traffic exits your internal network through the firewall. The openings allow returning traffic (that would normally be blocked) and additional data channels to enter your internal network back through the firewall. The traffic is allowed back through the firewall only if it is part of the same session as the original traffic that triggered CBAC when exiting through the firewall.

Throughout this chapter, the terms “inbound” and “outbound” are used to describe the direction of traffic relative to the router interface on which CBAC is applied. For example, if a CBAC rule is applied inbound on interface E0, then packets entering interface E0 from the network will be inspected. If a CBAC rule is applied outbound on interface E0, then packets leaving interface E0 to the network will be inspected. This is similar to the way ACLs work.

For example, consider a CBAC inspection rule named *hqusers*, and suppose that rule is applied inbound at interface E0:

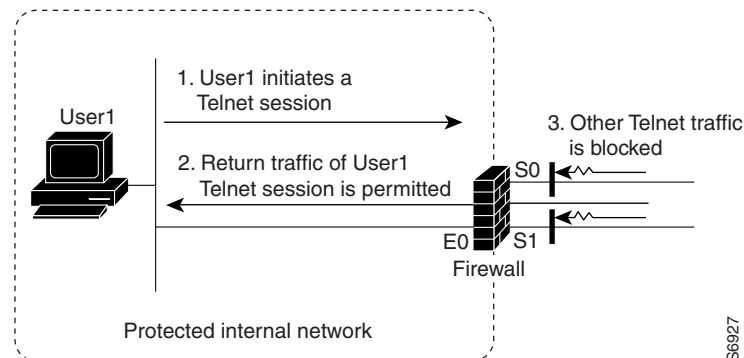
```
router (config-if)# ip inspect hqusers in
```

This command causes CBAC to inspect the packets coming into this interface from the network. If a packet is attempting to initiate a session, CBAC will then determine if this protocol is allowed, create a CBAC session, add the appropriate ACLs to allow return traffic and do any needed content inspection on any future packets for this session.

The terms “input” and “output” are used to describe the interfaces at which network traffic enters or exits the firewall router. A packet enters the firewall router via the input interface, is inspected by the firewall software and then exits the router via the output interface.

In [Figure 20](#), the inbound access lists at S0 and S1 are configured to block Telnet traffic, and there is no outbound access list configured at E0. When the connection request for User1's Telnet session passes through the firewall, CBAC creates a temporary opening in the inbound access list at S0 to permit returning Telnet traffic for User1's Telnet session. (If the same access list is applied to both S0 and S1, the same opening would appear at both interfaces.) If necessary, CBAC would also have created a similar opening in an outbound access list at E0 to permit return traffic.

Figure 20 *CBAC Opens Temporary Holes in Firewall Access Lists*



How CBAC Works—Details

This section describes how CBAC inspects packets and maintains state information about sessions to provide intelligent filtering.

Packets Are Inspected

With CBAC, you specify which protocols you want to be inspected, and you specify an interface and interface direction (in or out) where inspection originates. Only specified protocols will be inspected by CBAC.

Packets entering the firewall are inspected by CBAC only if they first pass the inbound access list at the input interface and outbound access list at the output interface. If a packet is denied by the access list, the packet is simply dropped and not inspected by CBAC.

CBAC inspection tracks sequence numbers in all TCP packets, and drops those packets with sequence numbers that are not within expected ranges.

CBAC inspection recognizes application-specific commands (such as illegal SMTP commands) in the control channel, and detects and prevents certain application-level attacks.

When CBAC suspects an attack, the DoS feature can take several actions:

- Generate alert messages
- Protect system resources that could impede performance
- Block packets from suspected attackers

CBAC uses timeout and threshold values to manage session state information, helping to determine when to drop sessions that do not become fully established. Setting timeout values for network sessions helps prevent DoS attacks by freeing up system resources, dropping sessions after a specified amount of time. Setting threshold values for network sessions helps prevent DoS attacks by controlling the number of half-open sessions, which limits the amount of system resources applied to half-open sessions. When a

session is dropped, CBAC sends a reset message to the devices at both end points (source and destination) of the session. When the system under DoS attack receives a reset command, it releases, or frees up, processes and resources related to that incomplete session.

CBAC provides three thresholds against DoS attacks:

- The total number of half-open TCP or UDP sessions
- The number of half-open sessions based upon time
- The number of half-open TCP-only sessions per host

If a threshold is exceeded, CBAC has two options:

- Send a reset message to the end points of the oldest half-open session, making resources available to service newly arriving SYN packets.
- In the case of half open TCP only sessions, CBAC blocks all SYN packets temporarily for the duration configured by the threshold value. When the router blocks a SYN packet, the TCP three-way handshake is never initiated, which prevents the router from using memory and processing resources needed for valid connections.

DoS detection and prevention requires that you create a CBAC inspection rule and apply that rule on an interface. The inspection rule must include the protocols that you want to monitor against DoS attacks. For example, if you have TCP inspection enabled on the inspection rule, then CBAC can track all TCP connections to watch for DoS attacks. If the inspection rule includes FTP protocol inspection but not TCP inspection, CBAC tracks only FTP connections for DoS attacks.

For detailed information about setting timeout and threshold values in CBAC to detect and prevent DoS attacks, refer in the [“Configuring Global Timeouts and Thresholds”](#) section.

A State Table Maintains Session State Information

Whenever a packet is inspected, a state table is updated to include information about the state of the session.

Return traffic will only be permitted back through the firewall if the state table contains information indicating that the packet belongs to a permissible session. CBAC controls the traffic that belongs to a valid session. When return traffic is inspected, the state table information is updated as necessary.

UDP “Sessions” Are Approximated

With UDP—a connectionless service—there are no actual sessions, so the software approximates sessions by examining the information in the packet and determining if the packet is similar to other UDP packets (for example, same source/destination addresses and port numbers) and if the packet was detected soon after another similar UDP packet. “Soon” means within the configurable UDP idle timeout period.

Access List Entries Are Dynamically Created and Deleted to Permit Return Traffic and Additional Data Connections

CBAC dynamically creates and deletes access list entries at the firewall interfaces, according to the information maintained in the state tables. These access list entries are applied to the interfaces to examine traffic flowing back into the internal network. These entries create temporary openings in the firewall to permit only traffic that is part of a permissible session.

The temporary access list entries are never saved to NVRAM.

When and Where to Configure CBAC

Configure CBAC at firewalls protecting internal networks. Such firewalls should be Cisco routers with the Cisco IOS Firewall feature set configured as described previously in the section “Cisco IOS Firewall.”

Use CBAC when the firewall will be passing traffic such as the following:

- Standard TCP and UDP Internet applications
- Multimedia applications
- Oracle support

Use CBAC for these applications if you want the application’s traffic to be permitted through the firewall only when the traffic session is initiated from a particular side of the firewall (usually from the protected internal network).

In many cases, you will configure CBAC in one direction only at a single interface, which causes traffic to be permitted back into the internal network only if the traffic is part of a permissible (valid, existing) session. This is a typical configuration for protecting your internal networks from traffic that originates on the Internet.

You can also configure CBAC in two directions at one or more interfaces. CBAC is configured in two directions when the networks on both sides of the firewall should be protected, such as with extranet or intranet configurations, and to protect against DoS attacks. For example, if the firewall is situated between two partner companies’ networks, you might wish to restrict traffic in one direction for certain applications, and restrict traffic in the opposite direction for other applications.

The CBAC Process

This section describes a sample sequence of events that occurs when CBAC is configured at an external interface that connects to an external network such as the Internet.

In this example, a TCP packet exits the internal network through the firewall’s external interface. The TCP packet is the first packet of a Telnet session, and TCP is configured for CBAC inspection.

1. The packet reaches the firewall’s external interface.
2. The packet is evaluated against the interface’s existing outbound access list, and the packet is permitted. (A denied packet would simply be dropped at this point.)
3. The packet is inspected by CBAC to determine and record information about the state of the packet’s connection. This information is recorded in a new state table entry created for the new connection.

(If the packet’s application—Telnet—was not configured for CBAC inspection, the packet would simply be forwarded out the interface at this point without being inspected by CBAC. See the section “[Defining an Inspection Rule](#)” later in this chapter for information about configuring CBAC inspection.)

4. Based on the obtained state information, CBAC creates a temporary access list entry which is inserted at the beginning of the external interface’s inbound extended access list. This temporary access list entry is designed to permit inbound packets that are part of the same connection as the outbound packet just inspected.
5. The outbound packet is forwarded out the interface.
6. Later, an inbound packet reaches the interface. This packet is part of the same Telnet connection previously established with the outbound packet. The inbound packet is evaluated against the inbound access list, and it is permitted because of the temporary access list entry previously created.

7. The permitted inbound packet is inspected by CBAC, and the connection's state table entry is updated as necessary. Based on the updated state information, the inbound extended access list temporary entries might be modified in order to permit only packets that are valid for the current state of the connection.
8. Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and they are forwarded through the interface.
9. When the connection terminates or times out, the connection's state table entry is deleted, and the connection's temporary inbound access list entries are deleted.

In the sample process just described, the firewall access lists are configured as follows:

- An outbound IP access list (standard or extended) is applied to the external interface. This access list permits all packets that you want to allow to exit the network, including packets you want to be inspected by CBAC. In this case, Telnet packets are permitted.
- An inbound extended IP access list is applied to the external interface. This access list denies any traffic to be inspected by CBAC—including Telnet packets. When CBAC is triggered with an outbound packet, CBAC creates a temporary opening in the inbound access list to permit only traffic that is part of a valid, existing session.

If the inbound access list had been configured to permit *all* traffic, CBAC would be creating pointless openings in the firewall for packets that would be permitted anyway.

Supported Protocols

This section provides a list of CBAC supported protocols and includes a more detailed look at support for multimedia applications, specifically RTSP and H.323.

CBAC Supported Protocols

You can configure CBAC to inspect the following types of sessions:

- All TCP sessions, regardless of the application-layer protocol (sometimes called “single-channel” or “generic” TCP inspection)
- All UDP sessions, regardless of the application-layer protocol (sometimes called “single-channel” or “generic” UDP inspection)

You can also configure CBAC to specifically inspect certain application-layer protocols. The following application-layer protocols can all be configured for CBAC:

- CU-SeeMe (only the White Pine version)
- FTP
- H.323 (such as NetMeeting, ProShare)
- HTTP (Java blocking)
- Microsoft NetShow
- UNIX R-commands (such as rlogin, rexec, and rsh)
- RealAudio
- RTSP (Real Time Streaming Protocol)
- RPC (Sun RPC, not DCE RPC)

- SMTP (Simple Mail Transport Protocol)

**Note**

CBAC can be configured to inspect SMTP but not ESMTP (Extended Simple Mail Transport Protocol). SMTP is described in RFC 821. CBAC SMTP inspect does not inspect the ESMTP session or command sequence. Configuring SMTP inspection is not useful for ESMTP, and it can cause problems.

To determine whether a mail-server is doing SMTP or ESMTP, contact your mail-server software vendor, or telnet to the mail-server port 25 and observe the banner to see if it reports SMTP or ESMTP.

- SQL*Net
- StreamWorks
- TFTP
- VDOLive

When a protocol is configured for CBAC, that protocol traffic is inspected, state information is maintained, and in general, packets are allowed back through the firewall only if they belong to a permissible session.

RTSP and H.323 Protocol Support for Multimedia Applications

CBAC supports a number of protocols for multimedia applications that require delivery of data with real-time properties such as audio and video conferencing. This support includes the following multimedia application protocols:

- Real Time Streaming Protocol (RTSP)
- H.323 Version 2 (H.323 V2)

RTSP and H.323 V2 inspection allows clients on a protected network to receive data associated with a multimedia session from a server on an unprotected network.

RTSP Support

RTSP is the IETF standards-based protocol (RFC 2326) for control over the delivery of data with real-time properties such as audio and video streams. It is useful for large-scale broadcasts and audio or video on demand streaming, and is supported by a variety of vendor products of streaming audio and video multimedia, including Cisco IP/TV, RealNetworks RealAudio G2 Player, and Apple QuickTime 4 software.

RFC 2326 allows RTSP to run over either UDP or TCP, though CBAC currently supports only TCP-based RTSP. RTSP establishes a TCP-based control connection, or channel, between the multimedia client and server. RTSP uses this channel to control commands such as “play” and “pause” between the client and server. These control commands and responses are text-based and are similar to HTTP.

RTSP typically relies on a UDP-based data transport protocol such as standard Real-Time Transport Protocol (RTP) to open separate channels for data and for RTP Control Protocol (RTCP) messages. RTP and RTCP channels occur in pairs, with RTP being an even numbered port and RTCP being the next consecutive port. Understanding the relationship of RTP and RTCP is important for verifying session information using CBAC **show** commands.

The RTSP client uses TCP port 554 or 8554 to open a multimedia connection with a server. The data channel or data control channel (using RTCP) between the client and the server is dynamically negotiated between the client and the server using any of the high UDP ports (1024 to 65536).

CBAC uses this port information along with connection information from the client to create dynamic access control list (ACL) entries in the firewall. As TCP or UDP connections are terminated, CBAC removes these dynamic entries from the appropriate ACLs.

CBAC support for RTSP includes the following data transport modes:

- **Standard Real-Time Transport Protocol (RTP)**
RTP is an IETF standard (RFC 1889) supporting delivery of real-time data such as audio and video. RTP uses the RTP Control Protocol (RTCP) for managing the delivery of the multimedia data stream. This is the normal mode of operation for Cisco IP/TV and Apple QuickTime 4 software.
- **RealNetworks Real Data Transport (RDT)**
RDT is a proprietary protocol developed by RealNetworks for data transport. This mode uses RTSP for communication control and uses RDT for the data connection and retransmission of lost packets. This is the normal mode of operation for the RealServer G2 from RealNetworks.
- **Interleaved (Tunnel Mode)**
In this mode, RTSP uses the control channel to tunnel RTP or RDT traffic.
- **Synchronized Multimedia Integration Language (SMIL)**
SMIL is a layout language that enables the creation of multimedia presentations consisting of multiple elements of music, voice, images, text, video and graphics. This involves multiple RTSP control and data streams between the player and the servers. This mode is available only using RTSP and RDT. SMIL is a proposed specification of the World Wide Web Consortium (W3C). The RealNetworks RealServer and RealServer G2 provide support for SMIL—Cisco IP/TV and Apple QuickTime 4 do not.

H.323 Support

CBAC support for H.323 inspection includes H.323 Version 2 and H.323 Version 1. H.323 V2 provides additional options over H.323 V1, including a “fast start” option. The fast start option minimizes the delay between the time that a user initiates a connection and the time that the user gets the data (voice, video). H.323 V2 inspection is backward compatible with H.323 V1.

With H.323 V1, after a TCP connection is established between the client and server (H.225 Channel), a separate channel for media control (H.245 Channel) is opened through which multimedia channels for audit and video are further negotiated.

The H.323 V2 client opens a connection to server which is listening on port 1720. The data channel between the client and the server is dynamically negotiated using any of the high UDP ports (1024 to 65536).

CBAC uses this port information along with connection information from the client to create dynamic access control list (ACL) entries in the firewall. As TCP or UDP connections are terminated, CBAC removes these dynamic entries from the appropriate ACLs.

Restrictions

CBAC has the following restrictions:

- CBAC is available only for IP protocol traffic. Only TCP and UDP packets are inspected. (Other IP traffic, such as ICMP, cannot be inspected with CBAC and should be filtered with basic access lists instead.)
- If you reconfigure your access lists when you configure CBAC, be aware that if your access lists block TFTP traffic into an interface, you will not be able to netboot over that interface. (This is not a CBAC-specific limitation, but is part of existing access list functionality.)
- Packets with the firewall as the source or destination address are not inspected by CBAC.
- CBAC ignores ICMP Unreachable messages.
- H.323 V2 and RTSP protocol inspection supports only the following multimedia client-server applications: Cisco IP/TV, RealNetworks RealAudio G2 Player, Apple QuickTime 4.

You can use CBAC together with all the other firewall features mentioned previously in the “Cisco IOS Firewall Overview” chapter.

CBAC works with fast switching and process switching.

This section also discusses restrictions concerning:

- [FTP Traffic and CBAC](#)
- [IPSec and CBAC Compatibility](#)

FTP Traffic and CBAC

- With FTP, CBAC does not allow third-party connections (three-way FTP transfer).
- When CBAC inspects FTP traffic, it only allows data channels with the destination port in the range of 1024 to 65535.
- CBAC will not open a data channel if the FTP client-server authentication fails.

IPSec and CBAC Compatibility

When CBAC and IPSec are enabled on the same router, and the firewall router is an endpoint for IPSec for the particular flow, then IPSec is compatible with CBAC (that is, CBAC can do its normal inspection processing on the flow).

If the router is not an IPSec endpoint, but the packet is an IPSec packet, then CBAC will not inspect the packets because the protocol number in the IP header of the IPSec packet is not TCP or UDP. CBAC only inspects UDP and TCP packets.

Memory and Performance Impact

CBAC uses less than approximately 600 bytes of memory per connection. Because of the memory usage, you should use CBAC only when you need to. There is also a slight amount of additional processing that occurs whenever packets are inspected.

Sometimes CBAC must evaluate long access lists, which might have presented a negative impact to performance. However, this impact is avoided, because CBAC evaluates access lists using an accelerated method (CBAC hashes access lists and evaluates the hash).

CBAC Configuration Task List

To configure CBAC, perform the tasks described in the following sections. The tasks in the first seven sections are required; the task of verifying the CBAC configuration is optional.

- [Picking an Interface: Internal or External](#) (Required)
- [Configuring IP Access Lists at the Interface](#) (Required)
- [Configuring Global Timeouts and Thresholds](#) (Required)
- [Defining an Inspection Rule](#) (Required)
- [Applying the Inspection Rule to an Interface](#) (Required)
- [Configuring Logging and Audit Trail](#) (Required)
- [Other Guidelines for Configuring a Firewall](#) (Required)
- [Verifying CBAC](#) (Optional)

Following CBAC configuration, you can monitor and maintain CBAC using the information in this section.

**Note**

If you try to configure Context-based Access Control (CBAC) but do not have a good understanding of how CBAC works, you might inadvertently introduce security risks to the firewall and to the protected network. You should be sure you understand what CBAC does before you configure CBAC.

**Note**

As with all networking devices, protect access into the firewall by configuring passwords as described in the “Configuring Passwords and Privileges” chapter. You should also consider configuring user authentication, authorization, and accounting as described in the “Authentication, Authorization, and Accounting (AAA)” part of this guide. Additional guidelines to help you establish a good security policy can be found in the “Cisco IOS Firewall Overview” chapter.

For CBAC configuration examples, refer to the “[CBAC Configuration Examples](#)” section at the end of this chapter.

Picking an Interface: Internal or External

You must decide whether to configure CBAC on an internal or external interface of your firewall.

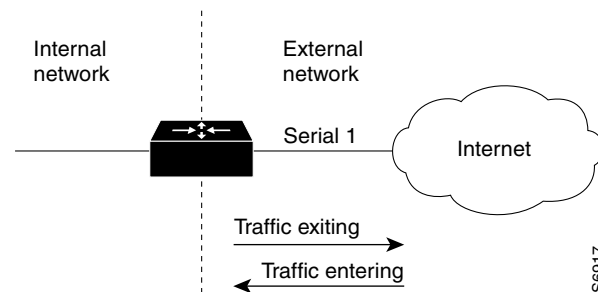
“Internal” refers to the side where sessions must originate for their traffic to be permitted through the firewall. “External” refers to the side where sessions cannot originate (sessions originating from the external side will be blocked).

If you will be configuring CBAC in two directions, you should configure CBAC in one direction first, using the appropriate “internal” and “external” interface designations. When you configure CBAC in the other direction, the interface designations will be swapped. (CBAC can be configured in two directions at one or more interfaces. Configure CBAC in two directions when the networks on both sides of the firewall require protection, such as with extranet or intranet configurations, and for protection against DoS attacks.)

The firewall is most commonly used with one of two basic network topologies. Determining which of these topologies is most like your own can help you decide whether to configure CBAC on an internal interface or on an external interface.

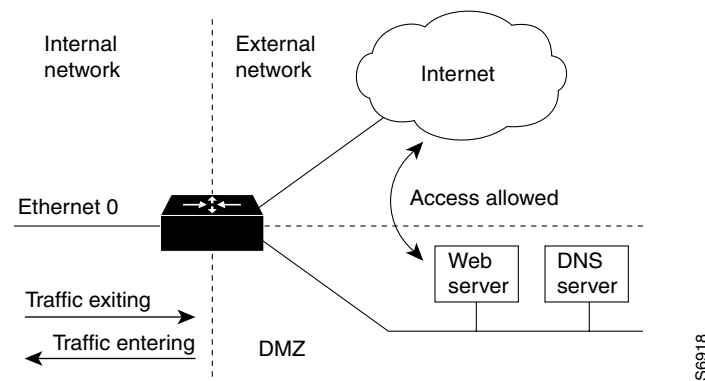
The first topology is shown in [Figure 21](#). In this simple topology, CBAC is configured for the *external* interface Serial 1. This prevents specified protocol traffic from entering the firewall and the internal network, unless the traffic is part of a session initiated from within the internal network.

Figure 21 Simple Topology—CBAC Configured at the External Interface



The second topology is shown in [Figure 22](#). In this topology, CBAC is configured for the *internal* interface Ethernet 0. This allows external traffic to access the services in the Demilitarized Zone (DMZ), such as DNS services, but prevents specified protocol traffic from entering your internal network—unless the traffic is part of a session initiated from within the internal network.

Figure 22 DMZ Topology—CBAC Configured at the Internal Interface



Using these two sample topologies, decide whether to configure CBAC on an internal or external interface.

To view various firewall configuration scenarios, see the [“CBAC Configuration Examples”](#) section at the end of this chapter.

Configuring IP Access Lists at the Interface

For CBAC to work properly, you need to make sure that you have IP access lists configured appropriately at the interface.

Follow these three general rules when evaluating your IP access lists at the firewall:

- Start with a basic configuration.

If you try to configure access lists without a good understanding of how access lists work, you might inadvertently introduce security risks to the firewall and to the protected network. You should be sure you understand what access lists do before you configure your firewall. For more information about access control lists, refer to the “Access Control Lists: Overview and Guidelines” chapter.

A basic initial configuration allows all network traffic to flow from the protected networks to the unprotected networks, while blocking network traffic from any unprotected networks.

- Permit CBAC traffic to leave the network through the firewall.

All access lists that evaluate traffic leaving the protected network should permit traffic that will be inspected by CBAC. For example, if Telnet will be inspected by CBAC, then Telnet traffic should be permitted on all access lists that apply to traffic leaving the network.

- Use extended access lists to deny CBAC return traffic entering the network through the firewall.

For temporary openings to be created in an access list, the access list must be an extended access list. So wherever you have access lists that will be applied to returning traffic, you must use extended access lists. The access lists should deny CBAC return traffic because CBAC will open up temporary holes in the access lists. (You want traffic to be normally blocked when it enters your network.)


Note

If your firewall only has two connections, one to the internal network and one to the external network, using all inbound access lists works well because packets are stopped before they get a chance to affect the router itself.

This section contains the following sections:

- [Basic Configuration](#)
- [External Interface](#)
- [Internal Interface](#)

Basic Configuration

The first time you configure the Cisco IOS Firewall, it is helpful to start with a basic access list configuration that makes the operation of the firewall easy to understand without compromising security. The basic configuration allows all network traffic from the protected networks access to the unprotected networks, while blocking all network traffic (with some exceptions) from the unprotected networks to the protected networks.

Any firewall configuration depends on your site security policy. If the basic configuration does not meet your initial site security requirements, configure the firewall to meet your policy. If you are unfamiliar with that policy or need help with the configuration, contact your network administration group for assistance. For additional guidelines on configuring a firewall, refer to the “[Other Guidelines for Configuring a Firewall](#)” section in this chapter.

Use the following guidelines for configuring the initial firewall access lists:

- Do not configure an access list for traffic from the protected networks to the unprotected networks, meaning that all traffic from the protected networks can flow through the interface.

This helps to simplify firewall management by reducing the number of access lists applied at the interfaces. Of course this assumes a high level of trust for the users on the protected networks, and it assumes there are no malicious users on the protected networks who might launch attacks from the “inside.” You can fine tune network access for users on the protected networks as you gain experience with access list configuration and the operation of the firewall.

- Configure an access list that includes entries permitting certain ICMP traffic from unprotected networks.

While an access list that denies all IP traffic not part of a connection inspected by CBAC seems most secure, it is not practical for normal operation of the router. The router expects to see ICMP traffic from other routers in the network. Additionally, ICMP traffic is not inspected by CBAC, meaning specific entries are needed in the access list to permit return traffic for ICMP commands. For example, a user on a protected network uses the **ping** command to get the status of a host on an unprotected network; without entries in the access list that permit **echo reply** messages, the user on the protected network gets no response to the **ping** command.

Include access list entries to permit the following ICMP messages:

Message	Description
echo reply	Outgoing ping commands require echo-reply messages to come back.
time-exceeded	Outgoing traceroute commands require time-exceeded messages to come back.
packet-too-big	Path MTU discovery requires “too-big” messages to come back.
traceroute	Allow an incoming traceroute.
unreachable	Permit all “unreachable” messages to come back. If a router cannot forward or deliver a datagram, it sends an ICMP unreachable message back to the source and drops the datagram.

- Add an access list entry denying any network traffic from a source address matching an address on the protected network.

This is known as anti-spoofing protection because it prevents traffic from an unprotected network from assuming the identity of a device on the protected network.

- Add an entry denying broadcast messages with a source address of 255.255.255.255.

This entry helps to prevent broadcast attacks.

- By default, the last entry in an extended access list is an implicit denial of all IP traffic not specifically allowed by other entries in the access list.

Although this is the default setting, this final deny statement is not shown by default in an access list. Optionally, you can add an entry to the access list denying IP traffic with any source or destination address with no undesired effects.

For complete information about how to configure IP access lists, refer to the “Configuring IP Services” chapter of the *Cisco IOS IP Addressing Services Configuration Guide*.

For tips on applying access lists at an external or internal interface, review the sections “[External Interface](#)” and “[Internal Interface](#)” in this chapter.

External Interface

Here are some guidelines for your access lists when you will be configuring CBAC on an external interface:

- If you have an outbound IP access list at the external interface, the access list can be a standard or extended access list. This outbound access list should permit traffic that you want to be inspected by CBAC. If traffic is not permitted, it will not be inspected by CBAC, but will be simply dropped.

- The inbound IP access list at the external interface must be an extended access list. This inbound access list should deny traffic that you want to be inspected by CBAC. (CBAC will create temporary openings in this inbound access list as appropriate to permit only return traffic that is part of a valid, existing session.)
- For complete information about how to configure IP access lists, refer to the “Configuring IP Services” chapter of the *Cisco IOS IP Addressing Services Configuration Guide*.

Internal Interface

Here are some tips for your access lists when you will be configuring CBAC on an internal interface:

- If you have an inbound IP access list at the internal interface or an outbound IP access list at external interface(s), these access lists can be either a standard or extended access list. These access lists should permit traffic that you want to be inspected by CBAC. If traffic is not permitted, it will not be inspected by CBAC, but will be simply dropped.
- The outbound IP access list at the internal interface and the inbound IP access list at the external interface must be extended access lists. These outbound access lists should deny traffic that you want to be inspected by CBAC. (CBAC will create temporary openings in these outbound access lists as appropriate to permit only return traffic that is part of a valid, existing session.) You do not necessarily need to configure an extended access list at both the outbound internal interface and the inbound external interface, but at least one is necessary to restrict traffic flowing through the firewall into the internal protected network.
- For complete information about how to configure IP access lists, refer to the “Configuring IP Services” chapter of the *Cisco IOS IP Addressing Services Configuration Guide*.

Configuring Global Timeouts and Thresholds

CBAC uses timeouts and thresholds to determine how long to manage state information for a session, and to determine when to drop sessions that do not become fully established. These timeouts and thresholds apply globally to all sessions.

You can use the default timeout and threshold values, or you can change to values more suitable to your security requirements. You should make any changes to the timeout and threshold values before you continue configuring CBAC.



Note

If you want to enable the more aggressive TCP host-specific denial-of-service prevention that includes the blocking of connection initiation to a host, you must set the **block-time** specified in the **ip inspect tcp max-incomplete host** command (see the last row in [Table 24](#)).

All the available CBAC timeouts and thresholds are listed in [Table 24](#), along with the corresponding command and default value. To change a global timeout or threshold listed in the “Timeout or Threshold Value to Change” column, use the global configuration command in the “Command” column:

Table 24 **Timeout and Threshold Values**

Timeout or Threshold Value to Change	Command	Default
The length of time the software waits for a TCP session to reach the established state before dropping the session.	ip inspect tcp synwait-time <i>seconds</i>	30 seconds
The length of time a TCP session will still be managed after the firewall detects a FIN-exchange.	ip inspect tcp finwait-time <i>seconds</i>	5 seconds
The length of time a TCP session will still be managed after no activity (the TCP idle timeout). ¹	ip inspect tcp idle-time <i>seconds</i>	3600 seconds (1 hour)
The length of time a UDP session will still be managed after no activity (the UDP idle timeout). ¹	ip inspect udp idle-time <i>seconds</i>	30 seconds
The length of time a DNS name lookup session will still be managed after no activity.	ip inspect dns-timeout <i>seconds</i>	5 seconds
The number of existing half-open sessions that will cause the software to start deleting half-open sessions. ²	ip inspect max-incomplete high <i>number</i>	500 existing half-open sessions
The number of existing half-open sessions that will cause the software to stop deleting half-open sessions. ²	ip inspect max-incomplete low <i>number</i>	400 existing half-open sessions
The rate of new sessions that will cause the software to start deleting half-open sessions. ²	ip inspect one-minute high <i>number</i>	500 half-open sessions per minute
The rate of new sessions that will cause the software to stop deleting half-open sessions. ²	ip inspect one-minute low <i>number</i>	400 half-open sessions per minute
The number of existing half-open TCP sessions with the same destination host address that will cause the software to start dropping half-open sessions to the same destination host address. ³	ip inspect tcp max-incomplete host <i>number</i> block-time <i>minutes</i>	50 existing half-open TCP sessions; 0 minutes

1. The global TCP and UDP idle timeouts can be overridden for specified application-layer protocols' sessions as described in the **ip inspect name** (global configuration) command description, found in the "Context-Based Access Control Commands" chapter of the *Cisco IOS Security Command Reference*.
2. See the following section, "Half-Open Sessions," for more information.
3. Whenever the **max-incomplete host** threshold is exceeded, the software will drop half-open sessions differently depending on whether the **block-time** timeout is zero or a positive non-zero number. If the **block-time** timeout is zero, the software will delete the oldest existing half-open session for the host for every new connection request to the host and will let the SYN packet through. If the **block-time** timeout is greater than zero, the software will delete all existing half-open sessions for the host, and then block all new connection requests to the host. The software will continue to block all new connection requests until the **block-time** expires.

To reset any threshold or timeout to the default value, use the **no** form of the command in [Table 24](#).

Half-Open Sessions

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state—the TCP three-way handshake has not yet been completed. For UDP, "half-open" means that the firewall has detected no return traffic.

CBAC measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Rate measurements are made several times per minute.

When the number of existing half-open sessions rises above a threshold (the **max-incomplete high** number), the software will delete half-open sessions as required to accommodate new connection requests. The software will continue to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (the **max-incomplete low** number).

When the rate of new connection attempts rises above a threshold (the **one-minute high** number), the software will delete half-open sessions as required to accommodate new connection attempts. The software will continue to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (the **one-minute low** number). The rate thresholds are measured as the number of new session connection attempts detected in the last one-minute sample period.

Defining an Inspection Rule

After you configure global timeouts and thresholds, you must define an inspection rule. This rule specifies what IP traffic (which application-layer protocols) will be inspected by CBAC at an interface.

Normally, you define only one inspection rule. The only exception might occur if you want to enable CBAC in two directions as described earlier in the section “When and Where to Configure CBAC.” For CBAC configured in both directions at a single firewall interface, you should configure two rules, one for each direction.

An inspection rule should specify each desired application-layer protocol as well as generic TCP or generic UDP if desired. The inspection rule consists of a series of statements each listing a protocol and specifying the same inspection rule name.

Inspection rules include options for controlling alert and audit trail messages and for checking IP packet fragmentation.

To define an inspection rule, follow the instructions in the following sections:

- [Configuring Application-Layer Protocol Inspection](#)
- [Configuring Generic TCP and UDP Inspection](#)

Configuring Application-Layer Protocol Inspection

This section provides instructions for configuring CBAC with the following inspection information:

- [Configuring Application-Layer Protocols](#)
- [Configuring Java Blocking](#)
- [Configuring IP Packet Fragmentation Inspection](#)



Note

For CBAC inspection to work with NetMeeting 2.0 traffic (an H.323 application-layer protocol), you must also configure inspection for TCP, as described later in the “[Configuring Generic TCP and UDP Inspection](#)” section. This requirement exists because NetMeeting 2.0 uses an additional TCP channel not defined in the H.323 specification.

Configuring Application-Layer Protocols

To configure CBAC inspection for an application-layer protocol, use one or both of the following commands in global configuration mode:

Command	Purpose
Router(config)# ip inspect name <i>inspection-name</i> <i>protocol</i> [alert { on off }] [audit-trail { on off }] [timeout <i>seconds</i>]	Configures CBAC inspection for an application-layer protocol (except for RPC and Java). Use one of the protocol keywords defined in Table 25 . Repeat this command for each desired protocol. Use the same <i>inspection-name</i> value to create a single inspection rule.
Router(config)# ip inspect name <i>inspection-name</i> rpc program-number <i>number</i> [wait-time <i>minutes</i>] [alert { on off }] [audit-trail { on off }] [timeout <i>seconds</i>]	Enables CBAC inspection for the RPC application-layer protocol. You can specify multiple RPC program numbers by repeating this command for each program number. Use the same <i>inspection-name</i> value to create a single inspection rule.

Refer to the description of the **ip inspect name** global configuration command in the “Context-Based Access Control Commands” chapter of the *Cisco IOS Security Command Reference* for more information about how the command works with each application-layer protocol.

To enable CBAC inspection for Java blocking, see the following section, “[Configuring Java Blocking](#).” [Table 25](#) identifies application protocol keywords for the **ip inspect name** command.

Table 25 Application Protocol Keywords for the **ip inspect name** Command

Application Protocol	Protocol Keyword
CU-SeeMe	cuseeme
FTP	ftp
H.323	h323
Microsoft NetShow	netshow
UNIX R commands (rlogin, rexec, rsh)	rcmd
RealAudio	realaudio
SMTP	smtp
SQL*Net	sqlnet
StreamWorks	streamworks
TFTP	tftp
VDOLive	vdolive

Configuring Java Blocking

Java applet filtering distinguishes between trusted and untrusted applets by relying on a list of external sites that you designate as “friendly.” If an applet is from a friendly site, the firewall allows the applet through. If the applet is not from a friendly site, the applet will be blocked. (Alternately, you could permit applets from all external sites except for those you specifically designate as hostile.)

**Note**

Java blocking forces a strict order on TCP packets. To properly verify that Java applets are not in the response, a firewall will drop any TCP packet that is out of order. Because the network—not the firewall—determines how packets are routed, the firewall cannot control the order of the packets; the firewall can only drop and retransmit all TCP packets that are not in order.

To block all Java applets except for applets from friendly locations, use the following commands in global configuration mode:

	Command	Purpose
Step 1	<pre>Router(config)# ip access-list standard name permit ... deny ... (Use permit and deny statements as appropriate.) or Router(config)# access-list access-list-number {deny permit} protocol source [source-wildcard] eq www destination [destination-wildcard]</pre>	<p>Creates a standard access list that permits traffic only from friendly sites, and denies traffic from hostile sites.</p> <p>Use the any keyword for the destination as appropriate—but be careful to not misuse the any keyword to inadvertently allow all applets through.</p>
Step 2	<pre>Router(config)# ip inspect name inspection-name http [java-list access-list] [alert {on off}] [audit-trail {on off}] [timeout seconds]</pre>	<p>Blocks all Java applets except for applets from the friendly sites defined previously in the access list. Java blocking only works with numbered standard access lists.</p> <p>To create a single inspection rule, use the same <i>inspection-name</i> value as when you specified other protocols.</p>

**Caution**

CBAC does not detect or block encapsulated Java applets. Therefore, Java applets that are wrapped or encapsulated, such as applets in .zip or .jar format, are *not* blocked at the firewall. CBAC also does not detect or block applets loaded from FTP, gopher, HTTP on a nonstandard port, and so forth.

Configuring IP Packet Fragmentation Inspection

CBAC inspection rules can help protect hosts against certain DoS attacks involving fragmented IP packets.

Using fragmentation inspection, the firewall maintains an *interfragment state* (structure) for IP traffic. Non-initial fragments are discarded unless the corresponding initial fragment was permitted to pass through the firewall. Non-initial fragments received before the corresponding initial fragments are discarded.

**Note**

Fragmentation inspection can have undesirable effects in certain cases, because it can result in the firewall discarding any packet whose fragments arrive out of order. There are many circumstances that can cause out-of-order delivery of legitimate fragments. Applying fragmentation inspection in situations where legitimate fragments, which are likely to arrive out of order, might have a severe performance impact.

Because routers running Cisco IOS software are used in a large variety of networks, and because the CBAC feature is often used to isolate parts of internal networks from one another, the fragmentation inspection feature is disabled by default. Fragmentation detection must be explicitly enabled for an inspection rule using the **ip inspect name** command. Unfragmented traffic is never discarded because it lacks a fragment state. Even when the system is under heavy attack with fragmented packets, legitimate fragmented traffic, if any, gets some fraction of the firewall's fragment state resources, and legitimate, unfragmented traffic can flow through the firewall unimpeded.

Configuring Generic TCP and UDP Inspection

You can configure TCP and UDP inspection to permit TCP and UDP packets to enter the internal network through the firewall, even if the application-layer protocol is not configured to be inspected. However, TCP and UDP inspection do not recognize application-specific commands, and therefore might not permit all return packets for an application, particularly if the return packets have a different port number than the previous exiting packet.

Any application-layer protocol that is inspected will take precedence over the TCP or UDP packet inspection. For example, if inspection is configured for FTP, all control channel information will be recorded in the state table, and all FTP traffic will be permitted back through the firewall if the control channel information is valid for the state of the FTP session. The fact that TCP inspection is configured is irrelevant to the FTP state information.

With TCP and UDP inspection, packets entering the network must exactly match the corresponding packet that previously exited the network. The entering packets must have the same source/destination addresses and source/destination port numbers as the exiting packet (but reversed); otherwise, the entering packets will be blocked at the interface. Also, all TCP packets with a sequence number outside of the window are dropped.

With UDP inspection configured, replies will only be permitted back in through the firewall if they are received within a configurable time after the last request was sent out. (This time is configured with the **ip inspect udp idle-time** command.)

To configure CBAC inspection for TCP or UDP packets, use one or both of the following commands in global configuration mode:

Command	Purpose
Router(config)# ip inspect name <i>inspection-name</i> tcp [alert {on off}] [audit-trail {on off}] [timeout <i>seconds</i>]	Enables CBAC inspection for TCP packets. To create a single inspection rule, use the same <i>inspection-name</i> value as when you specified other protocols.
Router(config)# ip inspect name <i>inspection-name</i> udp [alert {on off}] [audit-trail {on off}] [timeout <i>seconds</i>]	Enables CBAC inspection for UDP packets. To create a single inspection rule, use the same <i>inspection-name</i> value as when you specified other protocols.

Applying the Inspection Rule to an Interface

After you define an inspection rule, you apply this rule to an interface.

Normally, you apply only one inspection rule to one interface. The only exception might occur if you want to enable CBAC in two directions as described earlier in the section “When and Where to Configure CBAC.” For CBAC configured in both directions at a single firewall interface, you should apply two rules, one for each direction.

If you are configuring CBAC on an external interface, apply the rule to outbound traffic.

If you are configuring CBAC on an internal interface, apply the rule to inbound traffic.

To apply an inspection rule to an interface, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# ip inspect <i>inspection-name</i> {in out}	Applies an inspection rule to an interface.

Configuring Logging and Audit Trail

Turn on logging and audit trail to provide a record of network access through the firewall, including illegitimate access attempts, and inbound and outbound services. To configure logging and audit trail functions, enter the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# service timestamps log datetime	Adds the date and time to syslog and audit trail messages.
Step 2	Router(config)# logging host	Specifies the host name or IP address of the host where you want to send syslog messages.
Step 3	Router(config)# logging facility <i>facility-type</i>	Configures the syslog facility in which error messages are sent.
Step 4	Router(config)# logging trap level	(Optional) Uses this command to limit messages logged to the syslog servers based on severity. The default is level 7 (informational).
Step 5	Router(config)# ip inspect audit-trail	Turns on CBAC audit trail messages.

For information on how to interpret the syslog and audit trail messages, refer to the “[Interpreting Syslog and Console Messages Generated by CBAC](#)” section.

To configure audit trail functions on a per-application basis, refer to the “[Defining an Inspection Rule](#)” section for more information.

For complete information about how to configure logging, refer to the “Troubleshooting the Router” chapter of the *Cisco IOS Network Management Configuration Guide*.

Other Guidelines for Configuring a Firewall

As with all networking devices, you should always protect access into the firewall by configuring passwords as described in the module “Configuring Security with Passwords, Privilege Levels, and Login Usernames for CLI Sessions on Networking Devices.” You should also consider configuring user authentication, authorization, and accounting as described in the “Authentication, Authorization, and Accounting (AAA)” part of this guide.

You should also consider the following recommendations:

- When setting passwords for privileged access to the firewall, use the **enable secret** command rather than the **enable password** command, which does not have as strong an encryption algorithm.

- Put a password on the console port. In authentication, authorization, and accounting (AAA) environments, use the same authentication for the console as for elsewhere. In a non-AAA environment, at a minimum configure the **login** and **password password** commands.
- Think about access control *before* you connect a console port to the network in any way, including attaching a modem to the port. Be aware that a *break* on the console port might give total control of the firewall, even with access control configured.
- Apply access lists and password protection to all virtual terminal ports. Use access lists to limit who can Telnet into your router.
- Do not enable any local service (such as SNMP or NTP) that you do not use. Cisco Discovery Protocol (CDP) and Network Time Protocol (NTP) are on by default, and you should turn these off if you do not need them.

To turn off CDP, enter the **no cdp run** global configuration command. To turn off NTP, enter the **ntp disable** interface configuration command on each interface not using NTP.

If you must run NTP, configure NTP only on required interfaces, and configure NTP to listen only to certain peers.

Any enabled service could present a potential security risk. A determined, hostile party might be able to find creative ways to misuse the enabled services to access the firewall or the network.

For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring access lists to deny packets for the services at specific interfaces.

- Protect against spoofing: protect the networks on both sides of the firewall from being spoofed from the other side. You could protect against spoofing by configuring input access lists at all interfaces to pass only traffic from expected source addresses, and to deny all other traffic.

You should also disable source routing. For IP, enter the **no ip source-route** global configuration command. Disabling source routing at *all* routers can also help prevent spoofing.

You should also disable minor services. For IP, enter the **no service tcp-small-servers** and **no service udp-small-servers** global configuration commands. In Cisco IOS Release 12.0 and later, these services are disabled by default.

- Prevent the firewall from being used as a relay by configuring access lists on any asynchronous Telnet ports.
- Normally, you should disable directed broadcasts for all applicable protocols on your firewall and on all your other routers. For IP, use the **no ip directed-broadcast** command. Rarely, some IP networks do require directed broadcasts; if this is the case, do not disable directed broadcasts.

Directed broadcasts can be misused to multiply the power of denial-of-service attacks, because every denial-of-service packet sent is broadcast to every host on a subnet. Furthermore, some hosts have other intrinsic security risks present when handling broadcasts.
- Configure the **no proxy-arp** command to prevent internal addresses from being revealed. (This is important to do if you do not already have NAT configured to prevent internal addresses from being revealed.)
- Keep the firewall in a secured (locked) room.

Verifying CBAC

You can view and verify CBAC configuration, status, statistics, and session information by using one or more of the following commands in EXEC mode:

Command	Purpose
Router# show ip access-lists	Displays the contents of all current IP access lists.
Router# show ip inspect name <i>inspection-name</i>	Shows a particular configured inspection rule.
Router# show ip inspect config	Shows the complete CBAC inspection configuration.
Router# show ip inspect interfaces	Shows interface configuration with regards to applied inspection rules and access lists.
Router# show ip inspect session [<i>detail</i>]	Shows existing sessions that are currently being tracked and inspected by CBAC.
Router# show ip inspect all	Shows all CBAC configuration and all existing sessions that are currently being tracked and inspected by CBAC.

In most cases, you can tell whether CBAC is inspecting network traffic properly because network applications are working as expected. In some cases, however, you might want to verify CBAC operation. For example, to verify RTSP or H.323 inspection, initiate an RTSP- or H.323-based application through the firewall. Use the **show ip inspect session** and **show ip access lists** commands to verify CBAC operation. These commands display the dynamic ACL entries and the established connections for a multimedia session.

In the case of RTSP inspection, session output can vary based on the multimedia protocol and the transport mode. This section uses examples of RTSP and H.323 V2 sessions to illustrate verification procedures and to illustrate how session information, and the interpretation of that session information, varies based on the protocol being inspected. This section provides the following sample session output:

- [RTSP with RDT](#)
- [RTSP with TCP Only \(Interleaved Mode\)](#)
- [RTSP with SMIL](#)
- [RTSP with RTP \(IP/TV\)](#)
- [H.323 V2](#)

RTSP with RDT

The following example illustrates the result of the **show ip inspect session** command. It shows that a control channel (rtsp) and data channel (rtsp-data) are open between hosts 192.168.155.2 and 192.168.35.1.

```
router# show ip inspect session
Established Sessions
  Session 616B4F1C (192.168.155.2:7548)=>(192.168.35.1:6970) rtsp-data SIS_OPEN
  Session 611E2904 (192.168.35.1:1221)=>(192.168.155.2:554) rtsp SIS_OPEN
```

The following example illustrates the result of the **show ip access-list** command. It shows that two dynamic entries (permit statements) were added to ACL 100 for the multimedia session. The TCP entry creates a dynamic opening through the firewall between port 554 (RTSP protocol port) on the client and port 1221 on the server. The UDP entry creates a dynamic opening between data port 7548 on the client and data port 6970 on the server.

```
router# show ip access-list
Extended IP access list 100
  permit udp host 192.168.155.2 eq 7548 host 192.168.35.1 eq 6970 (31 matches)
  permit tcp host 192.168.155.2 eq 554 host 192.168.35.1 eq 1221 (27 matches)
```


After closing the multimedia session, review the session output using the **show** commands to verify the firewall software has removed the dynamic entries from the configuration.

RTSP with TCP Only (Interleaved Mode)

The following example illustrates the result of the **show ip inspect session** command. It shows that only a single control channel (rtsp) is open between hosts 192.168.155.2 and 192.168.35.1. In this mode, data is tunneled through the firewall using the TCP connection to interleave RDT or RTP data.

```
router# show ip inspect session
Established Sessions
  Session 611E2904 (192.168.35.1:1228)=>(192.168.155.2:554) rtsp SIS_OPEN
```

The following example illustrates the result of the **show ip access-list** command. It shows that a single dynamic entry (permit statement) was added to ACL 100 for the multimedia session. The TCP entry creates a dynamic opening through the firewall between port 554 (RTSP protocol port) on the client and port 1228 on the server.

```
router# show ip access-lists
Extended IP access list 100
  permit tcp host 192.168.155.2 eq 554 host 192.168.35.1 eq 1228 (391 matches)
```

After closing the multimedia session, review the session output using the **show** commands to verify the firewall software has removed the dynamic entries from the configuration.

RTSP with SMIL

The following example illustrates the result of the **show ip inspect session** command for RTSP using Synchronized Multimedia Integration Language (SMIL). It shows that a single control channel (rtsp) and multiple data channels (rtsp-data) are open between hosts 192.168.155.2 and 192.168.35.1. The data channels appear as half open sessions because the UDP data flows in one direction only, which is from the server to the client.

```
router# show ip inspect session
Established Sessions
  Session 616CA914 (192.168.155.2:30616)=>(192.168.35.1:6974) rtsp-data SIS_OPEN
  Session 616B4E78 (192.168.35.1:1230)=>(192.168.155.2:554) rtsp SIS_OPEN
  Session 614AB61C (192.168.155.2:29704)=>(192.168.35.1:6976) rtsp-data SIS_OPEN
  Session 616CAA88 (192.168.155.2:26764)=>(192.168.35.1:6972) rtsp-data SIS_OPEN
Half-open Sessions
  Session 614AAEF0 (192.168.155.2:15520)=>(192.168.35.1:6970) rtsp-data SIS_OPENING
```

The following example illustrates the result of the **show ip access-lists** command. It shows that multiple dynamic entries (permit statements) were added to ACL 100 for the multimedia session. The TCP entry creates a dynamic opening through the firewall between port 554 (RTSP protocol port) on the client and port 1230 on the server. The UDP entries create dynamic openings between negotiated data ports on the client (192.168.155.2) and the server (192.168.35.1).

```
router# show ip access-list
Extended IP access list 100
  permit udp host 192.168.155.2 eq 29704 host 192.168.35.1 eq 6976 (182 matches)
  permit udp host 192.168.155.2 eq 30616 host 192.168.35.1 eq 6974 (268 matches)
  permit udp host 192.168.155.2 eq 26764 host 192.168.35.1 eq 6972 (4 matches)
  permit udp host 192.168.155.2 eq 15520 host 192.168.35.1 eq 6970 (12 matches)
  permit tcp host 192.168.155.2 eq 554 host 192.168.35.1 eq 1230 (41 matches)
```

After closing the multimedia session, review the session output using the **show** commands to verify the firewall software has removed the dynamic entries from the configuration.

RTSP with RTP (IP/TV)

The following example illustrates the result of the **show ip inspect session** command for RTSP with the Cisco IP/TV application. The output shows that a single control channel (rtsp) and multiple data channels (rtsp-data) are open between hosts 192.168.2.15 and 192.168.102.23. The data channels appear as half-open sessions because the UDP data flows in one direction only, which is from the server to the client.

```
router# show ip inspect session
Established Sessions
  Session 611493C0 (192.168.2.15:2571)=>(192.168.102.23:8554) rtsp SIS_OPEN
Half-open Sessions
  Session 6114A22C (192.168.102.23:2428)=>(192.168.2.15:20112) rtsp-data SIS_OPENING
  Session 61149F44 (192.168.102.23:2428)=>(192.168.2.15:20113) rtsp-data SIS_OPENING
  Session 6114A0B8 (192.168.102.23:2429)=>(192.168.2.15:20115) rtsp-data SIS_OPENING
  Session 6114A3A0 (192.168.102.23:2429)=>(192.168.2.15:20114) rtsp-data SIS_OPENING
```

The following example illustrates the result of the **show ip access-lists** command. It shows that multiple dynamic entries (permit statements) were added to ACL 100 for the multimedia session. The TCP entry creates a dynamic opening through the firewall between port 554 (RTSP protocol port) on the client and port 1230 on the server. The UDP entries create dynamic openings between negotiated data ports on the client (192.168.2.15) and the server (192.168.102.23).

```
router# show ip access-lists
Extended IP access list 100
  permit udp host 192.168.102.23 eq 2428 host 192.168.2.15 eq 20113 (11 matches)
  permit udp host 192.168.102.23 eq 2428 host 192.168.2.15 eq 20112 (256 matches)
  permit udp host 192.168.102.23 eq 2429 host 192.168.2.15 eq 20115 (11 matches)
  permit udp host 192.168.102.23 eq 2429 host 192.168.2.15 eq 20114 (4598 matches)
  permit tcp host 192.168.102.23 eq 8554 host 192.168.2.15 eq 2571 (22 matches)
```

After closing the multimedia session, review the session output using the **show** commands to verify that the firewall software has removed the dynamic entries from the configuration.

H.323 V2

The following example illustrates the result of the **show ip inspect session** command for H.323 V2. It shows a single H.323 control channel, an RTP Control Protocol channel for both audio and video data, and an RTP data channel between hosts 192.168.155.2 and 192.168.35.1.

```
Session 615E2688 (192.168.35.1:49609)=>(192.168.155.1:49609) H323-RTCP-audio SIS_OPEN
Session 615E2688 (192.168.35.1:49508)=>(192.168.155.1:49508) H323-RTP-audio SIS_OPEN
Session 615E2688 (192.168.35.1:49410)=>(192.168.155.1:49410) H323-RTP-video SIS_OPEN
Session 615E2688 (192.168.35.1:49611)=>(192.168.155.1:49611) H323-RTCP-video SIS_OPEN
Session 615E1640 (192.168.35.1:4414)=>(192.168.155.1:1720) H323 SIS_OPEN
```

The following example illustrates the result of the **show ip access-lists** command. It shows that multiple dynamic entries (permit statements) were added to ACL 100 for the multimedia session. The TCP entry creates a dynamic opening through the firewall between port 1720 (H.323 V2 protocol port) on the client and port 4414 on the server. The UDP entries create dynamic openings between negotiated data ports on the client (192.168.155.1) and the server (192.168.35.1).

```
router# show ip access-lists
Extended IP access list 100
  permit udp host 192.168.155.1 eq 49609 host 192.168.35.1 eq 49609 (11 matches)
  permit udp host 192.168.155.1 eq 49508 host 192.168.35.1 eq 49508 (256 matches)
  permit udp host 192.168.155.1 eq 49411 host 192.168.35.1 eq 49411 (11 matches)
  permit udp host 192.168.155.1 eq 49610 host 192.168.35.1 eq 49610 (4598 matches)
  permit tcp host 192.168.155.1 eq 1720 host 192.168.35.1 eq 4414 (22 matches)
```

Monitoring and Maintaining CBAC

You can watch for network attacks and investigate network problems using debug commands and system messages. This section has the following sections:

- [Debugging Context-Based Access Control](#)
- [Interpreting Syslog and Console Messages Generated by CBAC](#)
- [Turning Off CBAC](#)

Debugging Context-Based Access Control

To assist CBAC debugging, you can turn on audit trail messages that will be displayed on the console after each CBAC session closes. Audit trail information is also configurable on a per-application basis using the CBAC inspection rules.

To turn on audit trail messages, use the following command in global configuration mode:

Command	Purpose
Router(config)# ip inspect audit-trail	Turns on CBAC audit trail messages.

If required, you can also use the CBAC **debug** commands listed in this section. (Debugging can be turned off for each of the commands in this section by using the **no** form of the command. To disable all debugging, use the privileged EXEC commands **no debug all** or **undebg all**.)

The following **debug** commands are available:

- [Generic Debug Commands](#)
- [Transport Level Debug Commands](#)
- [Application Protocol Debug Commands](#)

For a complete description of the debug commands, refer to the *Cisco IOS Debug Command Reference*.



Note

Effective with Cisco IOS Release 12.4(20)T, the **debug ip inspect** command is replaced by the **debug policy-firewall** command. See the *Cisco IOS Debug Command Reference* for more information.

Generic Debug Commands

You can use the following generic **debug** commands, entered in privileged EXEC mode:

Command	Purpose
Router# debug ip inspect function-trace	Displays messages about software functions called by CBAC.
Router# debug ip inspect object-creation	Displays messages about software objects being created by CBAC. Object creation corresponds to the beginning of CBAC-inspected sessions.
Router# debug ip inspect object-deletion	Displays messages about software objects being deleted by CBAC. Object deletion corresponds to the closing of CBAC-inspected sessions.

Command	Purpose
Router# debug ip inspect events	Displays messages about CBAC software events, including information about CBAC packet processing.
Router# debug ip inspect timers	Displays messages about CBAC timer events such as when a CBAC idle timeout is reached.
Router# debug ip inspect detail	Enables the detailed option, which can be used in combination with other options to get additional information.

Transport Level Debug Commands

You can use the following transport-level **debug** commands, entered in privileged EXEC mode:

Command	Purpose
Router# debug ip inspect tcp	Displays messages about CBAC-inspected TCP events, including details about TCP packets.
Router# debug ip inspect udp	Displays messages about CBAC-inspected UDP events, including details about UDP packets.

Application Protocol Debug Commands

You can use the following application protocol **debug** command, entered in privileged EXEC mode:

Command	Purpose
Router# debug ip inspect protocol	Displays messages about CBAC-inspected protocol events, including details about the protocol's packets. Refer to Table 26 to determine the protocol keyword.

[Table 26](#) identifies application protocol keywords for the **debug ip inspect** command.

Table 26 Application Protocol Keywords for the **debug ip inspect** Command

Application Protocol	Protocol Keyword
CU-SeeMe	cuseeme
FTP commands and responses	ftp-cmd
FTP token (enables tracing of the FTP tokens parsed)	ftp-token
H.323	h323
HTTP (Java applets)	http
Microsoft NetShow	netshow
UNIX R commands (rlogin, rexec, rsh)	rcmd
RealAudio	realaudio
RPC	rpc
SMTP	smtp

Table 26 **Application Protocol Keywords for the debug ip inspect Command (continued)**

Application Protocol	Protocol Keyword
SQL*Net	sqlnet
StreamWorks	streamworks
TFTP	tftp
VDOLive	vdolive

Interpreting Syslog and Console Messages Generated by CBAC

CBAC provides syslog messages, console alert messages, and audit trail messages. These messages are useful because they can alert you to network attacks and because they provide an audit trail that provides details about sessions inspected by CBAC. While they are generally referred to as error messages, not all error messages indicate problems with your system.

Audit trail and alert information is configurable on a per-application basis using the CBAC inspection rules.

The following types of messages can be generated by CBAC:

- [Denial-of-Service Attack Detection Error Messages](#)
- [SMTP Attack Detection Error Messages](#)
- [Java Blocking Error Messages](#)
- [FTP Error Messages](#)
- [Audit Trail Messages](#)

For explanations and recommended actions related to the error messages mentioned in this section, refer to the *Cisco IOS System Error Messages*.

Denial-of-Service Attack Detection Error Messages

CBAC detects and blocks denial-of-service attacks and notifies you when denial-of-service attacks occur. Error messages such as the following may indicate that denial-of-service attacks have occurred:

```
%FW-4-ALERT_ON: getting aggressive, count (550/500) current 1-min rate: 250
%FW-4-ALERT_OFF: calming down, count (0/400) current 1-min rate: 0
```

When %FW-4-ALERT_ON and %FW-4-ALERT_OFF error messages appear together, each “aggressive/calming” pair of messages indicates a separate attack. The preceding example shows one separate attack.

Error messages such as the following may indicate that a denial-of-service attack has occurred on a specific TCP host:

```
%FW-4-HOST_TCP_ALERT_ON: Max tcp half-open connections (50) exceeded for host
172.21.127.242.
%FW-4-BLOCK_HOST: Blocking new TCP connections to host 172.21.127.242 for 2 minutes
(half-open count 50 exceeded)
%FW-4-UNBLOCK_HOST: New TCP connections to host 172.21.127.242 no longer blocked
```

SMTP Attack Detection Error Messages

CBAC detects and blocks SMTP attacks (illegal SMTP commands) and notifies you when SMTP attacks occur. Error messages such as the following may indicate that an SMTP attack has occurred:

```
%FW-4-SMTP_INVALID_COMMAND: Invalid SMTP command from initiator (192.168.12.3:52419)
```

CBAC also detects a limited number of SMTP attack signatures. A signature in a SYSLOG message indicates a possible attack against the protected network, such as the detection of illegal SMTP commands in a packet. Whenever a signature is detected, the connection will be reset.

The Cisco IOS Firewall supports the following SMTP attack signatures:

Signature	Description
Mail: bad rcpt	Triggers on any mail message with a “pipe” () symbol in the recipient field.
Mail: bad from	Triggers on any mail message with a “pipe” () symbol in the “From:” field.
Mail: old attack	Triggers when “wiz” or “debug” commands are sent to the SMTP port.
Mail: decode	Triggers on any mail message with a “:decode@” in the header.
Majordomo	A bug in the Majordomo program will allow remote users to execute arbitrary commands at the privilege level of the server.

The following is a sample SMTP attack signature message:

```
02:04:55: %FW-4-TCP_MAJORDOMO_EXEC_BUG: Sig:3107:Majordomo Execute Attack - from
192.168.25.1 to 192.168.205.1:
```

Java Blocking Error Messages

CBAC detects and selectively blocks Java applets and notifies you when a Java applet has been blocked. Error messages such as the following may indicate that a Java applet has been blocked:

```
%FW-4-HTTP_JAVA_BLOCK: JAVA applet is blocked from (172.21.127.218:80) to
(172.16.57.30:44673).
```

FTP Error Messages

CBAC detects and prevents certain FTP attacks and notifies you when this occurs. Error messages such as the following may appear when CBAC detects these FTP attacks:

```
%FW-3-FTP_PRIV_PORT: Privileged port 1000 used in PORT command -- FTP client 10.0.0.1 FTP
server 10.1.0.1
%FW-3-FTP_SESSION_NOT_AUTHENTICATED: Command issued before the session is authenticated
-- FTP client 10.0.0.1
%FW-3-FTP_NON_MATCHING_IP_ADDR: Non-matching address 172.19.148.154 used in PORT command
-- FTP client 172.19.54.143 FTP server 172.16.127.242
```

Audit Trail Messages

CBAC provides audit trail messages to record details about inspected sessions. Audit trail information is configurable on a per-application basis using the CBAC inspection rules. To determine which protocol was inspected, use the responder's port number. The port number follows the responder's address. The following are sample audit trail messages:

```
%FW-6-SESS_AUDIT_TRAIL: tcp session initiator (192.168.1.13:33192) sent 22 bytes --  
responder (192.168.129.11:25) sent 208 bytes  
%FW-6-SESS_AUDIT_TRAIL: http session initiator (172.16.57.30:44673) sent 1599 bytes --  
responder (172.21.127.218:80) sent 93124 bytes
```

Turning Off CBAC

You can turn off CBAC using the **no ip inspect** global configuration command.

**Note**

The **no ip inspect** command removes all CBAC configuration entries and resets all CBAC global timeouts and thresholds to the defaults. All existing sessions are deleted and their associated access lists removed.

In most situations, turning off CBAC has no negative security impact because CBAC creates “permit” access lists. Without CBAC configured, no “permit” access lists are maintained. Therefore, no derived traffic (returning traffic or traffic from the data channels) can go through the firewall. The exception is SMTP and Java blocking. With CBAC turned off, unacceptable SMTP commands or Java applets may go through the firewall.

CBAC Configuration Examples

The following sections provide CBAC configuration examples:

- [Ethernet Interface Configuration Example](#)
- [ATM Interface Configuration Example](#)
- [Remote Office to ISP Configuration Example](#)
- [Remote Office to Branch Office Configuration Example](#)
- [Two-Interface Branch Office Configuration Example](#)
- [Multiple-Interface Branch Office Configuration Example](#)

The first example develops a CBAC inspection rule for specific protocols and a supporting access control list (ACL). This example focuses how to configure CBAC; it does not provide a complete router configuration and does not describe other elements of the configuration.

The next example develops a CBAC inspection rule for sites that might have remote traffic through an ATM interface. This example further illustrates on how to configure CBAC and emphasizes the application of the configuration rule at the interface, whatever that interface might be. This example does not provide a complete router configuration and does not describe other elements of the configuration.

The remote-office examples also focus on the firewall configuration but do not provide detailed descriptions of other configuration elements, such as the Basic Rate Interface (BRI) and dialer interface configurations.

Other examples provide more complete firewall configurations, further illustrating ways in which to apply CBAC.

In each example, configuring protocol inspection using CBAC has four components:

- Defining an access list with the appropriate permissions.
- Applying the ACL at an interface where you want to control access.
- Defining an inspection rule that includes the protocol that you want to inspect.
- Applying the inspection rule at an interface where you want to inspect traffic.

Ethernet Interface Configuration Example

This example looks at each of these four components. For this example, CBAC is being configured to inspect RTSP and H.323 protocol traffic inbound from the protected network on a router with two Ethernet interfaces. Interface Ethernet1/0 is the protected network and interface Ethernet1/1 is the unprotected network. The security policy for the protected site uses access control lists (ACLs) to restrict inbound traffic on the unprotected interface to specific ICMP protocol traffic, denying inbound access for TCP and UDP protocol traffic. Inbound access for specific protocol traffic is provided through dynamic access lists, which are generated according to CBAC inspection rules.

ACL 100 denies TCP and UDP traffic from any source or destination while permitting specific ICMP protocol traffic. The final deny statement is not required, but is included for explicitness—the final entry in any ACL is an implicit denial of all IP protocol traffic.

```
Router(config)# access-list 100 deny tcp any any
Router(config)# access-list 100 deny udp any any
Router(config)# access-list 100 permit icmp any any echo-reply
Router(config)# access-list 100 permit icmp any any time-exceeded
Router(config)# access-list 100 permit icmp any any packet-too-big
Router(config)# access-list 100 permit icmp any any traceroute
Router(config)# access-list 100 permit icmp any any unreachable
Router(config)# access-list 100 deny ip any any
```

ACL 100 is applied inbound at interface Ethernet1/1 to block all access from the unprotected network to the protected network.

```
Router(config)# interface Ethernet1/1
Router(config-if)# ip access-group 100 in
```

An inspection rule is created for “hquers” that covers two protocols: RTSP and H.323.

```
Router(config)# ip inspect name hquers rtsp
Router(config)# ip inspect name hquers h323
```

The inspection rule is applied inbound at interface Ethernet1/0 to inspect traffic from users on the protected network. When CBAC detects multimedia traffic from the protected network, CBAC creates dynamic entries in access list 100 to allow return traffic for multimedia sessions.

```
Router(config)# interface Ethernet1/0
Router(config-if)# ip inspect hquers in
```

ATM Interface Configuration Example

In this example, CBAC inspection (firewall protection) is required against inbound traffic on an ATM interface. This example might apply to sites where local hosts require access to hosts or services on a remote network. The security policy for this site uses access control lists (ACLs) to restrict inbound

traffic on the ATM interface to specific ICMP protocol traffic, denying inbound access for TCP and UDP protocol traffic. Inbound access for specific TCP and UDP protocol traffic is provided through dynamic access lists, which are generated according to CBAC inspection rules.

For information on how to select the interface on which to apply CBAC, refer to the [“Picking an Interface: Internal or External”](#) section.


Note

For Frame Relay or ATM interfaces, you can apply CBAC inspection rules separately on each sub-interface, even though the subinterfaces are physically connected through one interface.

```

! -----
! Create the Inspection Rule
! -----
!
! Create the CBAC inspection rule "test", allowing inspection of the protocol traffic
! specified by the rule. This inspection rule sets the timeout value to 30 seconds for
! each protocol (except for RPC). The timeout value defines the maximum time that a
! connection for a given protocol can remain active without any traffic passing through
! the router. When these timeouts are reached, the dynamic ACLs that are inserted to
! permit the returning traffic are removed, and subsequent packets (possibly even valid
! ones) are not permitted.
ip inspect name test cuseeme timeout 30
ip inspect name test ftp timeout 30
ip inspect name test h323 timeout 30
ip inspect name test realaudio timeout 30
ip inspect name test rpc program-number 100000
ip inspect name test streamworks timeout 30
ip inspect name test vdolive timeout 30
!
! -----
! Create the Access Control List
! -----
!
! In this example, ACL 105 denies all TCP and UDP protocol traffic. ICMP traffic from
! subnet 192.168.1.0 is permitted to allow access for routing and control traffic.
! ACL 105 specifies that only the return traffic for protocols defined in the
! inspection rule is allow access through the interface where this rule is applied. The
! final deny statement is added for explicitness.
access-list 105 deny TCP any any
access-list 105 deny UDP any any
access-list 105 permit icmp any any echo-reply
access-list 105 permit icmp any 192.168.1.0 0.0.0.255 time-exceeded
access-list 105 permit icmp any 192.168.1.0 0.0.0.255 packet-too-big
access-list 105 permit icmp any 192.168.1.0 0.0.0.255 traceroute
access-list 105 permit icmp any 192.168.1.0 0.0.0.255 unreachable
access-list 105 deny ip any any
!
! -----
! Apply the Inspection Rule and ACL
! -----
!
! In this example, the inspection rule "test" is applied to traffic at interface ATM3/0
! for connections initiated in the outbound direction; that is, from hosts that are
! located on a local network. CBAC creates dynamic access list entries for traffic
! initiated by local hosts. These dynamic entries allow inbound (returning) traffic for
! that connection. ACL 105 is applied at interface ATM3/0 in the inbound direction to
! block traffic initiated from hosts on a remote network that is not part of an
! existing connection.
interface ATM3/0
    ip address 10.1.10.1 255.0.0.0
    ip access-group 105 in

```

```

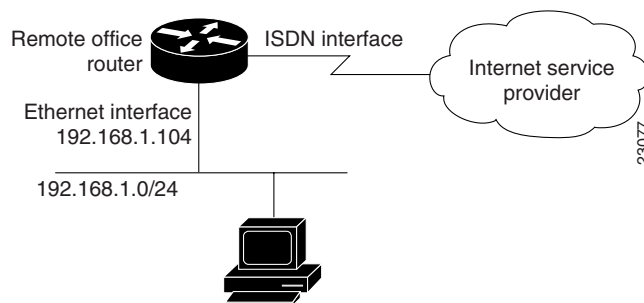
no ip directed-broadcast
ip inspect test out
no shutdown
atm clock INTERNAL
atm pvc 7 7 7 aal5snap
map-group atm

```

Remote Office to ISP Configuration Example

This example describes one possible Cisco IOS Firewall configuration for a remote office router connected to an Internet service provider (ISP). In this configuration, the site security policy allows hosts on the local network to initiate traffic to the ISP while traffic inbound to the router from the ISP is blocked at the ISDN interface. Specific ICMP control message traffic is permitted through the firewall. No mail or Web services are available from the local network. [Figure 23](#) illustrates this example.

Figure 23 Remote Office to ISP Sample Configuration



The firewall has two interfaces:

- An Ethernet interface connects to the internal protected network.
Interface Ethernet0 has no ACL applied to it, meaning that all traffic initiated on the LAN is allowed access to the ISP. In this configuration example, Network Address Translation (NAT) is not turned on, and the addresses on interface Ethernet0 are reserved IP addresses. In a production environment, addresses on Ethernet0 either must be registered network addresses, or you must turn on NAT to hide these inside addresses from being visible on the Internet.
- An ISDN Basic Rate Interface (BRI) connects the router to the ISP. In this example, a dialer profile is used to control the BRI interface. This means that the ACL and CBAC inspection rules are applied at the dialer interface, not directly at the physical ISDN (BRI) interface using a dialer map.

```

! -----
! General Cisco IOS Firewall Guidelines
! -----
! The following global configuration entries illustrate good security practices.
enable secret 5 <elided>
no ip source-route
no cdp run
!
! -----
! Create the CBAC inspection rule
! -----
! Create the CBAC inspection rule STOP to allow inspection of the protocol traffic
! specified by the rule.
ip inspect name STOP tcp
ip inspect name STOP ftp
ip inspect name STOP smtp

```

```

ip inspect name STOP h323
ip inspect name STOP rcmd
!
! -----
! Create Access Control List 105
! -----
! ACL 105 denies all IP protocol traffic except for specific ICMP control traffic.
! This means that only the return traffic for protocols defined in the
! inspection rule and the specified ICMP traffic is allowed access through the
! interface where this rule is applied.
!
! Deny broadcast messages with a source address of 255.255.255.255; this helps to
! prevent broadcast attacks.
access-list 105 deny ip host 255.255.255.255 any
!
! Add anti-spoofing protection by denying traffic with a source address matching a host
! on the Ethernet interface.
acl 105 deny ip 192.168.1.0 0.0.0.255 any
!
! ICMP traffic is not inspected by CBAC. To control the type of ICMP traffic at the
! interface, add static access list entries. This example has the following ICMP
! requirements: outgoing ping commands require echo-reply messages to come back,
! outgoing traceroute commands require time-exceeded messages to come back, path MTU
! discovery requires "too-big" messages to come back, and incoming traceroute
! messages must be allowed. Additionally, permit all "unreachable" messages to come
! back; that is, if a router cannot forward or deliver a datagram, it sends an ICMP
! unreachable message back to the source and drops the datagram.
access-list 105 permit icmp any any echo-reply
access-list 105 permit icmp any 192.168.1.0 0.0.0.255 time-exceeded
access-list 105 permit icmp any 192.168.1.0 0.0.0.255 packet-too-big
access-list 105 permit icmp any 192.168.1.0 0.0.0.255 traceroute
access-list 105 permit icmp any 192.168.1.0 0.0.0.255 unreachable
!
! Final deny for explicitness. This entry is not required but helps complete the access
! list picture. By default, the final entry in any access list is an implicit deny of
! IP protocol traffic. This ensures that the firewall blocks any traffic not explicitly
! permitted by the access list.
access-list 105 deny ip any any
!
! -----
! Configure the interface
! -----
! In this example, no ACLs or inspection rules are applied at interface Ethernet0,
! meaning that all traffic on the local network is allowed to go out. This assumes a
! high-level of trust for the users on the local network.
interface Ethernet0
    ip address 192.168.1.104 255.255.255.0
!
no ip directed-broadcast
!
! This example uses a dialer profile, so the ACL and CBAC inspection rules are applied
! at the dialer interface, not the physical BRI interface. The dialer pool-member
! command is used to associate the physical interface with a dialer profile.
interface BRI0
    no ip address
    no ip directed-broadcast
    encapsulation ppp
    dialer pool-member 1
    isdn switch-type basic-5ess
!
! -----
! Create the dialer profile.
! -----
! Through the dialer profile, the ACL and CBAC inspection rules are

```

```

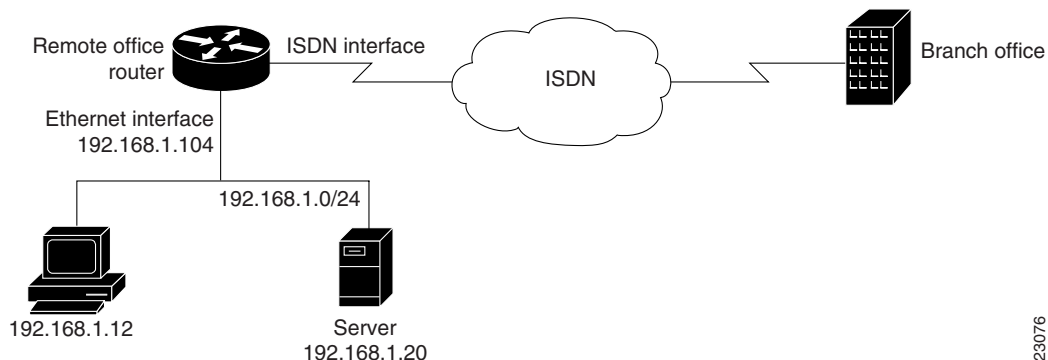
! applied to every pool member. In this example, the ACL is applied in, meaning that it
! applies to traffic inbound from the ISP. The CBAC inspection rule STOP is applied
! out, meaning that CBAC monitors the traffic through the interface and controls return
! traffic to the router for an existing connection.
interface Dialer0
    ip address negotiated
    ip access-group 105 in
    no ip directed-broadcast
    ip inspect STOP out
    encapsulation ppp
    dialer remote-name <ISP router>
    dialer idle-timeout 500
    dialer string <elided>
    dialer pool 1
    dialer-group 1
    ppp authentication callin
!
! -----
! Additional entries
! -----
! Configure the router to forward packets destined for an unrecognized subnet of
! a directly connected network.
ip classless
! Route traffic to the dialer interface.
ip route 0.0.0.0 0.0.0.0 Dialer0
! Include a dialer list protocol entry to specify the protocol that triggers dialing.
dialer-list 1 protocol ip permit
! Add a user name (name of the router your are configuring) and password for caller
! identification and password authentication with the ISP router.
username <router host name> password 5 <elided>

```

Remote Office to Branch Office Configuration Example

This example describes one possible Cisco IOS Firewall configuration for a remote office router connected to a branch office. In this configuration, the site security policy allows hosts on the local network to initiate traffic to the branch office. Mail or Web services are available from a server on the local network, and access to these services is available from the branch office. Traffic from the branch office, except for mail and Web traffic, is blocked at the outside interface. Specific ICMP control message traffic is permitted through the firewall. [Figure 24](#) illustrates this example.

Figure 24 Remote Office to Branch Office Sample Configuration



The firewall has two interfaces:

- An Ethernet interface connects to the internal protected network.

23076

Interface Ethernet0 has no ACL applied to it, meaning that all traffic initiated from the LAN is allowed access through the firewall.

- An ISDN Basic Rate Interface (BRI) connects the router to the branch office. In this example, a dialer profile is used to control the BRI interface. This means that the ACL and CBAC inspection rules are applied at dialer interface, not directly at the physical ISDN (BRI) interface.

```
! -----
! General firewall configuration guidelines
! -----
! The following global configuration entries illustrate good security practices.
enable secret 5 <elided>
no ip source-route
no cdp run
!
! -----
! Create the Inspection Rule
! -----
! Create the CBAC inspection rule STOP to allow inspection of the specified protocol
! traffic. Create the inspection rule GO to allow inspection of SMTP traffic.
ip inspect name STOP tcp
ip inspect name STOP ftp
ip inspect name STOP smtp
ip inspect name STOP h323
ip inspect name GO smtp
!
! -----
! Create Access Control Lists 106 and 51
! -----
! ACL 106 permits mail and Web traffic from any host to the specified server. ACL 106
! denies all other ip protocol traffic except for specific ICMP control traffic.
! This means that only the return traffic for protocols defined in the
! inspection rule and the specified ICMP traffic is allowed access through the
! interface where this rule is applied.
!
! Deny broadcast messages with a source address of 255.255.255.255; this helps to
! prevent broadcast attacks.
access-list 106 deny ip host 255.255.255.255 any
!
! Add anti-spoofing protection by denying traffic with a source address matching a host
! on the Ethernet interface.
access-list 106 deny ip 192.168.1.0 0.0.0.255 any
!
! ICMP traffic is not inspected by CBAC. To control the type of ICMP traffic at the
! interface, add static access list entries. This example has the following ICMP
! requirements: outgoing ping commands require echo-reply messages to come back,
! outgoing traceroute commands require time-exceeded messages to come back, path MTU
! discovery requires "too-big" messages to come back, and incoming traceroute must be
! allowed. Additionally, permit all "unreachable" messages to come back; that is, if a
! router cannot forward or deliver a datagram, it sends an ICMP unreachable message
! back to the source and drops the datagram.
access-list 106 permit icmp any any echo-reply
access-list 106 permit icmp any 192.168.1.0 0.0.0.255 time-exceeded
access-list 106 permit icmp any 192.168.1.0 0.0.0.255 packet-too-big
access-list 106 permit icmp any 192.168.1.0 0.0.0.255 traceroute
access-list 106 permit icmp any 192.168.1.0 0.0.0.255 unreachable
!
! Permit mail and Web access to a specific server.
access-list 106 permit tcp any host 192.168.1.20 eq smtp
access-list 106 permit tcp any host 192.168.1.20 eq www
!
! Final deny for explicitness. This entry is not required but helps complete the access
! list picture. By default, the final entry in any access list is an implicit deny of
! IP protocol traffic. This ensures that the firewall blocks any traffic not explicitly
```

```

! permitted by the access list.
access-list 106 deny ip any any
!
! -----
! Configure the interface.
! -----
! In this example, no ACLs or inspection rules are applied at interface Ethernet0,
! meaning that all traffic on the local network is allowed to go out. This assumes a
! high-level of trust for the users on the local network.
interface Ethernet0
    ip address 192.168.1.104 255.255.255.0
    no ip directed-broadcast
!
! This example uses a dialer profile, so the ACL and CBAC inspection rules are applied
! at the dialer interface, not the physical BRI interface. The dialer pool-member
! command is used to associate the physical interface with a dialer profile.
interface BRI0
    no ip address
    no ip directed-broadcast
    encapsulation ppp
    dialer pool-member 1
    isdn switch-type basic-5ess
!
! -----
! Apply the ACL and CBAC inspection rules at the dialer interface.
! -----
! Through the dialer profile, the ACL and CBAC inspection rules are
! applied to every pool member. In this example, the ACL is applied in, meaning that it
! applies to traffic inbound from the branch office. The CBAC inspection rule STOP is
! applied out, meaning that CBAC monitors the traffic and controls return traffic to
! the router for an existing connection. The CBAC inspection rule GO is applied in,
! protecting against certain types of DoS attacks as described in this document. Note
! that the GO inspection rule does not control return traffic because there is no ACL
! blocking traffic in that direction; however, it does monitor the connections.
interface Dialer0
    ip address <ISDN interface address>
    ip access-group 106 in
    no ip directed-broadcast
    ip inspect STOP out
    ip inspect GO in
    encapsulation ppp
    dialer remote-name <branch office router>
    dialer idle-timeout 500
    dialer string <elided>
    dialer pool 1
    dialer-group 1
    ppp authentication
!
! -----
! Additional entries
! -----
! Configure the router to forward packets destined for an unrecognized subnet of
! a directly connected network.
ip classless
! Route traffic to the dialer interface.
ip route 0.0.0.0 0.0.0.0 Dialer0
! Include a dialer list protocol entry to specify the protocol that triggers dialing.
dialer-list 1 protocol ip permit
! Add a user name (name of the router your are configuring) and password for caller
! identification and password authentication with the ISP router.
username <router host name> password 5 <elided>

```

Two-Interface Branch Office Configuration Example

This sample configuration file describes a firewall configured with CBAC. The firewall is positioned between a protected field office's internal network and a WAN connection to the corporate headquarters. CBAC is configured on the firewall in order to protect the internal network from potential network threats coming from the WAN side.

The firewall has two interfaces configured:

- Interface Ethernet0 connects to the internal protected network
- Interface Serial0 connects to the WAN with Frame Relay

```
! -----
! This first section contains some configuration that is not required for CBAC,
! but illustrates good security practices. Note that there are no
! services on the Ethernet side. Email is picked up via POP from a server on the
! corporate side.
! -----
!
hostname user1-examplecorp-fr
!
boot system flash c1600-fw1600-1
enable secret 5 <elided>
!
username user1 password <elided>
ip subnet-zero
no ip source-route
ip domain-name example.com
ip name-server 172.19.2.132
ip name-server 198.92.30.32
!
!
! -----
! The next section includes configuration required specifically for CBAC.
! -----
!
! The following commands define the inspection rule "myfw", allowing
! the specified protocols to be inspected. Note that Java applets will be permitted
! according to access list 51, defined later in this configuration.
ip inspect name myfw cuseeme timeout 3600
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http java-list 51 timeout 30
ip inspect name myfw rcmd timeout 3600
ip inspect name myfw realaudio timeout 3600
ip inspect name myfw smtp timeout 3600
ip inspect name myfw tftp timeout 30
ip inspect name myfw udp timeout 15
ip inspect name myfw tcp timeout 3600
!
! The following interface configuration applies the "myfw" inspection rule to
! inbound traffic at Ethernet 0. Since this interface is on the internal network
! side of the firewall, traffic entering Ethernet 0 is actually
! exiting the internal network. Applying the inspection rule to this interface causes
! inbound traffic (which is exiting the network) to be inspected; return traffic will
! only be permitted back through the firewall if part of a session which began from
! within the network.
! Also note that access list 101 is applied to inbound traffic at Ethernet 0.
! (Traffic blocked by the access list will not be inspected.)
interface Ethernet0
description ExampleCorp Ethernet chez user1
ip address 172.19.139.1 255.255.255.248
ip broadcast-address 172.19.131.7
```

```

no ip directed-broadcast
no ip proxy-arp
ip inspect myfw in
ip access-group 101 in
no cdp enable
!
interface Serial0
description Frame Relay (Telco ID 22RTQQ062438-001) to ExampleCorp HQ
no ip address
ip broadcast-address 0.0.0.0
encapsulation frame-relay IETF
no arp frame-relay
bandwidth 56
service-module 56k clock source line
service-module 56k network-type dds
frame-relay lmi-type ansi
!
! Note that the following interface configuration applies access list 111 to
! inbound traffic at the external serial interface. (Inbound traffic is
! entering the network.) When CBAC inspection occurs on traffic exiting the
! network, temporary openings will be added to access list 111 to allow returning
! traffic that is part of existing sessions.
!
interface Serial0.1 point-to-point
ip unnumbered Ethernet0
ip access-group 111 in
bandwidth 56
no cdp enable
frame-relay interface-dlci 16
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0.1
!
! The following access list defines "friendly" and "hostile" sites for Java
! applet blocking. Because Java applet blocking is defined in the inspection
! rule "myfw" and references access list 51, applets will be actively denied
! if they are from any of the "deny" addresses and allowed only if they are from
! either of the two "permit" networks.
!
access-list 51 deny    172.19.1.203
access-list 51 deny    172.19.2.147
access-list 51 permit 172.18.0.0 0.1.255.255
access-list 51 permit 192.168.1.0 0.0.0.255
access-list 51 deny    any
!
! The following access list 101 is applied to interface Ethernet 0 above.
! This access list permits all traffic that should be CBAC inspected, and also
! provides anti-spoofing. The access list is deliberately set up to deny unknown
! IP protocols, because no such unknown protocols will be in legitimate use.
!
access-list 101 permit tcp 172.19.139.0 0.0.0.7 any
access-list 101 permit udp 172.19.139.0 0.0.0.7 any
access-list 101 permit icmp 172.19.139.0 0.0.0.7 any
access-list 101 deny    ip any any
!
! The following access list 111 is applied to interface Serial 0.1 above.
! This access list filters traffic coming in from the external side. When
! CBAC inspection occurs, temporary openings will be added to the beginning of
! this access list to allow return traffic back into the internal network.
! This access list should restrict traffic that will be inspected by
! CBAC. (Remember that CBAC will open holes as necessary to permit returning traffic.)
! Comments precede each access list entry. These entries are not all specifically
! related to CBAC, but are created to provide general good security.
!

```



```
! Anti-spoofing.
access-list 111 deny ip 172.19.139.0 0.0.0.7 any
! Sometimes EIGRP is run on the Frame Relay link. When you use an
! input access list, you have to explicitly allow even control traffic.
! This could be more restrictive, but there would have to be entries
! for the EIGRP multicast as well as for the office's own unicast address.
access-list 111 permit igrp any any
!
! These are the ICMP types actually used...
! administratively-prohibited is useful when you are trying to figure out why
! you cannot reach something you think you should be able to reach.
access-list 111 permit icmp any 172.19.139.0 0.0.0.7 administratively-prohibited
!
! This allows network admins at headquarters to ping hosts at the field office:
access-list 111 permit icmp any 172.19.139.0 0.0.0.7 echo
!
! This allows the field office to do outgoing pings
access-list 111 permit icmp any 172.19.139.0 0.0.0.7 echo-reply
!
! Path MTU discovery requires too-big messages
access-list 111 permit icmp any 172.19.139.0 0.0.0.7 packet-too-big
!
! Outgoing traceroute requires time-exceeded messages to come back
access-list 111 permit icmp any 172.19.139.0 0.0.0.7 time-exceeded
!
! Incoming traceroute
access-list 111 permit icmp any 172.19.139.0 0.0.0.7 traceroute
!
! Permits all unreachable because if you are trying to debug
! things from the remote office, you want to see them. If nobody ever did
! any debugging from the network, it would be more appropriate to permit only
! port unreachable or no unreachable at all.
access-list 111 permit icmp any 172.19.139.0 0.0.0.7 unreachable
!
!
! These next two entries permit users on most ExampleCorp networks to Telnet to
! a host in the field office. This is for remote administration by the network admins.
access-list 111 permit tcp 172.18.0.0 0.1.255.255 host 172.19.139.1 eq telnet
access-list 111 permit tcp 192.168.1.0 0.0.0.255 host 172.19.139.1 eq telnet
!
! Final deny for explicitness
access-list 111 deny ip any any
!
no cdp run
snmp-server community <elided> RO
!
line con 0
exec-timeout 0 0
password <elided>
login local
line vty 0
exec-timeout 0 0
password <elided>
login local
length 35
line vty 1
exec-timeout 0 0
password 7 <elided>
login local
line vty 2
exec-timeout 0 0
password 7 <elided>
login local
line vty 3
```

```
exec-timeout 0 0
password 7 <elided>
login local
line vty 4
exec-timeout 0 0
password 7 <elided>
login local
!
scheduler interval 500
end
```

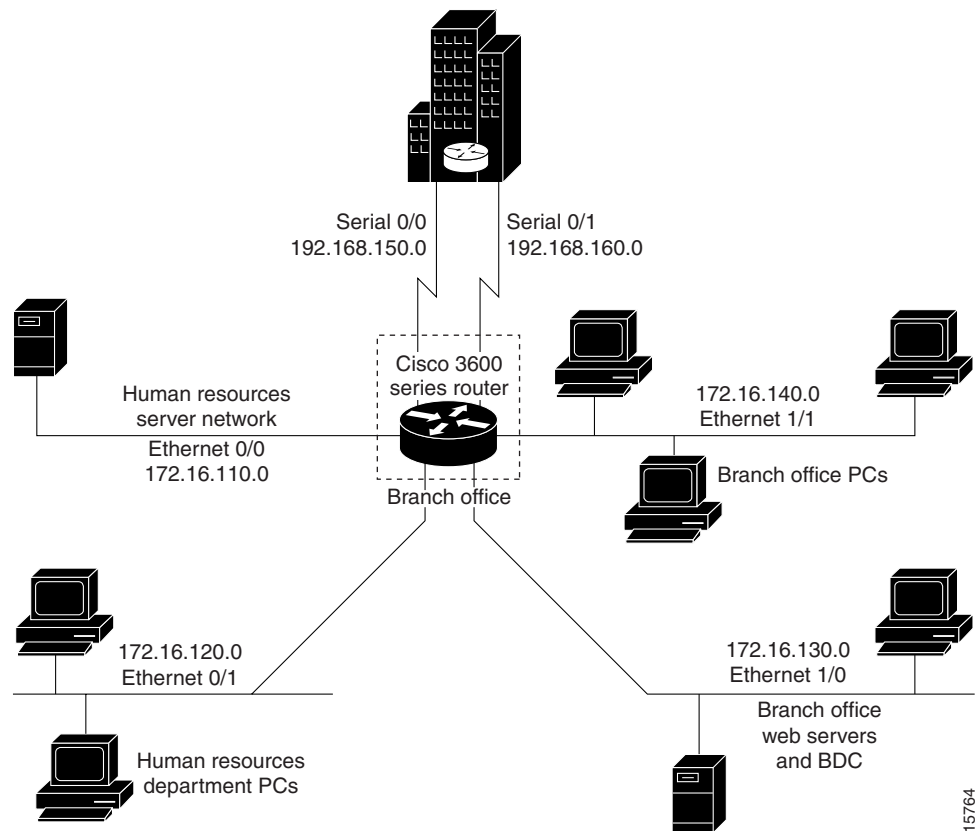
Multiple-Interface Branch Office Configuration Example

In this configuration example, a single Cisco 3600 series firewall router is positioned at a branch office. It has four internal networks and two WAN connections to the corporate headquarters. CBAC is configured on the firewall to protect two of the internal networks from potential network threats coming from the WAN side and from less secure internal networks. Anti-spoofing protection is added at each interface with client systems. [Figure 25](#) illustrates this configuration.

**Note**

This example shows a moderately high level of trust by the administrators toward the expected users. Additional protection could be added to this configuration for a situation in a lower level of trust. That configuration would include ICMP filtering statements, significantly more protocol and address control through the use of more restrictive access control lists, and anti-spoofing applied everywhere. This configuration does not contain those additional restrictions because that would detract from the CBAC example.

Figure 25 Sample Cisco IOS Firewall Application Environment



The branch office has this sample network configuration:

- Ethernet interface 0/0 supports the Human Resources department servers. This network includes an email (SMTP and POP3) host and a Windows NT server. The Windows NT server is the Primary Domain Controller (PDC) for the Human Resources domain and has a trust relationship with the rest of the company; however, it contains applications and databases that must not be accessed by the rest of the company or the other groups in the branch office. The devices on this LAN are accessible only by users in the Human Resources department on Ethernet interface 0/1. The Mail server must be able to send and receive email (through SMTP sessions) with all other devices. The Windows 95 machines can use this machine as their email server (for sending email through SMTP sessions) and as a repository for accumulating email that they can then download through POP3 sessions. No one else in the company is allowed to form POP3 sessions to any machine on this LAN.
- Ethernet interface 0/1 supports the Windows 95 computers in the Human Resources department. These users must have access to the Human Resources mail servers located on Ethernet interface 0/0 as well as access to the rest of the company. Access to the Windows NT server resources are controlled through the Windows NT permissions assigned to each user in the Windows NT domain.
- Ethernet interface 1/0 supports the branch office web servers, which can be accessed by everyone in the company. These servers use TCP ports 80 (HTTP) and 443 (SHTTP) for inbound Web access. This network also includes a backup domain controller (BDC) for the overall domain that is also used as file, print, and service server.

Ethernet interface 1/1 supports all users who are not in the Human Resources department. These users have no access to the Human Resources department servers, but they can access the other network interfaces and the serial interfaces for WAN connectivity. Serial interface 0/0 and 0/1 connect to the WAN with T1 links (links to corporate headquarters). In this sample configuration, the Domain Name System (DNS) servers are located somewhere within the rest of the company.

Additionally, network management (SNMP) and Telnet sessions are limited to the management network (192.168.55.0), which is located somewhere within the rest of the company across the serial interface.

```
! -----
! This first section contains some configuration that is not required
! for CBAC, but illustrates good security practices.
! -----
! Add this line to get timestamps on the syslog messages.
service timestamps log datetime localtime show-timezone
!
hostname Router1
!
boot system flash c3600-fw3600-1
!
! Configure AAA user authentication.
aaa new-model
aaa authentication login lista group tacacs+ enable
!
enable secret 5 <elided>
ip subnet-zero
!
! Disable source routing to help prevent spoofing.
no ip source-route
!
! Set up the domain name and server IP addresses.
ip domain-name example.com
ip name-server 192.168.55.132
ip name-server 192.168.27.32
!
! The audit-trail command enables the delivery of specific CBAC messages
! through the syslog notification process.
ip inspect audit-trail
!
! Establish the time-out values for DNS queries. When this idle-timer expires,
! the dynamic ACL entries that were created to permit the reply to a DNS request
! will be removed and any subsequent packets will be denied.
ip inspect dns-timeout 10
!
! -----
! The next section includes configuration statements required specifically for CBAC.
! -----
! Define the CBAC inspection rule "inspect1", allowing the specified protocols to be
! inspected. The first rule enables SMTP specific inspection. SMTP inspection causes
! the exchange of the SMTP session to be inspected for illegal commands. Any packets
! with illegal commands are dropped, and the SMTP session will hang and eventually
! time out.
ip inspect name inspect1 smtp timeout 30
!
! In the next two lines of inspect1, define the maximum time that each of the UDP and
! TCP sessions are allowed to continue without any traffic passing
! through the router. When these timeouts are reached, the dynamic ACLs that
! are inserted to permit the returning traffic are removed and subsequent packets
! (possibly even valid ones) will not be permitted.
ip inspect name inspect1 udp timeout 30
ip inspect name inspect1 tcp timeout 30
!
```

```

! Define the CBAC inspection rule "inspect2", allowing the specified protocols to be
! inspected. These rules are similar to those used in the inspection rule "inspect1,"
! except that on the interfaces where this rule is applied, SMTP sessions are not
! expected to go through; therefore, the SMTP rule element is not applied here.
ip inspect name inspect2 udp timeout 30
ip inspect name inspect2 tcp timeout 30
!
! -----
! The next section shows the Ethernet interface configuration statements for each
! interface, including access lists and inspections rules.
! -----
! Apply the "inspect1" inspection rule to sessions that are initiated in the outbound
! direction (toward the LAN) at Ethernet interface 0/0. All packets in these sessions
! will be inspected by CBAC. Provided that network traffic passes the Access Control
! List (ACL) restrictions, traffic is then inspected by CBAC for access through the
! Cisco Secure Integrated Software. Traffic blocked by the access list is not inspected
! by CBAC. Access list 110 is applied to outbound traffic on this interface.
interface Ethernet0/0
    description HR_Server Ethernet
    ip address 172.16.110.1 255.255.255.0
    ip access-group 110 out
    no ip directed-broadcast
    no ip proxy-arp
    ip inspect inspect1 out
    no cdp enable
!
! Apply access list 120 to inbound traffic on Ethernet interface 0/1.
! Applying access list 120 to inbound traffic provides anti-spoofing on this interface
! by dropping traffic with a source address matching the IP address on a network other
! than Ethernet 0/1. The IP helper address lists the IP address of the DHCP server on
! Ethernet interface 1/0.
interface Ethernet0/1
    description HR_client Ethernet
    ip address 172.16.120.1 255.255.255.0
    ip access-group 120 in
    ip helper-address 172.16.130.66
    no ip directed-broadcast
    no ip proxy-arp
    no cdp enable
!
! Apply the "inspect2" inspection rule to sessions that are initiated in the outbound
! direction (toward the LAN) at Ethernet interface 1/0. Provided that network traffic
! passes the Access Control List (ACL) restrictions, traffic is then inspected by CBAC
! through the Cisco Secure Integrated Software. Traffic blocked by the access list is
! not inspected
! by CBAC. Access list 130 is applied to outbound traffic on this interface.
interface Ethernet1/0
    description Web_server Ethernet
    ip address 172.16.130.1 255.255.255.0
    ip access-group 130 out
    no ip directed-broadcast
    no ip proxy-arp
    ip inspect inspect2 out
    no cdp enable
!
! Apply access list 140 to inbound traffic at Ethernet interface 1/1. This
! provides anti-spoofing on the interface by dropping traffic with a source address
! matching the IP address of a network other than Ethernet 1/1. The IP helper address
! lists the IP address of the DHCP server on Ethernet interface 1/0.
interface Ethernet1/1
    description Everyone_else Ethernet
    ip address 172.16.140.1 255.255.255.0
    ip access-group 140 in
    ip helper-address 172.16.130.66

```

```

no ip directed-broadcast

no ip proxy-arp
no cdp enable
!
! -----
! The next section configures the serial interfaces, including access lists.
! -----
! Apply access list 150 to Serial interfaces 0/0. This provides anti-spoofing on the
! serial interface by dropping traffic with a source address matching the IP address
! of a host on Ethernet interface 0/0, 0/1, 1/0, or 1/1.
interface Serial0/0
    description T1 to HQ
    ip address 192.168.150.1 255.255.255.0
    ip access-group 150 in
    bandwidth 1544
!
interface Serial1/1
    description T1 to HQ
    ip address 192.168.160.1 255.255.255.0
    ip access-group 150 in
    bandwidth 1544
!
! -----
! Configure routing information.
! -----
router igrp 109
network 172.16.0.0
network 192.168.150.0
network 192.168.160.0
!
! Define protocol forwarding on the firewall. When you turn on a related command,
! ip helper-address, you forward every IP broadcast in the ip forward protocol
! command list, including several which are on by default: TFTP (port 69),
! DNS (port 53), Time service (port 37), NetBIOS Name Server (port 137),
! NetBIOS Datagram Server (port 138), BOOTP client and server datagrams
! (ports 67 and 68), and TACACS service (port 49). One common
! application that requires helper addresses is Dynamic Host Configuration
! Protocol (DHCP). DHCP information is carried inside of BOOTP packets. The
! "no ip forward protocol" statements turn off forwarding for the specified protocols.
no ip forward-protocol udp netbios-ns
no ip forward-protocol udp netbios-dgm
no ip forward-protocol udp tacacs
no ip forward-protocol udp tftp
ip forward-protocol udp bootpc
!
! Add this line to establish where router SYSLOG messages are sent. This includes the
! CBAC messages.
logging 192.168.55.131
!
! -----
! Define the configuration of each access list.
! -----
! Defines Telnet controls in access list 12.
access-list 12 permit 192.168.55.0 0.0.0.255
!
! Defines SNMP controls in access list 13.
access-list 13 permit 192.168.55.12
access-list 13 permit 192.168.55.19
!
! Access list 110 permits TCP and UDP protocol traffic for specific ports and with a
! source address on Ethernet interface 0/1. The access list denies IP protocol traffic
! with any other source and destination address. The access list permits ICMP access
! for any source and destination address. Access list 110 is deliberately set up to

```

```
! deny unknown IP protocols because no such unknown protocols will be in legitimate
! use. Access list 110 is applied to outbound traffic at Ethernet interface 0/0. In ACL
! 110, network traffic is being allowed access to the ports on any server on the HR
! server network. In less trusted environments, this can be a security problem;
! however, you can limit access more severely by specifying specific destination
! addresses in the ACL statements.
access-list 110 permit tcp 172.16.120.0 0.0.0.255 any eq smtp
access-list 110 permit tcp 172.16.120.0 0.0.0.255 any eq pop3
access-list 110 permit tcp 172.16.120.0 0.0.0.255 any eq 110
access-list 110 permit udp any any eq 137
access-list 110 permit udp any any eq 138
access-list 110 permit udp any any eq 139
access-list 110 permit icmp any any
access-list 110 deny ip any any!
!
! Access-list 120 permits TCP, UDP, and ICMP protocol traffic with a source address
! on Ethernet interface 0/1, but denies all other IP protocol traffic. Access list
! 120 is applied to inbound traffic on Ethernet interface 0/1.
access-list 120 permit tcp 172.16.120.0 0.0.0.255 any
access-list 120 permit udp 172.16.120.0 0.0.0.255 any
access-list 120 permit icmp 172.16.120.0 0.0.0.255 any
access-list 120 deny ip any any
!
! Access list 130 permits TCP, UDP, and ICMP protocol traffic for specific ports and
! with any source and destination address. It opens access to the web server and to
! all NBT services to the rest of the company, which can be controlled through the
! trust relations on the Windows NT servers. The bootpc entry permits access to the
! DHCP server. Access list 130 denies all other IP protocol traffic. Access list 130 is
! applied to outbound traffic at Ethernet interface 1/0.
access-list 130 permit tcp any any eq www
access-list 130 permit tcp any any eq 443
access-list 130 permit tcp any any eq 110
access-list 130 permit udp any any eq 137
access-list 130 permit udp any any eq 138
access-list 130 permit udp any any eq 139
access-list 130 permit udp any any eq bootpc
access-list 130 permit icmp any any
access-list 130 deny ip any any
!
! Access list 140 permits TCP, UDP, and ICMP protocol traffic with a source address on
! Ethernet interface 1/1, and it denies all other IP protocol traffic. Access list 140
! is applied to inbound traffic at Ethernet interface 1/1.
access-list 140 permit tcp 172.16.140.0 0.0.0.255 any
access-list 140 permit udp 172.16.140.0 0.0.0.255 any
access-list 140 permit icmp 172.16.140.0 0.0.0.255 any
access-list 140 deny ip any any
!
! Access list 150 denies IP protocol traffic with a source address on Ethernet
! interfaces 0/0, 0/1, 1/0, and 1/1, and it permits IP protocol traffic with any other
! source and destination address. Access list 150 is applied to inbound traffic
! on each of the serial interfaces.
access-list 150 deny ip 172.16.110.0 0.0.0.255 any
access-list 150 deny ip 172.16.120.0 0.0.0.255 any
access-list 150 deny ip 172.16.130.0 0.0.0.255 any
access-list 150 deny ip 172.16.140.0 0.0.0.255 any
access-list 150 permit ip any any
!
! Disable Cisco Discovery Protocol.
no cdp run
!
snmp-server community <elided> ro 13
tacacs-server host 192.168.55.2
tacacs-server key <elided>
!
```

```

! -----
! Configures the router console port and the virtual terminal line interfaces,
! including AAA authentication at login. Authentication is required for users defined
! in "lista." Access-class 12 is applied on each line, restricting Telnet access to
! connections with a source address on the network management network.
! -----
line console 0
exec-timeout 3 00
login authentication lista
line aux 0
exec-timeout 3 00
login authentication lista
line vty 0
    exec-timeout 1 30
    login authentication lista
    access-class 12 in
line vty 1
    exec-timeout 1 30
    login authentication lista
    access-class 12 in
line vty 2
    exec-timeout 1 30
    login authentication lista
    access-class 12 in
line vty 3
    exec-timeout 1 30
    login authentication lista
    access-class 12 in
line vty 4
    exec-timeout 1 30
    login authentication lista
    access-class 12 in
!
end

```

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Application Firewall—Instant Message Traffic Enforcement

The Application Firewall—Instant Message Traffic Enforcement feature enables users to define and enforce a policy that specifies which instant messenger traffic types are allowed into the network. Thus, the following additional functionality can also be enforced:

- Configuration of firewall inspection rules
- Deep packet inspection of the payload, looking for services such as text chat

History for the Application Firewall—Instant Message Traffic Enforcement Feature

Release	Modification
12.4(4)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions for Application Firewall—Instant Message Traffic Enforcement, page 2](#)
- [Information About Application Firewall—Instant Message Traffic Enforcement, page 2](#)
- [How to Define and Apply an Application Policy to a Firewall for Inspection, page 3](#)
- [Configuration Examples for Setting Up an Instant Messenger Traffic Inspection Engine, page 7](#)
- [Additional References, page 8](#)
- [Command Reference, page 9](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Restrictions for Application Firewall—Instant Message Traffic Enforcement

If an instant messenger traffic enforcement policy is configured on a Cisco IOS router with a server command, traffic destined to other services (such as Telnet, FTP, SMTP) that is running on the instant message server's IP address will also be treated as IM traffic by the Cisco IOS router. Thus, access to the other services is prevented through the Cisco IOS firewall; however, this limitation is not a problem for most IM application users who are connecting from a user's network.

Information About Application Firewall—Instant Message Traffic Enforcement

Before creating an application firewall policy for instant message traffic enforcement, you should understand the following concept:

- [What Is an Application Policy?, page 2](#)
- [Instant Messenger Application Policy Overview, page 2](#)

What Is an Application Policy?

The application firewall uses an application policy, which consists of a collection of static signatures, to detect security violations. A static signature is a collection of parameters that specify protocol conditions that must be met before an action is taken. These protocol conditions and reactions are defined by the end user via the command-line interface (CLI) to form an application policy.

Instant Messenger Application Policy Overview

Cisco IOS application firewall has been enhanced to support instant native messenger application policies. Thus, the Cisco IOS firewall can now detect and prohibit user connections to instant messenger servers for the AOL Instant Messenger (AIM), Yahoo! Messenger, and MSN Messenger instant messaging services. This functionality controls all connections for supported services, including text, voice, video, and file-transfer capabilities. The three applications can be individually denied or permitted. Each service may be individually controlled so that text-chat service is allowed, and voice, file transfer, video, and other services are restricted. This functionality augments existing Application Inspection capability to control IM application traffic that has been disguised as HTTP (web) traffic.

**Note**

If an instant messenger application is blocked, the connection will be reset and a syslog message will be generated, as appropriate.

How to Define and Apply an Application Policy to a Firewall for Inspection

This section contains the following procedures:

- [Defining an Application Policy to Permit or Deny Instant Messenger Traffic, page 3](#)
- [Applying an Instant Messenger Traffic Application Policy to a Firewall for Inspection, page 6](#)

Defining an Application Policy to Permit or Deny Instant Messenger Traffic

Use this task to create an instant messenger application firewall policy.

Prerequisites

Before defining and enabling an application policy for instant messenger traffic, you must have already properly configured your router with a Domain Name System (DNS) server IP address via the **ip domain lookup** command and the **ip name-server** command.

The IP address of the DNS server configured on the Cisco IOS router must be the same as that configured on all PCs connecting to the IM servers from behind the Cisco IOS firewall.



Note

If at least one DNS name was not specified for resolution under any of the application policies for IM protocols (AOL, Yahoo, or MSN), you do not need to configure the DNS server IP address in the Cisco IOS router.

Restrictions

Although application firewall policies are defined in global configuration mode, only one global policy for a given protocol is allowed per interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **appfw policy-name** *policy-name*
4. **application** *protocol*
5. **audit-trail** {on | off}
6. **server** {permit | deny} {name *string* | ip-address {*ip-address* | range *ip-address-start ip-address-end*}
7. **timeout** *seconds*
8. **service** {default | text-chat} **action** {allow [alarm] | reset [alarm] | alarm}
9. **alert** {on | off}
10. **exit**
11. **show appfw** {configuration | dns cache} [*policy policy-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	appfw policy-name <i>policy-name</i> Example: Router(config)# appfw policy-name my_policy	Defines an application firewall policy and enters application firewall policy configuration mode.
Step 4	application <i>protocol</i> Example: Router(cfg-appfw-policy)# application im aol	Allows you to configure inspection parameters for a given protocol. <ul style="list-style-type: none"> <i>protocol</i>— One of the following options: <ul style="list-style-type: none"> http (HTTP traffic will be inspected) im {aol yahoo msn} (Traffic for the specified instant messenger application will be inspected) This command puts the router in appfw-policy-protocol configuration mode, where “protocol” is dependent upon the specified protocol.
Step 5	audit-trail {on off} Example: Router(cfg-appfw-policy-aim)# audit-trail on	(Optional) Enables message logging for established or torn-down connections. If this command is not issued, the default value specified via the ip inspect audit-trail command will be used.
Step 6	server {permit deny} {name <i>string</i> ip-address {ip-address range ip-address-start ip-address-end} Example: Router(cfg-appfw-policy-aim)# server permit name login.cat.aol.com	Controls access to instant messenger servers. Note The server command helps the instant messenger application engine to recognize the port-hopping instant messenger traffic and to enforce the security policy for that instant messenger application; thus, if this command is not issued, the security policy cannot be enforced if IM applications use port-hopping techniques. To deploy IM traffic enforcement policies effectively, it is recommended that you issue the appropriate server command.

	Command or Action	Purpose
Step 7	<p>timeout <i>seconds</i></p> <p>Example: Router(cfg-appfw-policy-aim)# timeout 30</p>	<p>(Optional) Specifies the elapsed length of time before an inactive connection is torn down.</p> <ul style="list-style-type: none"> <i>seconds</i>—Available timeout range: 5 to 43200 (12 hours). <p>If this command is not issued, the default value specified via the ip inspect tcp idle-time command will be used.</p> <p>Note Some IM applications continue to send “keepalive-like” packets that effectively prevent timeout even when the user is idle.</p>
Step 8	<p>service {default text-chat} action {allow [alarm] reset [alarm] alarm}</p> <p>Example: Router(cfg-appfw-policy-aim)# service default action reset</p>	<p>(Optional) Specifies an action when a specific service is detected in the instant messenger traffic.</p> <ul style="list-style-type: none"> If a specific action is not specified for a service, the service default command will be performed. If the service default command is not specified for an application, the action is considered “reset” by the system.
Step 9	<p>alert {on off}</p> <p>Example: Router(cfg-appfw-policy-aim)# alert on</p>	<p>(Optional) Enables message logging when events, such as the start of a text-chat, begin.</p> <p>If this parameter is not configured, the global setting for the ip inspect alert-off command will take effect.</p>
Step 10	<p>exit</p> <p>Example: Router(cfg-appfw-policy-aim)# exit</p> <p>Example: Router(cfg-appfw-policy)# exit</p> <p>Example: Router(config)# exit</p>	<p>(Optional) Exits application firewall policy <i>protocol</i> configuration mode, application firewall policy configuration mode, and global configuration mode.</p>
Step 11	<p>show appfw {configuration dns cache} [policy <i>policy-name</i>]</p> <p>Example: Router# show appfw dns cache policy abc</p>	<p>(Optional) Displays the IP addresses that have been resolved by the DNS server and stored in the DNS cache of the IM traffic policy enforcement component of the Cisco IOS router.</p> <ul style="list-style-type: none"> If you don’t indicate a specific policy via the policy <i>policy-name</i> option, IP addresses gathered for all DNS names for all policies are displayed.

Troubleshooting Tips

Resolved IP addresses are never “timed out” and not automatically removed from the DNS cache. Thus, if you find an obsolete IP address in the instant messenger database (DNS cache), you can issue the **clear appfw dns cache** command to remove the IP address and prevent the address from being interpreted by the router as that of an IM server.

Always allow a couple of minutes for the DNS cache to populate after configuring the **server** command (with the **name string** option) in an application firewall policy for IM applications.

If you do not want the DNS resolver to send periodic queries, do not use the **server** command (with the **name string** option); instead, use the **server** command (with the **ip address** option).

If you issue the **server** command (with the **name string** option), ensure that you specify the name of every DNS server for an IM application in your policy. Always be alert to new names.

What to Do Next

After you have successfully defined an application policy for instant message traffic inspection, you must apply the policy to an inspection rule. Thereafter, the inspection rule must be applied to an interface. For information on completing this task, see the section “[Applying an Instant Messenger Traffic Application Policy to a Firewall for Inspection](#).”

Applying an Instant Messenger Traffic Application Policy to a Firewall for Inspection

Use this task to apply an IM application policy to an inspection rule, followed by applying the inspection rule to an interface.

Prerequisites

You must have already defined an application policy (as shown in the section “[Defining an Application Policy to Permit or Deny Instant Messenger Traffic](#)”).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip inspect name** *inspection-name* **appfw** *policy-name*
4. **interface** *type number*
5. **ip inspect** *inspection-name* {**in** | **out**}
6. **exit**
7. **exit**
8. **show appfw configuration** [*name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip inspect name inspection-name appfw policy-name Example: Router(config)# ip inspect name firewall appfw mypolicy	Defines a set of inspection rules for the application policy. <ul style="list-style-type: none"> <i>policy-name</i>—Must match the policy name specified via the appfw policy-name command.
Step 4	interface type number Example: Router#(config)# interface FastEthernet0/0	Configures an interface type and enters interface configuration mode.
Step 5	ip inspect inspection-name {in out} Example: Router#(config-if)# ip inspect firewall in	Applies the inspection rules (defined in Step 3) to all traffic entering the specified interface. <ul style="list-style-type: none"> The <i>inspection-name</i> argument must match the inspection name defined via the ip inspect name command.
Step 6	exit Example: Router#(config-if)# exit	Exits interface configuration mode.
Step 7	exit Example: Router(config)# exit	Exits global configuration mode.
Step 8	show appfw configuration [name] Example: Router# show appfw configuration	(Optional) Displays application firewall policy configuration information.

Configuration Examples for Setting Up an Instant Messenger Traffic Inspection Engine

This section contains the following configuration example:

- [Instant Messenger Application Policy Configuration: Example, page 8](#)

Instant Messenger Application Policy Configuration: Example

The following example shows to configure application policy “my-im-policy,” which allows text-chat for Yahoo! instant messenger users and blocks instant messenger traffic for all other users:

```
appfw policy-name my-im-policy
  application http
  port-misuse im reset
!
  application im yahoo
  server permit name scs.msg.yahoo.com
  server permit name scsa.msg.yahoo.com
  server permit name scsb.msg.yahoo.com
  server permit name scsc.msg.yahoo.com
  service text-chat action allow
  service default action reset
!
  application im aol
  server deny name login.oscar.aol.com
!
  application im msn
  server deny name messenger.hotmail.com
!
ip inspect name test appfw my-im-policy

interface FastEthernet0/0
  description Inside interface
  ip inspect test in
```

The **port-misuse im** command blocks all the three IM applications going through the HTTP protocol. It is always recommended that you block IM activity through HTTP and allow IM traffic to pass, if at all, through its native port.

The **server permit** commands help to identify all the servers for Yahoo! messenger services. A connection to any one of the specified servers will be recognized by the firewall as a Yahoo! IM session—even if the Yahoo! client uses port-hopping techniques (which can be accomplished by using server port-numbers such as 25 instead of the standard 5050.)

If a **server permit** command is not issued within the **application im yahoo** command, the Cisco IOS firewall will classify only the traffic going to server port 5050 as Yahoo! messenger traffic. Because the port classification scheme breaks if any of the Yahoo! clients are configured to use a port other than 5050, it is more reliable to have **server permit** command entries instead of relying on the port classification method.

The **server deny** commands under other IM applications deny connection to respective servers. This action operates at the network layer connection level—not at the application session level. When traffic is denied, the TCP connection to the server is denied, no data traffic is allowed, and all packets are dropped in the firewall.

Additional References

The following sections provide references related to the Application Firewall—Instant Message Traffic Enforcement feature.

Related Documents

Related Topic	Document Title
Application firewall: configure a firewall to detect and prohibit HTTP connections	<i>HTTP Inspection Engine</i> , Cisco IOS Release 12.3(14)T feature module
Additional firewall configuration tasks and overview information	The section “Traffic Filtering, Firewalls, and Virus Detection” in the <i>Cisco IOS Security Configuration Guide</i>
Firewall commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<i>Cisco IOS Security Command Reference, Release 12.4T</i>

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this

module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **alert**
- **application (application firewall policy)**
- **audit-trail**
- **clear appfw dns cache**
- **server (application firewall policy)**
- **service**
- **show appfw**
- **timeout**

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Cisco IOS Firewall MIB

First Published: February 27, 2006

Last Updated: February 27, 2006

The Cisco IOS Firewall MIB feature introduces support for the Cisco Unified Firewall MIB, which helps to manage and monitor firewall performance via Simple Network Management Protocol (SNMP). Statistics can be collected and monitored via standards-based SNMP techniques for firewall features such as stateful packet inspection and URL filtering.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Cisco IOS Firewall MIB](#)” section on [page 19](#).

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites, page 2](#)
- [Restrictions for Cisco IOS Firewall MIB, page 2](#)
- [Information About Cisco IOS Firewall MIB, page 2](#)
- [How to Use Firewall MIBs, page 7](#)
- [Configuration Examples for Cisco IOS Firewall MIB Monitoring, page 9](#)
- [Additional References, page 16](#)
- [Command Reference, page 17](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites

Before you can provide firewall connection and URL filtering statistics via SNMP, you must set up the firewall by performing the following tasks:

- Configure a firewall policy via the **ip inspect name** command.
- Enable the firewall by applying the firewall on a target via the **interface** command followed by the **ip inspect** command.
- Enable URL filtering, if applicable, via the **ip urlfilter server vendor** command.

You must also enable SNMP on the router. For more information on enabling SNMP, see the section [“Enabling SNMP for Firewall Sessions”](#) later in this document.

Restrictions for Cisco IOS Firewall MIB

- Cisco does not support all of the MIB variables that are defined in the Cisco Unified Firewall MIB. For a list of variables that are supported by this feature, see [Table 1](#), [Table 2](#), and [Table 3](#).
- MIB statistics are not provided when the firewall is configured using CPL.

Memory and Performance Impact

Depending on the number of targets that have a configured firewall and the number of configured URL filtering servers, the MIB functionality can create an adverse impact on memory. For each firewall policy that is configured on your system, more memory is required to store SNMP statistics.

The following information defines the minimum memory requirements for connection statistics only:

- Global connection statistics: approximately 64 bytes.
- Protocol-specific statistics: multiply the number of configured protocols by 56 to determine the minimum memory requirement.
- Policy-target-protocol statistics: multiply the number of configured protocols and the number of targets for which the firewall policies are configured by 48 to determine the minimum memory requirement.

The following information defines the minimum memory requirements for URL filtering statistics only:

- Global URL filtering statistics: approximately 96 bytes.
- URL filtering server-specific statistics: multiply the number of configured URL filtering servers by 40 to determine the minimum memory requirement.

Information About Cisco IOS Firewall MIB

To use Cisco IOS Firewall MIBs to monitor firewall performance, you should understand the following concepts:

- [Connection Statistics, page 3](#)
- [URL Filtering Statistics, page 4](#)

Connection Statistics

Connection statistics are a record of the firewall traffic streams that have attempted to flow through the firewall system. Connection statistics can be displayed on a global basis (that is, an aggregate of all connection statistics for the entire router), protocol-specific basis, or a firewall-policy-specific basis. The Firewall can allow, drop, or deny the connection based on firewall policies and firewall resources.

[Table 1](#) lists all supported connection statistics—global, protocol-specific¹, or firewall-policy-specific²—that are available via SNMP.

Table 1 *Connection Statistics*

Statistic Type	Connection Type	Description
<ul style="list-style-type: none"> Global Protocol-specific Firewall-policy-specific 	Aborted	Number of connections that were abnormally terminated after successful establishment
<ul style="list-style-type: none"> Global Protocol-specific Firewall-policy-specific 	Active	Number of connections that are currently active
<ul style="list-style-type: none"> Global Protocol-specific Firewall-policy-specific 	Attempted	Number of connection attempts sent to the firewall system
Global	Embryonic	Number of embryonic-application-layer connections
Global	Expired	Number of connections that were active but have since been terminated normally
<ul style="list-style-type: none"> Global Protocol-specific 	Five-Minute Connection Rate	Number of connection attempts that were established per second, averaged over the last 300 seconds
<ul style="list-style-type: none"> Global Protocol-specific Firewall-policy-specific 	Half-Open	Number of connections that are currently in the process of being established (half-open)
<ul style="list-style-type: none"> Global Protocol-specific 	One-Minute Connection Rate	Number of connection attempts that were establish per second, averaged over the last 60 seconds

1. All protocol-based statistics can be accessed with the following index—protocol, which is the protocol of interest such as ICMP, UDP, TCP, HTTP, and FTP. The protocols, which are a predefined static list, must be specified
2. All firewall-policy-specific statistics can be accessed with the following indexes: Policy, which is the name of the firewall security policy of interest. (The policy name is specified via the `ip inspect name` command.) Policy target type, which is the type of physical or virtual target that has the policy name applied to it. Currently, only include interface targets are supported.

Table 1 *Connection Statistics (continued)*

Statistic Type	Connection Type	Description
<ul style="list-style-type: none"> Global Protocol-specific Firewall-policy-specific 	Policy Declined	Number of connection attempts that were declined due to application of a firewall security policy
<ul style="list-style-type: none"> Global Protocol-specific Firewall-policy-specific 	Resource Declined	Number of connection attempts that were declined due to firewall resource constraints

URL Filtering Statistics

URL Filtering feature provides an Internet management application that allows you to control web traffic for a given host or user on the basis of a specified security policy. URL filtering statistics include the status of distinct URL filtering servers that are configured on the firewall and the impact of the performance of the URL filtering servers on the latency and throughput of the firewall.

[Table 2](#) and [Table 3](#) list all supported URL filtering statistics—on a global basis or per server—that are available via SNMP.

Table 2 *Global URL Filtering Statistics (across all servers)*

Connection Type	Description
Five minute URL Filtering Requests Declined Rate	Rate at which URL access requests were declined by the firewall via the URL filtering server or the firewall exclusive domain configuration, averaged over the last 300 seconds.
Five minute URL Filtering Requests Resource Dropped Rate	Rate at which URL access requests were dropped by the firewall due to firewall resource constraints, averaged over the last 300 seconds.
One minute URL Filtering Requests Declined Rate	Rate at which URL access requests were declined by the firewall via the URL filtering server or the firewall exclusive domain configuration, averaged over the last 60 seconds.
One minute URL Filtering Requests Resource Dropped Rate	Rate at which URL access requests were dropped by the firewall due to firewall resource constraints, averaged over the last 60 seconds.
URL Filtering Allow Mode On	Displays whether the firewall has allowed or discarded URL requests when the URL filtering server is not available. Returns a “true” statistics if the firewall allows all requested URLs to be retrieved from the remote host when the URL server is not available; returns a “false” statistic if the firewall discards all URL.
URL Filtering Allow Mode Requests Allowed	Number of URL access requests that were allowed by the firewall when the URL filtering server was not available.

Table 2 **Global URL Filtering Statistics (across all servers) (continued)**

Connection Type	Description
URL Filtering Allow Mode Requests Denied	Number of URL access requests that were denied by the firewall when the URL filtering server was not available.
URL Filtering Enabled	Displays whether or not URL filtering is enabled. Returns a “false” statistic if the firewall will not perform URL filtering, even if the system contains configuration information that pertains to other aspects of URL filtering.
URL Filtering Late Responses	Number of responses from the URL filtering server that were received after the original URL access request was dropped by the Firewall.
URL Filtering Requests Allowed	Number of URL access requests allowed by the firewall via the use of the URL filtering server or the firewall exclusive domain configuration.
URL Filtering Requests Declined	Number of URL access requests that were declined by the firewall via the URL filtering server or the firewall exclusive domain configuration.
URL Filtering Requests Processed	Number of URL access requests that were processed by the firewall.
URL Filtering Request Process Rate	Number of URL access requests that were processed per second by the firewall, averaged over the last 300 seconds.
URL Filtering Requests Resource Dropped	Number of incoming URL access requests that were dropped by the Firewall due to firewall resource constraints.
URL Filtering Responses Resource Dropped	Number of responses to URL access requests from remote hosts that were dropped by the firewall due to resource constraints while the firewall was waiting for a response from the URL filtering server.
URL Filtering Server Timeouts	Number of times the firewall did not receive a response from the URL Filtering server.

Table 3 *Per server URL Filtering Statistics*

Connection Type	Description
URL Filtering Protocol Version	Version of the transport protocol that is used by the firewall to communicate with the URL filtering server. For TCP, valid version values are 1 and 4. For UDP, 1 is the only valid version.
URL Filtering Server Late Responses	Number of URL access responses received by the firewall from the URL filtering server after the original URL access request was dropped by the firewall.
URL Filtering Server Requests	Number of URL access requests forwarded by the firewall to the URL filtering server.
URL Filtering Server Requests Allowed	Number of URL access requests allowed by the URL filtering server. The count does not include late responses.
URL Filtering Server Requests Declined	Number of URL access requests declined by the URL filtering server. The count does not include late responses.
URL Filtering Server Responses	Number of URL access responses received by the firewall from the URL filtering server. The count does not include late responses.
URL Filtering Server Response Time Rate	Average round-trip response time of the URL filtering server, averaged over the last 300 seconds. A value of zero indicates that there was insufficient data to compute this value over the last time interval.
URL Filtering Server Status	Status of the URL filtering server: ONLINE or OFFLINE.
URL Filtering Server Timeouts	Number of times the URL filtering server failed to respond to URL access requests sent by the firewall.
URL Filtering Server Transport Protocol	Transport protocol that is used by the firewall to communicate with the URL filtering server. The protocol will be TCP, UDP, or DEFAULT. DEFAULT is used in implementations that do not explicitly specify a transport protocol.
URL Filtering Server Vendor	Vendor who provided the URL filtering server. Currently only Websense and N2H2 servers are supported.

A URL filtering server is identified by the following items, which also form the indexes into the URL filtering server statistics table:

- URL Filtering Server Address Type—Type of IP address of the URL filtering server. For example, IPv4 or IPv6.
- URL Filtering Server Address—IP address of the URL filtering server.

- URL Filtering Server Port—Port number that the URL filtering server uses to receive filtering requests.

How to Use Firewall MIBs

This section contains the following task:

- [Enabling SNMP for Firewall Sessions, page 7](#)
- [Verifying Firewall Connection and URL Filtering Statistics, page 8](#)

Enabling SNMP for Firewall Sessions

Use this task to enable SNMP for firewall-related session management.

Prerequisites

Before you can begin monitoring firewall performance via SNMP, you must set up the firewall by performing the following tasks:

- Configure a firewall policy via the **ip inspect name** command.



Note Statistics are collected only for protocols that are specified via the **ip inspect name** command.

- Enable the firewall by applying the firewall on a target via the **interface** command followed by the **ip inspect** command.
- Enable URL filtering, if applicable, via the **ip urlfilter server vendor** command.

Firewall MIB Traps

To receive firewall MIB traps, you need a management station, and you must enable the **snmp-server enable trap firewall serverstatuschange** command (as shown in the configuration task table below).

Output for the SNMP trap fields, which are displayed on the management station, are as follows:

- Server IP Address Type (IPv4 or IPv6)
- Server IP Address Type Length. (4 for IPv4 and 16 for IPv6)
- Server IP Address
- Server Port



Note

Only IPv4 is currently supported.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **snmp-server community** *string*
4. **snmp-server host** *hostname community-string*
5. **snmp-server enable traps firewall** [serverstatuschange]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	snmp-server community <i>string</i> Example: Router(config)# snmp-server community public	Sets up the community access string to permit access to the SNMP.
Step 4	snmp-server host <i>hostname community-string</i> Example: Router(config)# snmp-server host 192.168.1.1 version 2c public	Specifies the recipient of the firewall-related SNMP notifications.
Step 5	snmp-server enable traps firewall [serverstatuschange] Example: Router(config)# snmp-server enable traps firewall serverstatuschange	Enables firewall-related SNMP notifications.

What to Do Next

After the firewall and SNMP have been properly enabled, statistics will begin to accumulate after the traffic flow starts. To verify whether statistics are being collected and view MIB counters, you can perform at least one of the steps in the task “[Verifying Firewall Connection and URL Filtering Statistics](#).”

Verifying Firewall Connection and URL Filtering Statistics

Use this task to verify firewall connection and URL filtering statistics via command-line interface (CLI). (These statistics can also be collected via any SNMP-capable client.)



Note

Effective with Cisco IOS Release 12.4(20)T, the **debug ip inspect** command is replaced by the **debug policy-firewall** command. See the *Cisco IOS Debug Command Reference* for more information.

SUMMARY STEPS

1. **enable**
2. **show ip inspect mib connection-statistics** {global | l4-protocol {all | icmp | tcp | udp} | l7-protocol {all | other | telnet | ftp} | policy *policy-name* target *target name* {l4-protocol {all | icmp | tcp | udp} | l7-protocol {all | other | telnet | ftp}}}
3. **show ip urlfilter** [mib] statistics {global | server {ip-address [port] | all}}
4. **debug ip inspect mib** {object-creation | object-deletion | events | retrieval | update}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show ip inspect mib connection-statistics {global l4-protocol {all icmp tcp udp} l7-protocol {all other telnet ftp} policy <i>policy-name</i> target <i>target name</i> {l4-protocol {all icmp tcp udp} l7-protocol {all other telnet ftp}}} Example: Router# show ip inspect mib connection-statistics global	Displays firewall performance summary statistics that are monitored via SNMP. <ul style="list-style-type: none"> • global—Provides global connection statistics. • l4-protocol—Provides Layer 4 statistics for a specified protocol. • l7-protocol—Provides Layer 7 statistics for a specified protocol. • policy <i>policy-name</i> target <i>target-name</i>—Provides statistics on a per-policy target basis. For example, per firewall policy name and the interface on which the firewall is configured.
Step 3	show ip urlfilter [mib] statistics [{global server {ip-address [port] all}}] Example: Router# show ip urlfilter mib statistics global	Displays URL filtering statistics for firewall-related MIB events.
Step 4	debug ip inspect mib {object-creation object-deletion events retrieval update} Example: Router# debug ip inspect mib events	Displays messages about firewall MIB events.

Troubleshooting Tips

All statistics are accumulated since the last reboot of the firewall system. Thus, you must reboot the system to clear MIB connection statistics from your system.

Configuration Examples for Cisco IOS Firewall MIB Monitoring

This section contains the following examples:

- [Sample Cisco IOS Firewall Configuration: Example, page 10](#)
- [Sample URL Filtering Configuration: Example, page 12](#)
- [show ip inspect mib Output: Examples, page 14](#)
- [show ip urlfilter mib statistics command output: Examples, page 15](#)

Sample Cisco IOS Firewall Configuration: Example

The following output from the show running-config command shows how to configure a Cisco IOS Firewall:

```
Router# show running-config

Building configuration...

Current configuration : 2205 bytes
!
version 12.4
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no logging console
!
no aaa new-model
!
resource policy
!
clock timezone MST -8
clock summer-time MDT recurring
no ip cef
!
!
!
!
ip inspect name test tcp
ip inspect name test udp
ip inspect name test icmp timeout 30
ip inspect name test ftp
ip inspect name test http
!
!
!
!
!
!
!
!
!
```

```
!  
!  
!  
!  
policy-map ratelimit  
class class-default  
police cir 10000000  
conform-action transmit  
exceed-action drop  
!  
!  
!  
!  
!  
!  
!  
interface FastEthernet0/0  
ip address 192.168.27.2 255.255.255.0  
ip access-group 101 out  
ip inspect test in  
duplex full  
service-policy input ratelimit  
!  
interface FastEthernet1/0  
no ip address  
no ip route-cache  
shutdown  
duplex half  
!  
interface FastEthernet4/0  
ip address 192.168.127.2 255.255.255.0  
ip access-group 102 in  
duplex full  
service-policy input ratelimit  
!  
router eigrp 100  
network 192.168.27.0  
network 192.168.127.0  
no auto-summary  
no eigrp log-neighbor-changes  
no eigrp log-neighbor-warnings  
!  
ip default-gateway 192.168.27.116  
ip route 192.168.100.0 255.255.255.0 192.168.27.1  
ip route 192.168.200.0 255.255.255.0 192.168.127.1  
no ip http server  
no ip http secure-server  
!  
!  
!  
logging alarm informational  
access-list 101 permit tcp any any fragments  
access-list 101 permit udp any any fragments  
access-list 101 deny tcp any any  
access-list 101 deny udp any any  
access-list 101 permit ip any any  
access-list 102 permit tcp any any fragments  
access-list 102 permit udp any any fragments  
access-list 102 permit udp any gt 1024 any eq snmp  
access-list 102 deny tcp any any  
access-list 102 deny udp any any  
access-list 102 permit ip any any  
snmp-server community public RO  
snmp-server location FW Testbed UUT
```

```

snmp-server contact STG/IOS FW Devtest
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
!
exception core-file sisu-devtest/coredump/Router.core
exception dump 192.168.27.116
!
end

```

Sample URL Filtering Configuration: Example

The following sample output from the show running-config command shows how to configure a Websense server for URL filtering:

```

Router# show running-config
Building configuration...

Current configuration : 2043 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no logging console
!
no aaa new-model
!
resource policy
!
clock timezone MST -8
clock summer-time MDT recurring
no ip cef
!

```

```
!  
ip inspect name test tcp  
ip inspect name test udp  
ip inspect name test http urlfilter  
!  
!  
ip urlfilter allow-mode on  
ip urlfilter exclusive-domain deny www.cnn.com  
ip urlfilter exclusive-domain permit www.cpp.com  
ip urlfilter server vendor websense 192.168.29.116  
!  
!  
!  
!  
!  
!  
!  
!  
!  
interface FastEthernet0/0  
ip address 192.168.29.2 255.255.255.0  
ip access-group 101 out  
ip inspect test in  
speed auto  
full-duplex  
!  
interface FastEthernet0/1  
ip address 192.168.129.2 255.255.255.0  
ip access-group 102 in  
duplex auto  
speed auto  
!  
router eigrp 100  
network 192.168.29.0  
network 192.168.129.0  
no auto-summary  
no eigrp log-neighbor-changes  
no eigrp log-neighbor-warnings  
!  
ip default-gateway 192.168.28.116  
ip route 192.168.100.0 255.255.255.0 192.168.29.1  
ip route 192.168.200.0 255.255.255.0 192.168.129.1  
!  
!  
ip http server  
no ip http secure-server  
!  
access-list 101 permit tcp any any fragments  
access-list 101 permit udp any any fragments  
access-list 101 deny tcp any any  
access-list 101 deny udp any any  
access-list 101 permit ip any any  
access-list 102 permit tcp any any fragments  
access-list 102 permit udp any any fragments  
access-list 102 permit udp any gt 1024 any eq snmp  
access-list 102 deny tcp any any  
access-list 102 deny udp any any  
access-list 102 permit ip any any  
snmp-server community public RO  
snmp-server location FW Testbed UUT  
snmp-server contact STG/IOS FW Devtest  
!  
!  
!
```

```

!
control-plane
!
!
!
line con 0
exec-timeout 0 0
transport output all
line aux 0
transport output all
line vty 0 4
login
!
exception core-file sisu-devtest/coredump/Router.core
exception dump 192.168.28.116
!
webvpn context Default_context
ssl authenticate verify all
!
no inservice
!
!
end

```

show ip inspect mib Output: Examples

The following examples are sample outputs from the **show ip inspect mib** command with global or protocol-specific keywords:

- [Global MIB Statistics, page 14](#)
- [Protocol-Based MIB Statistics, page 14](#)
- [Policy-Target-Based MIB Statistics, page 15](#)

Global MIB Statistics

```

Router# show ip inspect mib connection-statistics global
-----
Connections Attempted 7
Connections Setup Aborted 0
Connections Policy Declined 0
Connections Resource Declined 0
Connections Half Open 2 Connections Active 3
Connections Expired 2
Connections Aborted 0
Connections Embryonic 0
Connections 1-min Setup Rate 5
Connections 5-min Setup Rate 7

```

Protocol-Based MIB Statistics

```

Router# show ip inspect mib connection-statistics 14-protocol tcp
-----
Protocol tcp
Connections Attempted 3
Connections Setup Aborted 0
Connections Policy Declined 0
Connections Resource Declined 0
Connections Half Open 1

```



```

Connections Active 2
Connections Aborted 0
Connections 1-min Setup Rate 3
Connections 5-min Setup Rate 3

```

```

Router# show ip inspect mib connection-statistics 17-protocol http
-----
Protocol http
Connections Attempted 3
Connections Setup Aborted 0
Connections Policy Declined 2
Connections Resource Declined 0
Connections Half Open 0
Connections Active 1
Connections Aborted 0
Connections 1-min Setup Rate 1
Connections 5-min Setup Rate 2

```

Policy-Target-Based MIB Statistics

```

Router# show ip inspect mib connection-statistics policy ftp interface GigabitEthernet0/0
14-protocol tcp
! Policy Target Protocol Based Connection Summary Stats
-----
Policy ftp-inspection
Target GigabitEthernet0/0
Protocol tcp
Connections Attempted 3
Connections Setup Aborted 0
Connections Policy Declined 0
Connections Resource Declined 0
Connections Half Open 1
Connections Active 2
Connections Aborted 0

Router# show ip inspect mib connection-statistics policy ftp interface GigabitEthernet0/0
17-protocol ftp
! Policy Target Protocol Based Connection Summary Stats
-----
Policy ftp-inspection
Target GigabitEthernet0/0
Protocol ftp
Connections Attempted 3
Connections Setup Aborted 0
Connections Policy Declined 0
Connections Resource Declined 0
Connections Half Open 1
Connections Active 2
Connections Aborted 0

```

show ip urlfilter mib statistics command output: Examples

The following example is sample output when MIBs are enabled to track URL filtering statistics across the entire device (global):

```

Router# show ip urlfilter mib statistics global
URL Filtering Group Summary Statistics
-----
URL Filtering Enabled

```

```

Requests Processed 260
Requests Processed 1-minute Rate 240
Requests Processed 5-minute Rate 215
Requests Allowed 230
Requests Denied 30
Requests Denied 1-minute Rate 15
Requests Denied 5-minute Rate 0
Requests Cache Allowed 5
Requests Cache Denied 5
Allow Mode Requests Allowed 15
Allow Mode Requests Denied 15
Requests Resource Dropped 0
Requests Resource Dropped 1-minute Rate 0
Requests Resource Dropped 5-minute Rate 0
Server Timeouts 0
Server Retries 0
Late Server Responses 0
Access Responses Resource Dropped 0

```

The following example is sample output when MIBs are enabled to track URL filtering statistics across the server with IP address 192.168.27.116:

```

Router# show ip urlfilter mib statistics server address 192.168.27.116
URL Filtering Server Statistics
-----
URL Server Host Name 192.168.27.116
Server Address 192.168.27.116
Server Port 15868
Server Vendor Websense
Server Status Online
Requests Processed 4
Requests Allowed 1
Requests Denied 3
Server Timeouts 0
Server Retries 9
Responses Received 1
Late Server Responses 12
1 Minute Average Response Time 0
5 Minute Average Response Time 0

```

Additional References

The following sections provide references related to Cisco IOS Firewall MIB.

Related Documents

Related Topic	Document Title
Description of SNMP, SNMP MIBs, and how to configure SNMP on Cisco devices	“Configuring SNMP Support” in the <i>Cisco IOS Network Management Configuration Guide</i> , Release 12.4
Description of Cisco IOS firewalls and functions such as how to configure a firewall and URL filtering	“Configuring Context-based Access Control” in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
<ul style="list-style-type: none">CISCO-UNIFIED-FIREWALL-MIB.myCISCO-FIREWALL-TC.my	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information

about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug ip inspect**
- **show ip inspect**
- **show ip urlfilter statistics**
- **snmp-server enable traps firewall**

Feature Information for Cisco IOS Firewall MIB

Table 4 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

**Note**

Table 4 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 4 Feature Information for Cisco IOS Firewall MIB

Feature Name	Releases	Feature Information
Cisco IOS Firewall MIB	12.4(6)T	Introduces support for the Cisco Unified Firewall MIB, which helps to manage and monitor firewall performance via SNMP. Statistics can be collected and monitored via standards-based SNMP techniques for firewall features such as stateful packet inspection and URL filtering.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Cisco IOS Firewall Performance Improvements

Feature History

Release	Modification
12.2(8)T	This feature was introduced.

This document describes the Cisco IOS Firewall Performance Improvements feature in Cisco IOS Release 12.2(8)T. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 3](#)
- [Supported Standards, MIBs, and RFCs, page 4](#)
- [Configuration Tasks, page 5](#)
- [Configuration Examples, page 5](#)
- [Command Reference, page 6](#)

Feature Overview

The Cisco IOS Firewall Performance Improvements feature introduces three performance metrics for Context-Based Access Control (CBAC)—[Throughput Improvement](#), [Connections Per Second Improvement](#), and [CPU Utilization Improvement](#).

CBAC is a context-based firewall that performs the following:

- Inspects traffic in one direction for network, transport, and application layer information
- Extracts relevant port information
- Dynamically creates access list entries for return traffic
- Closes ports at the end of a connection

CBAC also forces protocol conformance for some protocols, has a limited vulnerability signature detection mechanism, and extensive denial-of-service (DOS) prevention mechanisms. However, many of these features are CPU intensive, thereby, adversely affecting the performance of the router. The router is also affected during times of heavy traffic due to the processing of the base engine itself. With this feature, the performance of the router running CBAC is no longer subdued.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Throughput Improvement

Throughput is a metric defined by the number of packets transferred from the input interface to the output interface within 1 second by a router running CBAC. When the CBAC base engine inspects packets that belong to an existing session, it must find out which session the packet belongs to; thus, the base engine implements a hash table to search for the session of the packet.

Collisions in a hash table result in poor hash function distribution because many entries are hashed into the same bucket for certain patterns of addresses. Even if a hash function distribution evenly dispenses the input across all of the buckets, a small hashtable size will not scale well if there are a large number of sessions. As the number of sessions increase, the collisions increase, which increases the length of the linked lists, thereby, deteriorating the throughput performance.

The Cisco IOS Firewall Performance Improvements feature allows users to dynamically change the size of the session hash table without reloading the router by using the **ip inspect hashtable** command. By increasing the size of the hash table, the number of sessions per hash bucket can be reduced, which improves the throughput performance of the base engine.

Connections Per Second Improvement

Connections per second is a metric defined by the number of short-lived connections that can be created and deleted within 1 second by a router running CBAC. (These connections apply only to TCP connections because UDP is a connectionless protocol.)

Initially, CBAC had several restrictions that limited the connections per second metric. While a packet was being processed for connection setup and connection teardown of TCP connections, the base engine (which allocates and de-allocates memory while processing packets) would “bump up” several packets to the process switching path. Bumping up these packets drastically slowed down their processing. Also, the base engine had to process each packet again when it was bumped up into the process switching path, which also contributed to the degrading performance.

The Cisco IOS Firewall Performance Improvements feature prevents these restrictions by allowing only the first packet of any connection to be bumped up to the process switching path while the remaining packets are processed by the base engine in the fast path. Thus, the base engine is no longer slowed down by bumping up several packets or by processing packets twice.

**Note**

In this document, a connection is defined as creating a session, sending a data packet, and immediately deleting a session.

CPU Utilization Improvement

The CPU utilization of the router running CBAC can be measured while a specific throughput or connections per second metric is maintained. This improvement is used in conjunction with the throughput and connections per second metrics.

Benefits

Layer 4 Processing Performance Improvement

This enhancement improves the connections per second metric and the CPU utilization. The code path for connection initiation and teardown was rewritten, thereby, enabling quicker creation of the connections per second metric, which reduces CPU utilization per connection.

Hash Table Function Performance Improvement

With this enhancement, the hash function has been rewritten to ensure better distribution. This newly improved feature allows users to dynamically configure the size of the session hash table from 1K to 8K. When a packet belonging to an existing session comes into the router, a hash table is used to map the packet to an existing firewall session. As the number of sessions increases, the number of sessions hashing into the same bucket increases if the size of the hash table is fixed. By allowing the user to change the size of the hash table when the number of concurrent sessions increases or to reduce the search time for the session, the throughput performance of the base engine is greatly improved.

Application Module Tuning Performance Improvement

This enhancement makes changes to application modules, ensuring that only the connection-initiating packet from all the packets belonging to the connection initiation and teardown is bumped up to the process switching path. Thus, the connections per second metric is significantly improved.

Restrictions

To benefit from the performance enhancements, your router must be running CBAC.

Related Documents

- “Traffic Filtering and Firewalls” part in the *Cisco IOS Security Configuration Guide*, Release 12.2
- “Traffic Filtering and Firewalls” part in the *Cisco IOS Security Command Reference*, Release 12.2

Supported Platforms

- Cisco 800 series
- Cisco 805
- Cisco 820
- Cisco 827
- Cisco 1400 series
- Cisco 1600 series
- Cisco 1700 series
- Cisco 2500 series
- Cisco 2600 series
- Cisco 3620
- Cisco 3640

- Cisco 3660
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7500 series
- Cisco Catalyst 6500 series MSFC software
- Cisco uBR7200 series
- Cisco uBR905
- Cisco uBR925

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

RFCs

None

Configuration Tasks

See the following sections for configuration tasks for the Cisco IOS Firewall Performance Improvements feature. Each task in the list is identified as either required or optional.

- [Changing the Size of the Hash Table](#) (required)
- [Verifying CBAC Configurations](#) (optional)

Changing the Size of the Hash Table

You can increase the hash table to improve packet distribution. To change the size of the session hash table, use the following command in global configuration mode:

Command	Purpose
Router# ip inspect hashtable <i>number</i>	<p>Changes the size of the hash table.</p> <p><i>number</i> specifies the size of the hash table in terms of buckets. Possible values for the hash table are 1024, 2048, 4096, and 8192; the default value is 1024.</p> <p>Note You should increase the hash table size when the total number of sessions running through the CBAC router is approximately twice the current hash size; decrease the hash table size when the total number of sessions is reduced to approximately half the current hash size. Essentially, try to maintain a 1:1 ratio between the number of sessions and the size of the hash table.</p>

Verifying CBAC Configurations

To verify all CBAC configurations and all existing sessions that are currently being tracked and inspected by CBAC, use the **show ip inspect all** command in EXEC mode.

Configuration Examples

This section provides the following configuration example:

- [Changing the Size of the Hash Table Example](#)

Changing the Size of the Hash Table Example

The following example shows how to change the size of the hash table to 2048 buckets:

```
ip inspect hashtable 2048
```

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **ip inspect hashtable**

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Cisco IOS Firewall—SIP Enhancements: ALG and AIC

First Published: April 14, 2008

Last Updated: July 11, 2008

Enhanced Session Initiation Protocol (SIP) inspection in the Cisco IOS firewall provides basic SIP inspect functionality (SIP packet inspection and pinholes opening) as well as protocol conformance and application security. These enhancements give the user a more control than in previous releases on what policies and security checks to apply to SIP traffic and the capability to filter out unwanted messages or users.

The development of additional SIP functionality in Cisco IOS provides increased support for Cisco Call Manager (CCM), Cisco Call Manager Express (CCME), and Cisco IP-IP Gateway based voice/video systems. Application Layer Gateway (ALG), and Application Inspection and Control (AIC) SIP enhancements also support RFC 3261 and its extensions.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Cisco IOS Firewall—SIP Enhancements: ALG and AIC” section on page 21](#).

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Cisco IOS Firewall—SIP Enhancements: ALG and AIC, page 2](#)
- [Restrictions for Cisco IOS Firewall—SIP Enhancements: ALG and AIC, page 2](#)
- [Information About Cisco IOS Firewall—SIP Enhancements: ALG and AIC, page 3](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008 Cisco Systems, Inc. All rights reserved.

- [How to Configure Cisco IOS Firewall—SIP Enhancements: ALG and AIC, page 4](#)
- [Configuration Examples for Cisco IOS Firewall—SIP Enhancements: ALG and AIC, page 18](#)
- [Additional References, page 19](#)
- [Command Reference, page 20](#)
- [Feature Information for Cisco IOS Firewall—SIP Enhancements: ALG and AIC, page 21](#)

Prerequisites for Cisco IOS Firewall—SIP Enhancements: ALG and AIC

The following prerequisites apply to the configuration of Cisco IOS Firewall—SIP Enhancements: ALG and AIC.

Hardware Requirements

- A platform, which can be any of the following:
 - Cisco 861, Cisco 881, or Cisco 881G routers
 - Cisco 1700 routers
 - Cisco 1800 routers
 - Cisco 2600 routers
 - Cisco 2800 routers
 - Cisco 3700 routers
 - Cisco 3800 routers
 - Cisco 7200 routers
 - Cisco 7300 routers

Software Requirements

- Cisco IOS Release 12.4(15)XZ or a later release.

Restrictions for Cisco IOS Firewall—SIP Enhancements: ALG and AIC

DNS Name Resolution

Although SIP methods can have Domain Name System (DNS) names instead of raw IP addresses, this feature currently does not support DNS names.

Earlier Releases of Cisco IOS

Some Cisco IOS releases earlier than Release 12.4(15)XZ may accept the configuration commands for SIP that are shown in this document; however, those earlier versions will not function properly.

Information About Cisco IOS Firewall—SIP Enhancements: ALG and AIC

To configure the Cisco IOS Firewall—SIP Enhancements: ALG and AIC feature, you must understand the following concepts:

- [Firewall and SIP Overviews, page 3](#)
- [Firewall for SIP Functionality Description, page 3](#)
- [SIP Inspection, page 4](#)

Firewall and SIP Overviews

Cisco IOS Firewall

The Cisco IOS firewall extends the concept of static access control lists (ACLs) by introducing dynamic ACL entries that open on the basis of the necessary application ports on a specific application and close these ports at the end of the application session. The Cisco IOS firewall achieves this functionality by inspecting the application data, checking for conformance of the application protocol, extracting the relevant port information to create the dynamic ACL entries, and closing these ports at the end of the session. The Cisco IOS firewall is designed to easily allow a new application inspection whenever support is needed.

Session Initiation Protocol

SIP is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions could include Internet telephone calls, multimedia distribution, and multimedia conferences. SIP is based on an HTTP-like request/response transaction model. Each transaction consists of a request that invokes a particular method or function on the server and at least one response.

SIP invitations used to create sessions carry session descriptions that allow participants to agree on a set of compatible media types. SIP makes use of elements called proxy servers to help route requests to the user's current location, authenticate and authorize users for services, implement provider call-routing policies, and provide features to users. SIP also provides a registration function that allows users to upload their current locations for use by proxy servers. SIP runs on top of several different transport protocols.

Firewall for SIP Functionality Description

The firewall for SIP support feature allows SIP signaling requests to traverse directly between gateways or through a series of proxies to the destination gateway or phone. After the initial request, if the Record-Route header field is not used, subsequent requests can traverse directly to the destination gateway address as specified in the Contact header field. Thus, the Cisco IOS firewall is aware of all surrounding proxies and gateways and allows the following functionality:

- SIP signaling responses can travel the same path as SIP signaling requests.
- Subsequent signaling requests can travel directly to the endpoint (destination gateway).
- Media endpoints can exchange data between each other.

SIP UDP and TCP Support

RFC 3261 is the current RFC for SIP, which replaces RFC 2543. This feature supports the SIP User Datagram Protocol (UDP) and the TCP format for signaling.

SIP Inspection

This section describes the deployment scenarios supported by the Cisco IOS Firewall—SIP, ALG, and AIC Enhancements feature.

Cisco IOS Firewall Between SIP Phones and CCM

The Cisco IOS firewall is located between CCM or CCME and SIP phones. SIP phones are registered to CCM or CCME through the firewall, and any SIP calls from or to the SIP phones pass through the firewall.

Cisco IOS Firewall Between SIP Gateways

The Cisco IOS firewall is located between two SIP gateways, which can be CCM, CCME, or a SIP proxy. Phones are registered with SIP gateways directly. The firewall sees the SIP session or traffic only when there is a SIP call between phones registered to different SIP gateways. In some scenarios an IP-IP gateway can also be configured on the same device as the firewall. With this scenario all the calls between the SIP gateways are terminated in the IP-IP gateway.

Cisco IOS Firewall with Local CCME and Remote CCME/CCCM

The Cisco IOS firewall is located between two SIP gateways, which can be CCM, CCME, or a SIP proxy. One of the gateways is configured on the same device as the firewall. All the phones registered to this gateway are locally inspected by the firewall. The firewall also inspects SIP sessions between the two gateways when there is a SIP call between them. With this scenario the firewall locally inspects SIP phones on one side and SIP gateways on the other side.

Cisco IOS Firewall with Local CCME

The Cisco IOS firewall and CCME is configured on the same device. All the phones registered to the CCME are locally inspected by the firewall. Any SIP call between any of the phones registered will also be inspected by the Cisco IOS firewall.

How to Configure Cisco IOS Firewall—SIP Enhancements: ALG and AIC

Perform the following tasks to configure Cisco IOS Firewall—SIP Enhancements: ALG and AIC:

- [Configuring a Policy to Allow RFC 3261 Methods, page 5](#)
- [Configuring a Policy to Block Messages, page 7](#)
- [Configuring a 403 Response Alarm, page 9](#)
- [Limiting Application Messages, page 11](#)
- [Limiting Application Messages for a Particular Proxy, page 13](#)

Configuring a Policy to Allow RFC 3261 Methods

To configure a policy to allow basic RFC 3261 methods and block extension methods, perform the steps in this section.



Note

The Cisco IOS Firewall—SIP Enhancements: ALG and AIC feature provides essential support for the new SIP methods such as UPDATE and PRACK, as CCM 5.x and CCME 4.x also use these methods.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type inspect** *protocol-name* **match-any** *class-map-name*
4. **match request method** *method-name*
5. **exit**
6. **class-map type inspect** *protocol-name* **match-any** *class-map-name*
7. **match request method** *method-name*
8. **exit**
9. **policy-map type inspect** *protocol-name* *policy-map-name*
10. **class type inspect** *protocol-name* *class-map-name*
11. **allow**
12. **exit**
13. **class type inspect** *protocol-name* *class-map-name*
14. **reset**
15. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	class-map type inspect <i>protocol-name</i> match-any <i>class-map-name</i> Example: Router(config)# class-map type inspect sip match-any sip_class1	Creates an inspect type class map and enters class-map configuration mode.

	Command or Action	Purpose
Step 4	match request method <i>method-name</i> Example: Router(config-cmap)# match request method invite	Matches RFC 3261 methods. Methods include the following: <ul style="list-style-type: none"> ack, bye, cancel, info, invite, message, notify, options, prack, refer, register, subscribe, update.
Step 5	exit Example: Router(config-cmap)# exit	Exits class-map configuration mode.
Step 6	class-map type inspect <i>protocol-name</i> match-any <i>class-map-name</i> Example: Router(config)# class-map type inspect sip match-any sip_class2	Creates an inspect type class map and enters class-map configuration mode.
Step 7	match request method <i>method-name</i> Example: Router(config-cmap)# match request method message	Matches RFC 3261 methods, which include the following: <ul style="list-style-type: none"> ack, bye, cancel, info, invite, message, notify, options, prack, refer, register, subscribe, update.
Step 8	exit Example: Router(config-cmap)# exit	Exits class-map configuration mode.
Step 9	policy-map type inspect <i>protocol-name</i> <i>policy-map-name</i> Example: Router(config)# policy-map type inspect sip sip_policy	Creates an inspect type policy map and enters policy-map configuration mode.
Step 10	class type inspect <i>protocol-name</i> <i>class-map-name</i> Example: Router(config-pmap)# class type inspect sip sip_class1	Specifies the class on which the action is performed and enters policy-map-class configuration mode.
Step 11	allow Example: Router(config-pmap-c)# allow	Allows SIP inspection.
Step 12	exit Example: Router(config-pmap-c)# exit	Exits policy-map-class configuration mode.

	Command or Action	Purpose
Step 13	class type inspect <i>protocol-name class-map-name</i> Example: Router(config-pmap)# class type inspect sip sip_class2	Specifies the class on which the action is performed and enters policy-map-class configuration mode.
Step 14	reset Example: Router(config-pmap-c)# reset	Resets the class map.
Step 15	exit Example: Router(config-pmap-c)# exit	Exits policy-map-class configuration mode.

Configuring a Policy to Block Messages

To configure a policy to block SIP messages coming from a particular proxy device, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type regex** *parameter-map-name*
4. **pattern** *url-pattern*
5. **exit**
6. **class-map type inspect** *protocol-name class-map-name*
7. **match request header** *field* **regex** *regex-parameter-map*
8. **exit**
9. **policy-map type inspect** *protocol-name policy-map-name*
10. **class type inspect** *protocol-name class-map-name*
11. **reset**
12. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	parameter-map type regex <i>parameter-map-name</i> Example: Router(config)# parameter-map type regex unsecure_proxy	Configures a parameter-map type to match a specific traffic pattern and enters profile configuration mode.
Step 4	pattern url-pattern Example: Router(config-profile)# pattern "compromised.server.com"	Matches a call based on the SIP uniform resource identifier (URI).
Step 5	exit Example: Router(config-profile)# exit	Exits profile configuration mode.
Step 6	class-map type inspect <i>protocol-name</i> <i>class-map-name</i> Example: Router(config)# class-map type inspect sip sip_class	Creates an inspect type class map and enters class-map configuration mode.
Step 7	match request header <i>field</i> regex <i>regex-param-map</i> Example: Router(config-cmap)# match request header Via regex unsecure_proxy	Configures a class-map type to match a specific request header pattern.
Step 8	exit Example: Router(config-cmap)# exit	Exits class-map configuration mode.
Step 9	policy-map type inspect <i>protocol-name</i> <i>policy-map-name</i> Example: Router(config)# policy-map type inspect sip sip_policy	Creates an inspect type policy map and enters policy-map configuration mode.

	Command or Action	Purpose
Step 10	class type inspect <i>protocol-name class-map-name</i> Example: Router(config-pmap)# class type inspect sip sip_class	Specifies the class on which the action is performed and enters policy-map-class configuration mode.
Step 11	reset Example: Router(config-pmap-c)# reset	Resets the class map.
Step 12	exit Example: Router(config-pmap-c)# exit	Exits policy-map-class configuration mode.

Configuring a 403 Response Alarm

To configure a policy to generate an alarm whenever a 403 response is returned, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type regex** *parameter-map-name*
4. **pattern** *url-pattern*
5. **exit**
6. **class-map type inspect** *protocol-name class-map-name*
7. **match response status regex** *regex-parameter-map*
8. **exit**
9. **policy-map type inspect** *protocol-name policy-map-name*
10. **class type inspect** *protocol-name class-map-name*
11. **log**
12. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	parameter-map type regex <i>parameter-map-name</i> Example: Router(config)# parameter-map type regex allowed_im_users	Configures a parameter-map type to match a specific traffic pattern and enters profile configuration mode.
Step 4	pattern <i>url-pattern</i> Example: Router(config-profile)# pattern "+403"	Matches a call based on the SIP URI.
Step 5	exit Example: Router(config-profile)# exit	Exits profile configuration mode.
Step 6	class-map type inspect <i>protocol-name</i> <i>class-map-name</i> Example: Router(config)# class-map type inspect sip sip_class	Creates an inspect type class map and enters class-map configuration mode.
Step 7	match response status regex <i>regex-parameter-map</i> Example: Router(config-cmap)# match response status regex allowed_im_users	Configures a class-map type to match a specific response pattern.
Step 8	exit Example: Router(config-cmap)# exit	Exits class-map configuration mode.
Step 9	policy-map type inspect <i>protocol-name</i> <i>policy-map-name</i> Example: Router(config)# policy-map type inspect sip sip_policy	Creates an inspect type policy map and enters policy-map configuration mode.

	Command or Action	Purpose
Step 10	class type inspect <i>protocol-name class-map-name</i> Example: Router(config-pmap)# class type inspect sip sip_class	Specifies the class on which the action is performed and enters policy-map-class configuration mode.
Step 11	log Example: Router(config-pmap-c) # log	Generates a log of messages.
Step 12	exit Example: Router(config)# exit	Exits policy-map-class configuration mode.

Limiting Application Messages

To configure a policy to rate-limit INVITE messages, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type inspect** *protocol-name match-any class-map-name*
4. **match request method** *method-name*
5. **exit**
6. **policy-map type inspect** *protocol-name policy-map-name*
7. **class type inspect** *protocol-name class-map-name*
8. **rate-limit** *limit-number*
9. **exit**
10. **class-map type inspect** *protocol-name match-any class-map-name*
11. **match protocol** *protocol-name*
12. **exit**
13. **policy-map type inspect** *protocol-name policy-map-name*
14. **class type inspect** *protocol-name class-map-name*
15. **inspect**
16. **service-policy** *policy-map-name*
17. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	class-map type inspect protocol-name match-any class-map-name Example: Router(config)# class-map type inspect sip match-any class_2	Creates an inspect type class map and enters class-map configuration mode.
Step 4	match request method method-name Example: Router(config-cmap)# match request method invite	Matches RFC 3261 methods. Methods include the following: <ul style="list-style-type: none"> ack, bye, cancel, info, invite, message, notify, options, prack, refer, register, subscribe, update.
Step 5	exit Example: Router(config-cmap)# exit	Exits class-map configuration mode.
Step 6	policy-map type inspect protocol-name policy-map-name Example: Router(config)# policy-map type inspect sip policy_2	Creates an inspect type policy map and enters policy-map configuration mode.
Step 7	class type inspect protocol-name class-map-name Example: Router(config-pmap)# class type inspect sip class_2	Specifies the class on which the action is performed and enters policy-map-class configuration mode.
Step 8	rate-limit limit-number Example: Router(config-pmap-c)# rate-limit 16	Limits the number of SIP messages that strike the Cisco IOS firewall every second.
Step 9	exit Example: Router(config-pmap-c)# exit	Exits policy-map-class configuration mode.

	Command or Action	Purpose
Step 10	class-map type inspect <i>protocol-name</i> match-any <i>class-map-name</i> Example: Router(config)# class-map type inspect sip match-any class_1	Creates an inspect type class map and enters class-map configuration mode.
Step 11	match protocol <i>protocol-name</i> Example: Router(config-cmap)# match protocol sip	Configures the match criterion for a class map on the basis of the specified protocol.
Step 12	exit Example: Router(config-cmap)# exit	Exits class-map configuration mode.
Step 13	policy-map type inspect <i>protocol-name</i> <i>policy-map-name</i> Example: Router(config)# policy-map type inspect sip policy_1	Creates an inspect type policy map and enters policy-map configuration mode.
Step 14	class type inspect <i>protocol-name</i> <i>class-map-name</i> Example: Router(config-pmap)# class type inspect sip class_1	Specifies the class on which the action is performed and enters policy-map-class configuration mode.
Step 15	inspect Example: Router(config-pmap-c)# inspect	Enables stateful packet inspection.
Step 16	service-policy <i>policy-map-name</i> Example: Router(config-pmap-c)# service-policy policy_2	Attaches the policy map to the service policy for the interface or virtual circuit.
Step 17	exit Example: Router(config-pmap-c)# exit	Exits policy-map-class configuration mode.

Limiting Application Messages for a Particular Proxy

To configure a policy to rate-limit INVITE messages coming for a particular proxy, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type regex** *parameter-map-name*
4. **pattern** *url-pattern*
5. **exit**
6. **class-map type inspect** *protocol-name* **match-any** *class-map-name*
7. **match request method** *method-name*
8. **match request header field regex** *regex-parameter-map*
9. **exit**
10. **policy-map type inspect** *protocol-name* *policy-map-name*
11. **class type inspect** *protocol-name* *class-map-name*
12. **rate-limit** *limit-number*
13. **exit**
14. **class-map type inspect** *protocol-name* **match-any** *class-map-name*
15. **match protocol** *protocol-name*
16. **exit**
17. **policy-map type inspect** *protocol-name* *policy-map-name*
18. **class type inspect** *protocol-name* *class-map-name*
19. **inspect**
20. **service-policy** *policy-map-name*
21. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example: Router> enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	
Step 3	parameter-map type regex <i>parameter-map-name</i>	Configures a parameter-map type to match a specific traffic pattern and enters profile configuration mode.
	Example: Router(config)# parameter-map type regex rate_limited_proxy	

	Command or Action	Purpose
Step 4	pattern <i>url-pattern</i> Example: Router(config-profile)# pattern "compromised.server.com"	Matches a call based on the SIP URI.
Step 5	exit Example: Router(config-cmap)# exit	Exits profile configuration mode.
Step 6	class-map type inspect <i>protocol-name</i> match-any <i>class-map-name</i> Example: Router(config)# class-map type inspect sip match-all class_2	Creates an inspect type class map and enters class-map configuration mode.
Step 7	match request method <i>method-name</i> Example: Router(config-cmap)# match request method invite	Matches RFC 3261 methods. Methods include the following: <ul style="list-style-type: none"> ack, bye, cancel, info, invite, message, notify, options, prack, refer, register, subscribe, update.
Step 8	match request header <i>field</i> regex <i>regex-param-map</i> Example: Router(config-cmap)# match request header Via regex rate_limited_proxy	Configures a class-map type to match a specific request header pattern.
Step 9	exit Example: Router(config-cmap)# exit	Exits class-map configuration mode.
Step 10	policy-map type inspect <i>protocol-name</i> <i>policy-map-name</i> Example: Router(config)# policy-map type inspect sip policy_2	Creates an inspect type policy map and enters policy-map configuration mode.
Step 11	class type inspect <i>protocol-name</i> <i>class-map-name</i> Example: Router(config-pmap)# class type inspect sip class_2	Specifies the class on which the action is performed and enters policy-map-class configuration mode.
Step 12	rate-limit <i>limit-number</i> Example: Router(config-pmap-c)# rate-limit 16	Limits the number of SIP messages that strike the Cisco IOS firewall every second.

	Command or Action	Purpose
Step 13	exit Example: Router(config-pmap-c)# exit	Exits policy-map-class configuration mode.
Step 14	class-map type inspect <i>protocol-name</i> match-any <i>class-map-name</i> Example: Router(config)# class-map type inspect sip match-any class_1	Creates an inspect type class map and enters class-map configuration mode.
Step 15	match protocol <i>protocol-name</i> Example: Router(config-cmap)# match protocol sip	Configures the match criterion for a class map on the basis of the specified protocol.
Step 16	exit Example: Router(config-cmap)# exit	Exits class-map configuration mode.
Step 17	policy-map type inspect <i>protocol-name</i> <i>policy-map-name</i> Example: Router(config)# policy-map type inspect sip policy_1	Creates an inspect type policy map and enters policy-map configuration mode.
Step 18	class type inspect <i>protocol-name</i> <i>class-map-name</i> Example: Router(config-pmap)# class type inspect sip class_1	Specifies the class on which the action is performed and enters policy-map-class configuration mode.
Step 19	inspect Example: Router(config-pmap-c)# inspect	Enables stateful packet inspection.
Step 20	service-policy <i>policy-map-name</i> Example: Router(config-pmap-c)# service-policy policy_2	Attaches the policy map to the service policy for the interface or virtual circuit.
Step 21	exit Example: Router(config-pmap-c)# exit	Exits policy-map-class configuration mode.

Troubleshooting Tips

The following commands can be used to troubleshoot Cisco IOS Firewall—SIP Enhancements: ALG and AIC:

- **clear zone-pair**
- **debug cce**
- **debug ip inspect**
- **debug policy-map type inspect**
- **show policy-map type inspect zone-pair**
- **show zone-pair security**



Note

Effective with Cisco IOS Release 12.4(20)T, the **debug ip inspect** command is replaced by the **debug policy-firewall** command. See the *Cisco IOS Debug Command Reference* for more information.

Examples

show policy-map type inspect zone-pair

The following example shows sample output of the **show policy-map type inspect zone-pair** command when the **session** keyword is used.

```
Router# show policy-map type inspect zone-pair session
```

```
policy exists on zp zp_test_out_self
Zone-pair: zp_test_out_self
Service-policy inspect : test
Class-map: c_sip (match-any)
...
Number of Established Sessions = 2
Established Sessions
Session 6717A7A0 (192.168.105.118:62265)=>(192.168.105.2:5060) sip:udp SIS_OPEN
Created 00:10:27, Last heard 00:00:03
Bytes sent (initiator:responder) [35579:14964]
Session 67179EA0 (192.168.105.119:62266)=>(192.168.105.2:5060) sip:udp SIS_OPEN
Created 00:10:27, Last heard 00:03:17
Bytes sent (initiator:responder) [10689:4093]
Number of Pre-generated Sessions = 7
Pre-generated Sessions
Pre-gen session 6717A560 192.168.105.2[1024:65535]=>192.168.105.118[62265:62265]
sip:udp
Created never, Last heard never
Bytes sent (initiator:responder) [0:0]
Pre-gen session 67179C60 192.168.105.2[1024:65535]=>192.168.105.119[62266:62266]
sip:udp
Created never, Last heard never
Bytes sent (initiator:responder) [0:0]
Pre-gen session 67176F60 192.168.105.118[1024:65535]=>192.168.105.2[5060:5060]
sip:udp
Created never, Last heard never
Bytes sent (initiator:responder) [0:0]
Pre-gen session 67176AE0 192.168.105.118[1024:65535]=>192.168.105.2[18318:18318]
sip-RTP-data:udp
Created never, Last heard never
Bytes sent (initiator:responder) [0:0]
```

```

Pre-gen session 671768A0 192.168.105.2[1024:65535]=>192.168.105.118[62495:62495]
sip-RTP-data:udp
Created never, Last heard never
Bytes sent (initiator:responder) [0:0]
Pre-gen session 671783A0 192.168.105.118[1024:65535]=>192.168.105.2[18319:18319]
sip-RTCP-data:udp
Created never, Last heard never
Bytes sent (initiator:responder) [0:0]
Pre-gen session 67176420 192.168.105.2[1024:65535]=>192.168.105.118[62496:62496]
sip-RTCP-data:udp
Created never, Last heard never
Bytes sent (initiator:responder) [0:0]

```

show zone-pair security

The following example shows sample output of the **show zone-pair security** command.

```
Router# show zone-pair security
```

```

Zone-pair name zp_in_out
Source-Zone inside Destination-Zone outside
service-policy test
Zone-pair name zp_in_self
Source-Zone inside Destination-Zone self
service-policy test
Zone-pair name zp_self_out
Source-Zone self Destination-Zone outside
service-policy test

```

Configuration Examples for Cisco IOS Firewall—SIP Enhancements: ALG and AIC

This section contains the following example:

- [Firewall and SIP Configuration: Example, page 18](#)

Firewall and SIP Configuration: Example

The following example shows how to configure the Cisco IOS Firewall—SIP Enhancements: ALG and AIC feature when the Cisco IOS firewall is located between two SIP gateways (CCM or CCME), as described in the [Cisco IOS Firewall Between SIP Gateways, page 4](#). Some phones are registered to the CCME inside the firewall (inside zone). Other phones are registered to another CCME / CCM outside the firewall (outside zone). Cisco IOS firewall is configured for SIP inspection when there is no IP-IP gateway configured on the firewall device.

```

class-map type inspect sip match-any sip-aic-class
match request method invite
policy-map type inspect sip sip-aic-policy
class type inspect sip sip-aic-class
rate-limit 15
!
policy-map type inspect sip-policy
class type inspect sip-traffic-class
service-policy sip sip-aic-policy
!
class-map type inspect match-any sip-traffic-class
match protocol sip
!

```

```

policy-map type inspect sip-policy
class type inspect sip-traffic-class
inspect my-parameters
!
zone security inside
zone security outside
!
interface fastethernet 0
zone-member security inside
interface fastethernet 1
zone-member security outside
!
zone-pair security in-out source inside destination outside
service-policy type inspect sip-policy
!
zone-pair security in-self source inside destination self
service-policy type inspect sip-policy

```

Additional References

The following sections provide references related to the Cisco IOS Firewall—SIP Enhancements: ALG and AIC feature.

Related Documents

Related Topic	Document Title
Cisco IOS firewall information and configuration tasks	The chapter “Configuring Context-Based Access Control” in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4
Cisco IOS firewall commands	The chapter “Context-Based Access Control Commands” in the <i>Cisco IOS Security Command Reference</i> , Release 12.4
SIP information and configuration tasks	The chapter “Configuring Session Initiation Protocol for Voice over IP” in the <i>Cisco IOS Voice, Video, and Fax Configuration Guide</i> , Release 12.4
Additional SIP Information	Guide to Cisco Systems VoIP Infrastructure Solution for SIP
Access lists and the access-list command	The chapter “Configuring IPSec Network Security” in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4, and the <i>Cisco IOS Command Reference</i> , Release 12.4, respectively
Cisco IOS firewall support for SIP	The chapter “Configuring Cisco IOS Firewall” in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 3261	SIP: Session Initiation Protocol

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or a Cisco IOS master commands list.

- **class-map type inspect**
- **match protocol**
- **match protocol-violation**
- **match req-resp**
- **match request**
- **match response**
- **policy-map type inspect**
- **rate-limit (firewall)**

Feature Information for Cisco IOS Firewall—SIP Enhancements: ALG and AIC

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Cisco IOS Firewall—SIP Enhancements: ALG and AIC

Feature Name	Releases	Feature Information
Cisco IOS Firewall—SIP Enhancements: ALG and AIC	12.4(15)XZ 12.4(20)T	<p>This feature provides voice security enhancements within the Firewall feature set in Cisco IOS software for Release 12.4(15)XZ and later releases.</p> <p>In Release 12.4(15)XZ, this feature was introduced on the Cisco 861, Cisco 881, and Cisco 881G routers.</p> <p>In Release 12.4(20)T, this feature was implemented on the Cisco 1700, Cisco 1800, Cisco 2600, Cisco 2800, Cisco 3700, Cisco 3800, Cisco 7200, and Cisco 7300 routers.</p> <p>The following commands were introduced or modified: class-map type inspect, match protocol, match protocol-violation, match req-resp, match request, match response, policy-map type inspect, rate-limit (firewall).</p>

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and

coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.



E-mail Inspection Engine

The E-mail Inspection Engine feature allows the Cisco IOS Firewall to inspect Post Office Protocol 3 (POP3) and Internet Message Access Protocol (IMAP) e-mail, in addition to Simple Mail Transfer Protocol (SMTP) and Extended Simple Mail Transfer Protocol (ESMTP) e-mail which were previously supported.

The **secure-login** enhancement allows people to download external POP3 e-mail only if authentication methods are secure.

Feature History for E-mail Inspection Engine

Release	Modification
12.3(14)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for E-mail Inspection Engine, page 2](#)
- [Restrictions for E-mail Inspection Engine, page 2](#)
- [Information About E-mail Inspection Engine, page 2](#)
- [How to Configure E-mail Inspection Engine, page 4](#)
- [Configuration Examples for E-mail Inspection Engine, page 7](#)
- [Additional References, page 8](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Command Reference, page 10](#)
- [Glossary, page 11](#)

Prerequisites for E-mail Inspection Engine

- Configure CBAC.
- Enable SSL VPN tunnels.

Restrictions for E-mail Inspection Engine

None.

Information About E-mail Inspection Engine

To configure E-mail Inspection Engine, you need to understand the following concepts:

- [E-mail Inspection Engine Operation, page 2](#)
- [Inspection, page 3](#)
- [POP3, page 3](#)
- [IMAP Protocol, page 3](#)
- [Client Command Validation, page 4](#)
- [SMTP, page 4](#)
- [SSL, page 4](#)

E-mail Inspection Engine Operation

The client/server communication is validated from the time the TCP connection is initialized until the client is authenticated. The Cisco IOS Firewall uses a state router to track each stage of authentication. After the client is authenticated, the Cisco IOS Firewall allows all the client/server commands without further L7 inspection. TCP L4 inspection continues until the connection is closed. At the end of the e-mail session when the client host quits and before the TCP connection is closed, no further client/server interaction is allowed unless the client is reauthenticated.

During the authentication, any unrecognized command causes the Cisco IOS Firewall to drop the packet and close the connection.

If encryption is negotiated between the client and server control channel, no further validation occurs.

An e-mail client logging in from a nonsecure location may need to use encryption for authentication. For information about secure logins, see the description of the **secure-login** keyword of the **ip inspect name** command.

Inspection

Context Based Access Control (CBAC) inspects traffic that travels through the firewall to discover and manage state information for TCP and User Datagram Protocol (UDP) sessions. This state information is used to create temporary openings in the firewall's access lists to allow return traffic and additional data connections for permissible sessions.

Inspecting packets at the application layer and maintaining TCP and UDP session information provides CBAC with the ability to detect and prevent certain types of network attacks such as SYN-flooding. A SYN-flood attack occurs when a network attacker floods a server with a barrage of requests for connection and does not complete the connection. The resulting volume of half-open connections can overwhelm the server, causing it to deny service to valid requests. Network attacks that deny access to a network device are called denial-of-service (DoS) attacks.

POP3

The Post Office Protocol, Version 3 (POP3) is used to receive e-mail that is stored on a mail server. Unlike IMAP, POP only retrieves mail from a remote host.

POP3 works best when there is only one computer because it supports “offline” message access where messages are downloaded and then deleted from the mail server. This mode of access is not compatible with access from multiple computers because it tends to sprinkle messages across all the computers used for mail access.

With POP3-based e-mail clients, messages are downloaded to the user's local message store and can also be deleted from the mail server. Deletion is optional in most clients. When a new voice message arrives, the subscriber's only immediate notification is the activation of the MWI on the phone. New messages are displayed in the Inbox only after the client's local message store is updated with the Exchange message store. After the subscriber downloads new messages, the message state automatically changes from “new” to “read” on the server, even though the subscriber has not actually listened to the voice messages. MWIs on the subscriber's phone are extinguished, and the message state between the TUI and the subscriber's Inbox are not synchronized.

IMAP Protocol

The Internet Message Access Protocol (IMAP) is a method of accessing electronic mail or bulletin board messages that are kept on a mail server that may be shared. It permits a “client” e-mail program to access remote messages as though they were local. For example, e-mail stored on an IMAP server can be retrieved, sent, and managed from a desktop computer at home, from a workstation at the office, or from a laptop without transferring messages or files back and forth between the computers.

Only the message header and sender information are displayed in the Inbox until the user downloads the entire message, including attachments, from the server. When a new voice message arrives, the subscriber's only immediate notification is the activation of the Message Waiting Indication (MWI) on the phone. New messages are displayed in the Inbox only after the client's local message store is updated with the Exchange message store. When the subscriber listens to a new message by using the telephone user interface (TUI), the MWI is extinguished. In this case again, the message state is not updated in the Inbox until the client's message store is refreshed. However, if the subscriber uses an installed multimedia player to listen to the WaveForm Audio (WAV) attachment from the e-mail client's Inbox, message state changes are automatically synchronized with the TUI.

How message state changes are conveyed to the Cisco Unity subscriber, and how these changes are synchronized with the TUI, depend on whether the subscriber's e-mail client is configured to use POP3 or IMAP4 to access Exchange.

Client Command Validation

The Cisco IOS Firewall authenticates an e-mail client accessing an IMAP or POP3 server before allowing complete access into the server. The firewall searches the IMAP/POP3 TCP stream for valid protocol commands. If the client's commands are outside the protocol's definition, the Cisco IOS Firewall drops the packets and resets the connection.

Client command validation is typically needed in a DeMilitarized Zone (DMZ). Client access is allowed into the DMZ only if the e-mail server validates the user authentication. After the client is authenticated, the client becomes a trusted user and access is permitted.

SMTP

The Simple Mail Transfer Protocol (SMTP) is used to transfer e-mail between servers and clients on the Internet. E-mail clients and mail servers that use protocols other than Message Application Programming Interface (MAPI) can use the SMTP protocol to transfer a message from a client to the server, and then forward it to a message recipient's server. To retrieve, send, and manage these messages from the e-mail client use POP3 or IMAP4.

Cisco Unity uses SMTP to route voice messages via the Internet Voice Connector (IVC) gateway between other Exchange servers that are not connected by using a Site Message Connector. There is an IVC gateway on either end of the SMTP connection between Exchange servers. This ensures that MAPI message attributes survive the outbound transit between SMTP connections. It also ensures that the MIME-encoded attributes survive the inbound transit, and are included with the message stored in the Exchange message store.

SSL

The Secure Socket Layer (SSL) protocol is the standard protocol that delivers secure content over the Internet. It is a point-to-point security protocol that secures communication between a client and a server. SSL usually does not require a special client (that is, a Web browser often will suffice) and it does not require any additional operating system software.

SSL includes client and server authentication and data encryption for a limited set of applications (for example, the Web, e-mail, news, and file transfer). SSL is useful for securing e-commerce transactions over the Internet, and the protocol is well suited for extranets and remote access because it is relatively simple to deploy.

How to Configure E-mail Inspection Engine

This section contains the following procedures:

- [Configuring Firewall Inspection of POP3 or IMAP E-mail, page 5](#) (required)
- [Verifying the E-mail Inspection Engine Configuration, page 6](#) (optional)

Configuring Firewall Inspection of POP3 or IMAP E-mail

To allow the Cisco IOS Firewall to inspect POP3 or IMAP e-mail, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip inspect name** *inspection-name* *protocol* [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**reset**] [**secure-login**] [**timeout** *seconds*]
4. **interface** *type slot/port*
5. **ip inspect name** *inspection-name* {**in** | **out**}
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip inspect name inspection-name protocol [alert {on off}] [audit-trail {on off}] [reset] [secure-login] [timeout seconds] Example: Router(config)# ip inspect name mail-guard pop3	Defines a set of inspection rules.
Step 4	interface type slot/port Example: Router(config-if)# interface 1/0	Configures an interface type.
Step 5	ip inspect name inspection-name {in out} Example: Router(config-if)# ip inspect name mail-guard in	Enables the Cisco IOS Firewall on an interface.
Step 6	exit Example: Router(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.

Verifying the E-mail Inspection Engine Configuration

To verify the E-mail Inspection Engine configuration, perform the following steps.

**Note**

Effective with Cisco IOS Release 12.4(20)T, the **debug ip inspect** command is replaced by the **debug policy-firewall** command. See the *Cisco IOS Debug Command Reference* for more information.

SUMMARY STEPS

1. **debug ip inspect imap**
2. **debug ip inspect pop3**
3. **show ip inspect { name inspection-name | config | interfaces | session [detail] | all }**

DETAILED STEPS

Step 1 **debug ip inspect imap**

Use this command to display messages about Cisco IOS Firewall events related to IMAP protocol e-mail messages.

```
Router# debug ip inspect imap
```

Step 2 **debug ip inspect pop3**

Use this command to display messages about Cisco IOS Firewall events related to POP3 protocol e-mail messages.

```
Router# debug ip inspect pop3
```

Step 3 **show ip inspect {name *inspection-name* | config | interfaces | session [detail] | all}**

Use this command to view CBAC configuration and session information.

```
Router# show ip inspect
```

```
Session audit trail is disabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
  Inspection name mail-guard
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
```

Configuration Examples for E-mail Inspection Engine

- [Configuring IMAP and POP3 Protocol E-mail: Example, page 7](#)

Configuring IMAP and POP3 Protocol E-mail: Example

The following example configures the Cisco IOS Firewall inspection of IMAP and POP3 protocol e-mail:

```
configure terminal
ip inspect name mail-guard pop3
ip inspect name mail-guard imap
exit
```

The following commands enable this functionality on an interface:

```
configure terminal
interface 1/0
ip inspect name mail-guard in
exit
```

Additional References

The following sections provide references related to E-Mail Inspection Engine.

Related Documents

Related Topic	Document Title
IMAP and POP3	White Paper: <i>Deploying Cisco Unity in Diverse Messaging Environments (All Versions with Microsoft Exchange)</i>
CBAC	<i>Cisco IOS Security Configuration Guide, Release 12.3</i> <i>Cisco IOS Security Command Reference, Release 12.3T</i>

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 1939	J Myers and M. Rose, "Post Office Protocol, Version 3 (POP3)," May 1996.
RFC 3501	M. Crispin, " <i>Internet Message Access Protocol (IMAP4rev1</i> ," March 2003.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug ip inspect**
- **ip inspect name**
- **show ip inspect**

Glossary

authentication—Process during which any unrecognized command causes the Cisco IOS Firewall to drop the packet and close the connection.

CBAC—Context-Based Access Control. A Cisco IOS Firewall set feature that scrutinizes source and destination addresses to enhance security for TCP and UDP applications that use well-known ports, such as FTP and e-mail traffic.

ESMTP—Extended Simple Mail Transfer Protocol. An extended version of the Simple Mail Transfer Protocol (SMTP), which includes additional functionality, such as delivery notification and session delivery.

IMAP—Internet Message Access Protocol. A method of accessing e-mail or bulletin board messages kept on a mail server that can be shared. IMAP permits client e-mail applications to access remote message stores as if they were local without actually transferring the message.

POP—Post Office Protocol. A protocol that client e-mail applications use to retrieve mail from a mail server.

SMTP—Simple Mail Transfer Protocol. An Internet protocol providing e-mail services.

SSL—Secure Socket Layer Protocol. This protocol is used to deliver secure information over the Internet.

state router—A router that tracks the client/server commands until the client is authenticated.

TCP—Transmission Control Protocol. A connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

UDP—User Datagram Protocol. A connectionless transport-layer protocol for exchanging datagrams without acknowledgments or guaranteed delivery.

VPN—Virtual Private Network. A network that enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN network uses “tunneling” to encrypt all information at the IP level.

**Note**

Refer to [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



ESMTP Support for Cisco IOS Firewall

The ESMTP Support for Cisco IOS Firewall feature enhances the Cisco IOS Firewall to support Extended Simple Mail Transport Protocol (ESMTP), allowing customers who install mail servers behind Cisco IOS firewalls to install their servers on the basis of ESMTP (instead of Simple Mail Transport Protocol [SMTP]).

Feature History for ESMTP Support for Cisco IOS Firewall

Release	Modification
12.3(7)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for ESMTP Support for Cisco IOS Firewall, page 1](#)
- [Information About ESMTP Support for Cisco IOS Firewall, page 2](#)
- [How to Configure a Firewall to Support ESMTP, page 6](#)
- [Configuration Examples for Firewall ESMTP Support, page 8](#)
- [Additional References, page 8](#)
- [Command Reference, page 10](#)

Prerequisites for ESMTP Support for Cisco IOS Firewall

To enable this feature, your Cisco IOS image must contain the Cisco IOS firewall.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Information About ESMTP Support for Cisco IOS Firewall

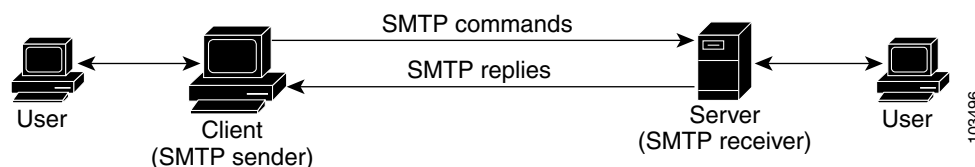
To configure a Cisco IOS firewall to inspect an ESMTP session and command sequence, you should understand the following concepts:

- [SMTP Functionality Overview, page 2](#)
- [ESMTP Overview, page 3](#)
- [SMTP Firewall and ESMTP Firewall Comparison, page 3](#)

SMTP Functionality Overview

SMTP inspection provides a basic method for exchanging e-mail messages. [Figure 26](#) and the following steps outline a basic SMTP session.

Figure 26 **Sample SMTP Exchange Topology**



After a user sends an e-mail request to the client (the “SMTP sender”), the client established a TCP channel with the server (the “SMTP receiver”). Thereafter, the client and the server exchange SMTP commands and responses until the mail transaction is complete. The steps of typical SMTP transaction are as follows:

4. The client establishes a TCP connection with the server.
5. The client sends a HELO command with its domain name. If the server can accept mail from that domain name, it responds with a 250 reply code, which allows the client to continue with the mail transaction. (If the server does not respond with a 250 reply code, the client will send a QUIT command and terminate the TCP session.)
6. The client sends the MAIL command, indicating who initiated the mail. If the server accepts the mail, it responds with an OK reply. Then, the client sends the RCPT command, identifying the recipient of the mail. If the server accepts mail for the specified recipient, it responds with an OK reply; if the server cannot accept mail for the specified recipient, it rejects the recipient but not the entire transaction. (Several recipients can be negotiated.)
7. After the list of recipients has been negotiated between the client and the server, the client sends a DATA command. If the server is ready to receive data, it responds with a 354 reply code. If the server is not ready to receive data, it responds with an error reply, and the client terminates the transaction.
8. The client sends mail data ending with a special sequence. When the server sees the end of the message, it sends a 250 code reply.
9. The client sends a QUIT command, waits for the server to respond, then terminates the session.

ESMTP Overview

Like SMTP, ESMTP inspection provides a basic method for exchanging e-mail messages. Although an ESMTP session is similar to SMTP, there is one difference—the EHLO command.

After the TCP connection has been established between the client (the ESMTP sender) and the server (the ESMTP receiver), the client sends the EHLO command (instead of the HELO command that is used for SMTP). If the server does not support ESMTP, it sends a failure reply to the client because it did not recognize the EHLO command. If it supports ESMTP, the server responds with the code 250 and a list of extensions that the server supports. (Refer to RFC 1869 for an explanation of the extensions that your server may support.)

The server may send any of the following error codes if it supports ESMTP but is unable to function as normal:

- Error code 501—The server recognizes the EHLO command but is unable to accept it.
- Error code 502—The server recognizes the EHLO command but does not implement it.
- Error code 554—The server is unable to list the service extensions it supports.

If the client receives any of these error codes, it should issue the HELO command to revert to SMTP mode or issue the QUIT command to end the session.

After the client receives a successful response to the EHLO command, it will work the same way as SMTP, except that the client may issue new extended commands, and it may add a few parameters to the MAIL FROM and REPT TO commands.

SMTP Firewall and ESMTP Firewall Comparison

Although a SMTP firewall and an ESMTP firewall support the same functionality—command inspection, session conversion, and Intrusion Detection System (IDS) detection—slight variations exist between the protocols. [Table 27](#) explains the firewall functionality and protocol-specific differences.

Table 27 *SMTP and ESMTP Firewalls Functionality Comparison*

Functionality	SMTP Firewall Description	ESMTP Firewall Description
Command Inspection	<p>The SMTP firewall inspects commands for illegal commands. Illegal commands found in a packet are modified to an “xxxx” pattern and forwarded to the server. This process causes the server to send a negative reply, forcing the client to issue a valid command.</p> <p>An illegal SMTP command is any command except the following: DATA, HELO, HELP, MAIL, NOOP, QUIT, RCPT, RSET, SAML, SEND, SOML, and VRFY.</p> <p>Note Prior to Cisco IOS Release 12.3(7)T, an SMTP firewall will reset the TCP connection upon detection of an illegal command. That is, an SMTP firewall no longer resets the TCP connection upon detecting an illegal command.</p>	<p>ESMTP command inspection is the same as SMTP command inspection, except that ESMTP supports three additional commands—AUTH, EHLO, and ETRN.</p> <p>An illegal ESMTP command is any command except the following: AUTH, DATA, EHLO, ETRN, HELO, HELP, MAIL, NOOP, QUIT, RCPT, RSET, SAML, SEND, SOML, and VRFY.</p>
Parameter Inspection	Not applicable.	<p>The ESMTP firewall inspects the following extensions by performing deeper command inspection:</p> <ul style="list-style-type: none"> • Message Size Declaration (SIZE) • Remote Queue Processing Declaration (ETRN) • Binary MIME (BINARYMIME) • Command Pipelining • Authentication • Delivery Status Notification (DSN) • Enhanced Status Code (ENHANCEDSTATUSCODE) • 8bit-MIMEtransport (8BITMIME) <p>Note All other extensions, including private extensions, are not supported.</p>

Table 27 *SMTP and ESMTP Firewalls Functionality Comparison (continued)*

Functionality	SMTP Firewall Description	ESMTP Firewall Description
EHLO Reply Inspection	Not applicable.	The ESMTP firewall inspects the EHLO reply, which contains a list of SMTP extensions that the server supports. Any unsupported extension that is found in the server's reply will be replaced with the "XXXX" pattern, which labels that extension "private." Thus, the client will no longer use the unsupported extension.
ESMTP to SMTP Session Conversion	<p>The SMTP firewall forces a client that initiates an ESMTP session to use SMTP. When a client attempts to initiate an ESMTP session by sending the ELHO command, the firewall treats the EHLO command as an illegal command and modified it to the "xxxx" pattern. This response causes the server to send a 5xx code reply, forcing the client to revert to SMTP mode.</p> <p>Note Prior to Cisco IOS Release 12.3(7)T, the firewall intercepts the EHLO command and changes it to the NOOP command. The server responds with a 250 code reply. The firewall intercepts the response and modifies it to 502 code reply, which tells the client that the EHLO command is not supported.</p>	Not applicable (because EHLO is supported in ESMTP).
IDS Signature Detection	The SMTP and ESMTP firewalls scan for a set of hard-coded IDS signatures. There are 11 signatures—6 are hard coded in the firewall and are enabled by default. The other 5 signatures remain in the IDS code and are disabled by default.	

Table 27 SMTP and ESMTP Firewalls Functionality Comparison (continued)

Functionality	SMTP Firewall Description	ESMTP Firewall Description
Command Pipelining	Not available. (The client sends a command to the server and must wait for a reply before sending another command.)	An ESMTP firewall can inspect commands that are in the pipeline. That is, commands that are sent before a response is received are inspected.
Resetting a Connection	<p>Both SMTP and ESMTP firewalls will always send a “5xx” error code and close the connection upon detection of an unsupported parameter or an IDS signature in a command. That is, the firewall sends an appropriate reply code and closes the connection with proper TCP closing sequence packets (such as FIN or FIN+ACK) so the client does not continually attempt to send the same message.</p> <p>Note Prior to Cisco IOS Release 12.3(7)T, an SMTP firewall will reset the TCP connection upon detection of an illegal command or IDS signature. This behavior causes the client to keep trying to send the same message for up to 4 days (which is when the original message is bounced back to the user).</p>	

How to Configure a Firewall to Support ESMTP

This section contains the following procedures:

- [Configuring a Firewall for ESMTP Inspection, page 6](#)

Configuring a Firewall for ESMTP Inspection

Use this task to configure a Cisco IOS Firewall to inspect an ESMTP session and command sequence.

Restrictions

SMTP and ESMTP cannot exist simultaneously. If SMTP is already configured, an attempt to configure ESMTP will result in the error message, “%ESMTP cannot coexist with SMTP, please unconfigure SMTP and try again...” If ESMTP is already configured, an attempt to configure SMTP will result in the error message, “%SMTP cannot coexist with ESMTP, please unconfigure ESMTP and try again...”

The following example illustrates how the router will react if you attempt to configure both protocols:

```
Router(config)# ip inspect name mail-guard smtp
Router(config)# ip inspect name mail-guard esmtp
ESMTP cannot coexist with SMTP, please unconfigure SMTP and try again...
Router(config)# end
Router# show running-config
.
.
.
ip inspect name mail-guard smtp
.
.
.
```

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip inspect name** *inspection-name* {**smtp** | **esmtplib**} [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**max-data** *number*] [**timeout** *seconds*]
4. **interface** *type number*
5. **ip inspect** *inspection-name* {**in** | **out**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip inspect name <i>inspection-name</i> { smtp esmtplib } [alert { on off }] [audit-trail { on off }] [max-data <i>number</i>] [timeout <i>seconds</i>] Example: Router(config)# ip inspect name test esmtplib	Configures inspection of a SMTP or an ESMTP session.
Step 4	interface <i>type number</i> Example: Router(config)# interface ethernet0	Configures an interface type and enters interface configuration mode.
Step 5	ip inspect <i>inspection-name</i> { in out } Example: Router(config-if)# ip inspect test in	Applies an inspection rule to an interface.

Troubleshooting Tips

To view and verify the inspection configuration, status, or session information, you can use any of the following EXEC commands:

- **show ip inspect name** *inspection-name*—Shows a particular configured inspection rule.
- **show ip inspect session**—Shows existing sessions that are currently being tracked and inspected by the firewall.
- **show ip inspect all**—Shows all inspection configuration and all existing sessions that are currently being tracked and inspected by the firewall.

Alert Messages

The existing SMTP-related alert message will not change. This message is logged every time the firewall detects an illegal or unsupported command. The message format is as follows:

```
FW-3-SMTP_INVALID_COMMAND: Invalid SMTP command (%s) (total %d chars) from initiator (%i:%d)
```

A new alert message is added. This message is logged whenever the firewall detects an illegal parameter in an SMTP command. The message includes the address and port of the sender as well as the illegal parameter. The message format is as follows:

```
FW-3-SMTP_INVALID_PARAMETER: Invalid SMTP parameter (%s) from initiator (%i:%d)
```

What to Do Next

To provide a record of network access through the firewall, including illegitimate access attempts, and inbound and outbound services, you should turn on logging and audit trail. For information on completing this task, refer to the section “Configuring Logging and Audit Trail” in the chapter “Configuring Context-Based Access Control” in the *Cisco IOS Security Configuration Guide*.

Configuration Examples for Firewall ESMTP Support

This section contains the following configuration example:

- [ESMTP Inspection Configuration: Example, page 8](#)

ESMTP Inspection Configuration: Example

The following example shows how to configure inspection of ESMTP traffic:

```
Router# configure terminal  
Router(config)# ip inspect name mail-guard esmtp timeout 30
```

Additional References

The following sections provide references related to ESMTP Support for Cisco IOS Firewall.

Related Documents

Related Topic	Document Title
Cisco IOS Firewall configuration	<i>The section “Traffic Filtering and Firewalls” in the Cisco IOS Security Configuration Guide</i>
Cisco IOS Firewall commands	<i>Cisco IOS Security Command Reference, Release 12.3 T</i>

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 821	<i>Simple Mail Transfer Protocol</i>
RFC 1652	SMTP Service Extension for 8bit-MIMEtransport
RFC 1845	SMTP Service Extension for Checkpoint/Restart
RFC 1869	<i>SMTP Service Extensions</i>
RFC 1870	SMTP Service Extension for Message Size Declaration
RFC 1891	SMTP Service Extension for Delivery Status Notifications
RFC 1985	SMTP Service Extension for Remote Message Queue Starting
RFC 2034	SMTP Service Extension for Returning Enhanced Error Codes
RFC 2554	SMTP Service Extension for Authentication
RFC 2645	ON-DEMAND MAIL RELAY (ODMR) SMTP with Dynamic IP Addresses
RFC 2920	SMTP Service Extension for Command Pipelining
RFC 3030	SMTP Service Extensions for Transmission of Large and Binary MIME Messages
RFC 3207	SMTP Service Extension for Secure SMTP over Transport Layer Security

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **ip inspect name**

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Firewall ACL Bypass

The Firewall ACL Bypass feature allows a packet to avoid redundant access control list (ACL) checks by allowing the firewall to permit the packet on the basis of existing inspection sessions instead of dynamic ACLs. Thus, input and output dynamic ACLs searches are eliminated, improving the overall throughput performance of the base engine.

Feature History for Firewall ACL Bypass

Release	Modification
12.3(4)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Information About Firewall ACL Bypass, page 1](#)
- [How to Use Firewall ACL Bypass, page 2](#)
- [Configuration Examples for Verifying Firewall Session Information, page 2](#)
- [Additional References, page 3](#)
- [Command Reference, page 4](#)
- [Glossary, page 6](#)

Information About Firewall ACL Bypass

To better understand how dynamic ACL bypass works, you should understand the following concepts:

- [Benefits of Firewall ACL Bypass, page 2](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Firewall ACL Bypass Functionality Overview, page 2](#)

Benefits of Firewall ACL Bypass

Because input and output dynamic ACLs are no longer necessary, the need for context-based access control (CBAC) to create dynamic ACLs on the interface is eliminated. Thus, the following benefits are now available:

- Improved connections per second performance of the firewall
- Reduced run-time memory consumption of the firewall

Firewall ACL Bypass Functionality Overview

Before ACL bypassing was implemented, a packet could be subjected to as many as three redundant searches—an input ACL search, an output ACL search, and an inspection session search. Each dynamic ACL that CBAC creates corresponds to a single inspection session. Thus, a matching dynamic ACL entry for a given packet implies that a matching inspection session exists and that the packet should be permitted through the ACL. Because a matching inspection session is often found in the beginning of IP processing, the input and output dynamic ACL searches are no longer necessary and can be eliminated.

ACL bypassing subjects the packet to one search—the inspection session search—during its processing path through the router. When a packet is subjected to a single inspection session search before the ACL checks, the packet is matched against the list of session identifiers that already exist on the interface. (Session identifiers keep track of the source and destination IP addresses and ports of the packets and on which interface the packet arrived.)



Note

Session identifiers are not created on interfaces for inspection sessions that are only Intrusion Detection Sessions (IDS).

How to Use Firewall ACL Bypass

After your firewall is configured for inspection, ACL bypassing is performed by default. That is, you should configure inspection as normal.

To configure CBAC for your firewall, see the following chapter “Configuring Context-Based Access Control” in the *Cisco IOS Security Configuration Guide*.

Configuration Examples for Verifying Firewall Session Information

After you have configured your firewall for inspection, you can use the **show ip inspect sessions detail** command to view session inspection information. The following examples show how eliminating dynamic ACLs changes the sample output:

- [Old show ip inspect CLI Output: Example, page 3](#)
- [New show ip inspect CLI Output: Example, page 3](#)

Old show ip inspect CLI Output: Example

The following is sample output from the **show ip inspect session detail** command, which shows that an outgoing ACL and an inbound ACL (dynamic ACLs) have been created to allow return traffic:

```
Router# show ip inspect session detail
```

```
Established Sessions
```

```
Session 80E87274 (192.168.1.116:32956)=>(192.168.101.115:23) tcp SIS_OPEN
Created 00:00:08, Last heard 00:00:04
Bytes sent (initiator:responder) [140:298] acl created 2
Outgoing access-list 102 applied to interface FastEthernet0/0
Inbound access-list 101 applied to interface FastEthernet0/1
```

```
Router# show access-lists
```

```
Extended IP access list 101
```

```
 permit tcp host 192.168.101.115 eq telnet host 192.168.1.116 eq 32956 (27 matches)
 deny udp any any
 deny tcp any any
 permit ip any any
```

```
Extended IP access list 102
```

```
 permit tcp host 192.168.101.115 eq telnet host 192.168.1.116 eq 32956 (27 matches)
 deny udp any any
 deny tcp any any
 permit ip any any
```

New show ip inspect CLI Output: Example

The following is sample output from the **show ip inspect session detail** command, which shows related ACL information (such as session identifiers [SID]), but does not show dynamic ACLs, which are no longer created:

```
Router# show ip inspect session detail
```

```
Established Sessions
```

```
Session 814063CC (192.168.1.116:32955)=>(192.168.101.115:23) tcp SIS_OPEN
Created 00:00:10, Last heard 00:00:06
Bytes sent (initiator:responder) [140:298]
In  SID 192.168.101.115[23:23]=>192.168.1.117[32955:32955] on ACL 101 (15 matches)
Out SID 192.168.101.115[23:23]=>192.168.1.116[32955:32955] on ACL 102
```

```
Router# show access-list
```

```
Extended IP access list 101
```

```
 deny udp any any (20229 matches)
 deny tcp any any
 permit ip any any (6 matches)
```

```
Extended IP access list 102
```

```
 deny udp any any
 deny tcp any any
 permit ip any any (1 match)
```

Additional References

The following sections provide references related to Dynamic ACL Bypass.

Related Documents

Related Topic	Document Title
Cisco IOS Firewalls and ACLs	<i>The section “Traffic Filtering and Firewalls” in the Cisco IOS Security Configuration Guide</i>
Cisco IOS Firewall commands	<i>Cisco IOS Security Command Reference, Release 12.3 T</i>

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at

<http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **show ip inspect**

Glossary

connections per second—Metric defined by the number of short-lived connections that can be created and deleted within 1 second by a router running CBAC. (These connections apply only to TCP connections because UDP is a connectionless protocol.)

throughput—Metric defined by the number of packets transferred from the input interface to the output interface within 1 second by a router running CBAC.

**Note**

Refer to [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Firewall N2H2 Support

The Firewall N2H2 Support feature provides users with an additional option when choosing the URL filter vendor. Just like the Websense URL filtering server, N2H2 interacts with your Cisco IOS firewall (also known as Cisco Secure Integrated Software [CSIS]) to allow you to prevent users from accessing specified websites on the basis of some policy. The Cisco IOS firewall works with the N2H2 Internet Filtering Protocol (IFP) server to know whether a particular URL should be allowed or denied (blocked).

Feature Specifications for the Firewall N2H2 Support feature

Feature History

Release	Modification
12.2(11)YU	This feature was introduced.
12.2(15)T	This feature was integrated into Cisco IOS Release 12.2(15)T.

Supported Platforms

For platforms supported in Cisco IOS Release 12.2(11)YU and 12.2(15)T, consult Cisco Feature Navigator.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions for Firewall N2H2 Support, page 2](#)
- [Information About Cisco N2H2 Support, page 2](#)
- [How to Configure N2H2 URL Support, page 5](#)
- [Configuration Examples for Firewall and Webserver, page 11](#)
- [Additional References, page 16](#)
- [Command Reference, page 18](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Glossary, page 20](#)

Restrictions for Firewall N2H2 Support

N2H2 IFP (Server) Requirement

To enable this feature, you must have at least one N2H2 server; however, two or more N2H2 servers are preferred. Although there is no limit to the number of N2H2 servers you may have, and you can configure as many servers as you wish, only one server will be active at any given time—the primary server. URL lookup requests will be sent only to the primary server.

URL Filtering Support Restriction

This feature supports only one active URL filtering scheme at a time. (Before enabling N2H2 URL filtering, you should always ensure that there is not another URL filtering scheme configured, such as Websense.)

Username Restriction

N2H2 requires the username to be supplied with the URL lookup request. Thus, the user-based policy will not work with N2H2 because the current Cisco IOS software does not retrieve the username.

Protocol Used to Communicate Between Firewall and N2H2 Server Restriction

TCP is currently the only protocol used to communicate between the Cisco IOS firewall (UNIX FileSystem [UFS]) and the N2H2 server.

Information About Cisco N2H2 Support

To configure Firewall N2H2 support, you must understand the following concepts:

- [Benefits of Firewall N2H2 Support, page 2](#)
- [Feature Design of Firewall N2H2 Support, page 4](#)
- [Supported N2H2 Filtering Methods, page 5](#)

Benefits of Firewall N2H2 Support

The Cisco IOS Firewall N2H2 Support feature provides an Internet management application that allows you to control web traffic for a given host or user on the basis of a specified security policy. In addition, the following functions are available in this feature:

Primary and Secondary Servers

When users configure multiple N2H2 servers, the firewall will use only one server at a time—the primary server; all other servers are called secondary servers. When the primary server becomes unavailable for any reason, it becomes a secondary server and one of the secondary servers becomes the primary server.

A firewall marks a primary server as down when sending a request to or receiving a response from the server fails. When a primary server goes down, the system will go to the beginning of the configured servers list and try to activate the first server on the list. If the first server on the list is unavailable, it will

try the second server on the list; the system will keep trying to activate a server until it is successful or until it reaches the end of the server list. If the system reaches the end of the server list, it will set a flag indicating that all of the servers are down, and it will enter allowmode.

When all the servers are down and the system is in allow mode, a periodic event that occurs for each minute will trace through the server list, trying to bring up a server by opening a TCP connection. If the TCP connection is successfully opened, the server is considered to be up, and the system will return to operational mode.

IP Cache Table

This function provides an IP cache table that contains the IP addresses of web servers whose underlying URLs can be accessed by all users and hosts.

The caching algorithm involves three parameters—the maximum number of IP addresses that can be cached, an idle time, and an absolute time. The algorithm also involves two timers—idle timer and absolute timer. The idle timer is a small periodic timer (1 minute) that checks to see whether the number of cached IP addresses in the cache table exceeds 80 percent of the maximum limit. If the cached IP addresses have exceeded 80 percent, it will start removing idle entries; if it has not exceeded 80 percent, it will quit and wait for the next cycle. The absolute timer is a large periodic timer (1 hour) that is used to remove all of the elapsed entries. (The age of an elapsed entry is greater than the absolute time.) An elapsed entry will also be removed during cache lookup.

The idle time value is fixed at 10 minutes. The absolute time value is taken from the N2H2 lookup response, which is often greater than 15 hours. The absolute value for cache entries made out of exclusive-domains is 12 hours. The maximum number of cache entries is configurable.

To configure cache table parameters, use the **ip urlfilter cache** command.

Packet Buffering

This function allows you to increase the maximum number of HTTP responses that a Cisco IOS firewall can hold. If the HTTP responses arrive prior to an N2H2 server reply, this buffering scheme allows your firewall to store a maximum of 200 HTTP responses. (After 200 responses have been reached, the firewall will drop further responses.) The responses will remain in the buffer until an allow or deny message is received from N2H2: if the status indicates that the URL is allowed, the firewall will release the HTTP responses in the buffer to the browser of the end user; if the status indicates that the URL is blocked, the firewall will discard the HTTP responses in the buffer and close the connection to both ends. This function prevents numerous HTTP responses from overwhelming your system.

To configure the maximum number of HTTP responses for your firewall, use the **ip urlfilter max-resp-pak** command.

Exclusive Domains

This function provides a configurable list of domain names so that the Cisco IOS firewall does not have to send a lookup request to the N2H2 server for the HTTP traffic that is destined for one of the domains in the exclusive list. Thus, the N2H2 server does not have to deal with look-up requests for HTTP traffic that is destined for a host that has already been marked as “allowed.”

Flexibility when entering domain names is also provided; that is, the user can enter the complete domain name or a partial domain name. If the user adds a complete domain name such as “www.cisco.com” to the exclusive domain list, all HTTP traffic whose URLs are destined for this domain (such as www.cisco.com/news and www.cisco.com/index) will be excluded from the N2H2 URL filtering policies and, on the basis of the configuration, the URLs will be permitted or blocked (denied).

If the user adds only a partial domain name to the exclusive domain list, such as “.cisco.com,” all URLs whose domain names end with this partial domain name (such as www.cisco.com/products and www.cisco.com/eng) will be excluded from the N2H2 URL filtering policies and, based upon the configuration, the URLs will be permitted or blocked (denied).

To configure an exclusive domain list, use the **ip urlfilter exclusive-domain** command.

Allow Mode

The system will go into allow mode when connections to all the N2H2 servers are down. The system will return to normal mode when a connection to at least one web N2H2 server is up. Allow mode directs your system to forward or drop all packets on the basis of the configurable allow mode setting. By default, allow mode is off, so all HTTP requests are forbidden if all N2H2 servers are down.

To configure allow mode for your system, use the **ip urlfilter allowmode** command.

Feature Design of Firewall N2H2 Support

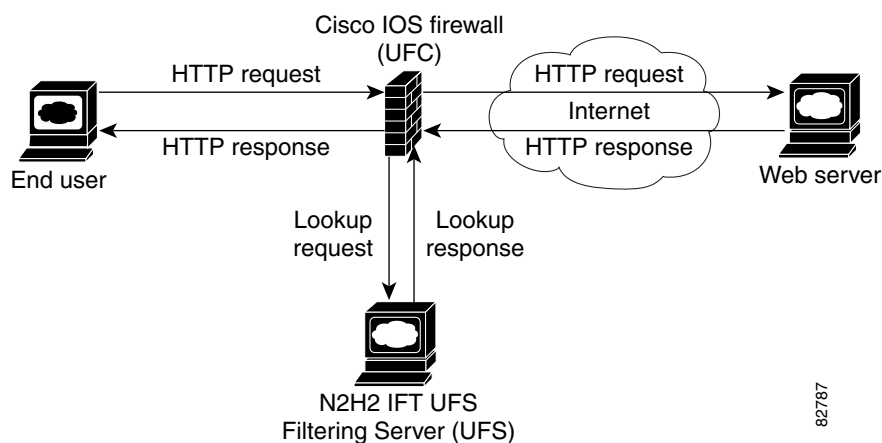


Note

This feature assumes that the N2H2 server will be part of a protected network and that requests from the Cisco IOS firewall will not travel over any unprotected network to reach the N2H2 server.

Figure 27 and the corresponding steps explain a sample URL filtering network topology.

Figure 27 Cisco IOS Firewall N2H2 URL Filtering Sample Topology



1. The end user browses a page on the web server, and the browser sends an HTTP request.
2. After the Cisco IOS firewall receives this request, it forwards the request to the web server, while simultaneously extracting the URL and sending a look-up request to the N2H2 server.
3. After the N2H2 server receives the look-up request, it checks its database to see whether it should permit or deny the URL; it returns a permit or deny status via a look-up response to the Cisco IOS firewall.
4. After the Cisco IOS Firewall receives this look-up response, it performs one of the following functions:
 - If the look-up response permits the URL, it sends the HTTP response to the end user.

- If the look-up response denies the URL, the N2H2 server redirects the user to its own internal web server, which displays a message that describes the category under which the URL is blocked; thereafter, the connection is reset to both ends.

Supported N2H2 Filtering Methods

The Cisco IOS firewall supports most of the filtering methods that are supported by the N2H2 server. [Table 28](#) lists N2H2 filtering methods and identifies which methods are supported by Cisco.

Table 28 *N2H2 Filtering Methods Supported on Cisco IOS Firewall*

N2H2 Filtering Method	Description	Supported by Cisco IOS Firewall?
Client-IP-based filtering	Filtering is applied to specified client IP addresses	Yes
Global filtering	Filtering is applied to all users, groups, and IP addresses	Yes
User-based filtering	Filtering is applied to a specified user	No

How to Configure N2H2 URL Support

To configure your Cisco IOS firewall to interact with at least one N2H2 server to provide URL filtering, configure the following procedures:

- [Configuring Cisco IOS Firewall N2H2 URL Filtering, page 5](#) (required)
- [Verifying Firewall and N2H2 URL Filtering, page 10](#) (optional)
- [Maintaining the Cache Table, page 10](#) (optional)
- [Monitoring the URL Filter Subsystems, page 11](#) (optional)

Configuring Cisco IOS Firewall N2H2 URL Filtering

N2H2 is based on a pass-through filtering technology, which is the most accurate, reliable, and scalable method of Internet filtering. Pass-through filtering requires all requests for web pages to pass through an Internet control point, such as a firewall, proxy server, or caching device. N2H2 is integrated with these control points and checks each request to determine whether it should be allowed or denied. All responses are logged for reporting purposes.

Prerequisites

- Before enabling N2H2 URL filtering, you should always ensure that there is not another URL filtering scheme configured, such as Websense. If you try to enter a new filtering scheme when one already exists, the new scheme will be ignored, and the system will display an error message that says, “different URL filtering scheme cannot co-exist.”

- URL filtering does not have an interface-specific command. It relies on Cisco IOS firewall C HTTP inspection to classify the traffic that needs filtering. This makes the configuration of Cisco IOS firewall inspection mandatory for the URL filtering feature to work. For more details on Cisco IOS firewall configuration, refer to the chapter “Cisco IOS Firewall Overview” in the IOS Security Configuration Guide, Release 12.2.

Restrictions

Enabling HTTP inspection (via the **ip inspect name** command) triggers the Java applet scanner, which is very CPU intensive. The only way to stop the Java applet scanner is to specify the **java-list access-list** option and configure a standard access-list to allow any traffic. Configuring URL filtering without enabling the **java-list access-list** option will severely impact performance.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip inspect name** *inspection-name* **http** [**urlfilter**] [**java-list** *access-list*] [**alert** {**on** | **off**}] [**timeout** *seconds*] [**audit-trail** {**on** | **off**}]
4. **ip urlfilter server vendor** {**websense** | **n2h2**} *ip-address* [**port** *port-number*] [**timeout** *seconds*] [**retransmit** *number*]
5. **ip urlfilter alert**
6. **ip urlfilter audit-trail**
7. **ip urlfilter urlf-server-log**
8. **ip urlfilter exclusive-domain** {**permit** | **deny**} *domain-name*
9. **ip urlfilter cache** *number*
10. **ip urlfilter allowmode** [**on** | **off**]
11. **ip urlfilter max-resp-pak** *number*
12. **ip urlfilter max-request** *number*
13. **interface** *type slot/port*
14. **ip inspect inspection-name** {**in** | **out**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example: Router> enable	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	

	Command or Action	Purpose
Step 3	<pre>ip inspect name inspection-name http [urlfilter] [java-list access-list] [alert {on off}] [timeout seconds] [audit-trail {on off}]</pre> <p>Example: Router(config)# ip inspect name fw_urlf http urlfilter java-list 51 timeout 30</p>	<p>Turns on HTTP inspection. The urlfilter keyword associates URL filtering with HTTP inspection.</p> <p>Note You may configure two or more inspections in a router, but URL filtering will work only with the inspections in which the urlfilter keyword is enabled.</p> <p>Note Enabling HTTP inspection with or without any options triggers the Java applet scanner, which is CPU intensive. The only way to stop the Java applet scanner is to specify the java-list access-list option. Configuring URL filtering without enabling the java-list access-list option will severely impact performance.</p>
Step 4	<pre>ip urlfilter server vendor {websense n2h2} ip-address [port port-number] [timeout seconds] [retransmit number]</pre> <p>Example: Router(config)# ip urlfilter server vendor websense 10.201.6.202</p>	<p>Configures an N2H2 server to interact with the firewall to filter HTTP requests based on a specified policy.</p> <ul style="list-style-type: none"> <i>ip-address</i>—IP address of the vendor server. port port-number—Port number that the vendor server listens on. The default port number is 4005. timeout seconds—Length of time that the firewall will wait for a response from the vendor server. The default timeout is 5 minutes. retransmit number—Number of times the firewall will retransmit the request when a response does not arrive. The default value is 2 times.
Step 5	<pre>ip urlfilter alert</pre> <p>Example: Router(config)# ip urlfilter alert</p>	<p>(Optional) Enables the system alert, which displays system messages such as a server entering allow mode or going down.</p> <ul style="list-style-type: none"> The system alert is enabled by default.
Step 6	<pre>ip urlfilter audit-trail</pre> <p>Example: Router(config)# ip urlfilter audit-trail</p>	<p>(Optional) Enables the logging of messages into the syslog server of router.</p> <ul style="list-style-type: none"> This function is disabled by default.
Step 7	<pre>ip urlfilter urlf-server-log</pre> <p>Example: Router(config)# ip urlfilter urlf-server-log</p>	<p>(Optional) Enables the logging of system messages on the URL filtering server (the N2H2 server). This function is disabled by default.</p>

	Command or Action	Purpose
Step 8	<p>ip urlfilter exclusive-domain {permit deny} <i>domain-name</i></p> <p>Example: Router(config)# ip urlfilter exclusive-domain permit www.cisco.com</p>	<p>(Optional) Adds a domain name to or from the exclusive domain list so the firewall does not have to send look-up requests to the N2H2 server.</p> <ul style="list-style-type: none"> • permit—Permits all traffic destined for the specified domain name. • deny—Denies all traffic destined for the specified domain name. • <i>domain-name</i>—Domain name that is added or removed from the exclusive domain list.
Step 9	<p>ip urlfilter cache <i>number</i></p> <p>Example: Router(config)# ip urlfilter cache 4500</p>	<p>(Optional) Configures cache table parameters.</p> <ul style="list-style-type: none"> • <i>number</i>—Specifies the maximum number of destination IP addresses that can be cached into the cache table; the default is 5000.
Step 10	<p>ip urlfilter allowmode [on off]</p> <p>Example: Router(config)# ip urlfilter allowmode on</p>	<p>(Optional) Turns on the default mode of the filtering systems.</p> <ul style="list-style-type: none"> • on—Allows HTTP requests to pass to the end user if all N2H2 servers are down. • off—Blocks all HTTP requests if all N2H2 servers are down; off is the default setting.
Step 11	<p>ip urlfilter max-resp-pak <i>number</i></p> <p>Example: Router(config)# ip urlfilter max-resp-pak 150</p>	<p>(Optional) Configures the maximum number of HTTP responses that the firewall can keep in its packet buffer.</p> <ul style="list-style-type: none"> • The default value is 200. The maximum value is 20000, so you may set the max-resp-pak <i>number</i> to a value up to 20000.
Step 12	<p>ip urlfilter max-request <i>number</i></p> <p>Example: Router(config)# ip urlfilter max-request 500</p>	<p>(Optional) Sets the maximum number of outstanding requests that can exist at any given time.</p> <ul style="list-style-type: none"> • The default value is 1000.
Step 13	<p>interface <i>type slot/port</i></p> <p>Example: Router(config)# interface FastEthernet 0/0</p>	Configures an interface type and enters interface configuration mode
Step 14	<p>ip inspect inspection-name {in out}</p> <p>Example: Router(config-if)# ip inspect inspection-name out</p>	<p>Applies a set of inspection rules to an interface.</p> <ul style="list-style-type: none"> • URL filtering is associated with inspection, and inspection is an interface-specific command. Hence, the ip inspect command needs to be configured on an interface.

Troubleshooting Tips

This feature introduces the following alert messages:

- “%URLF-3-SERVER_DOWN: Connection to the URL filter server 10.92.0.9 is down”

This level three LOG_ERR-type message is displayed when a configured UFS goes down. When this happens, the firewall will mark the configured server as secondary, try to bring up one of the other secondary servers, and mark that server as the primary server. If there is no other server configured, the firewall will enter allow mode and display the “URLF-3-ALLOW_MODE” message.

- %URLF-3-ALLOW_MODE: Connection to all URL filter servers are down and ALLOW MODE is OFF

This LOG_ERR type message is displayed when all UFSs are down and the system enters allow mode.



Note Whenever the system goes into allow mode (all filter servers are down), a periodic keepalive timer will be triggered which will try to bring up a server by opening a TCP connection.

- “%URLF-5-SERVER_UP: Connection to an URL filter server 10.92.0.9 is made, the system is returning from ALLOW MODE”

This LOG_NOTICE-type message is displayed when the UFSs are detected as being up and the system is returning from allow-mode.

- “%URLF-4-URL_TOO_LONG:URL too long (more than 3072 bytes), possibly a fake packet?”

This LOG_WARNING-type message is displayed when the URL in a look-up request is too long; any URL longer than 3K will be dropped.

- “%URLF-4-MAX_REQ: The number of pending request exceeds the maximum limit <1000>”

This LOG_WARNING-type message is displayed when the number of pending requests in the system exceeds the maximum limit and all further requests are dropped.

To display these alert messages, use the **ip urlfilter alert** command.

This feature introduces the following syslog messages:

- “%URLF-6-SITE_ALLOWED: Client 10.0.0.2:12543 accessed server 10.76.82.21:8080”

This message is logged for each request whose destination IP address is found in the cache. It includes the source IP address, source port number, destination IP address, and destination port number. The URL is not logged because the IP address of the request is found in the cache, so parsing the request and extracting the URL is a waste of time.

- “%URLF-4-SITE-BLOCKED: Access denied for the site ‘www.sports.com’; client 10.54.192.6:34557 server 172.24.50.12:80”

This message is logged when a request finds a match against one of the blocked domains in the exclusive-domain list or the corresponding entry in the IP cache.

- “%URLF-6-URL_ALLOWED: Access allowed for URL http://www.n2h2.com/; client 10.54.192.6:54123 server 192.168.0.1:80”

This message is logged for each URL request that is allowed by a UFS. It includes the allowed URL, source IP address, source port number, destination IP address, and destination port number. Longer URLs will be truncated to 300 bytes and logged.

- “%URLF-6-URL_BLOCKED: Access denied URL http://www.google.com; client 10.54.192.6:54678 server 172.19.14.2:80”

This message is logged for each URL request that is blocked by a UFS. It includes the blocked URL, source IP address, source port number, destination IP address, and destination port number. Longer URLs will be truncated to 300 bytes and then logged.

To display these syslog messages, use the **ip urlfilter audit-trail** command.

Verifying Firewall and N2H2 URL Filtering

To verify that the Firewall N2H2 Support feature is working, perform any of the following optional steps:

SUMMARY STEPS

1. **enable**
2. **show ip urlfilter cache**
3. **show ip urlfilter config**

DETAILED STEPS

Command or Action	Purpose
enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
show ip urlfilter cache Example: Router# show ip urlfilter cache	Displays the destination IP addresses that are cached into the cache table.
show ip urlfilter config Example: Router# show ip urlfilter config	Displays the size of the cache, the maximum number of outstanding requests, the allow mode state, and the list of configured N2H2 servers.
show ip urlfilter statistics Example: Router# show ip urlfilter statistics	Displays information such as the number of requests that are sent to the N2H2 server, the number of responses received from the N2H2 server, the number pending requests in the system, the number of failed requests, the number of blocked URLs.

Maintaining the Cache Table

To clear the cache table of a specified or all IP addresses, perform the following optional steps:

SUMMARY STEPS

1. **enable**
2. **clear ip urlfilter cache**

DETAILED STEPS

Command or Action	Purpose
enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
clear ip urlfilter cache { <i>ip-address</i> all } Example: Router# clear ip urlfilter cache all	Clears the cache table.

Monitoring the URL Filter Subsystems

To monitor the URL filter subsystems, perform the following optional steps:

SUMMARY STEPS

1. **enable**
2. **debug ip urlfilter** {**function-trace** | **detailed** | **events**}

DETAILED STEPS

Command or Action	Purpose
enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
debug ip urlfilter { function-trace detailed events } Example: Router# debug ip urlfilter detailed	Enables debugging information of URL filter subsystems. <ul style="list-style-type: none"> function-trace—Prints a sequence of important functions that are called when configuring URL filtering. detailed—Prints detailed information about various activities that occur during URL filtering. events—Prints various events such as queue event, timer event, and socket event.

Configuration Examples for Firewall and Webserver

This section provides the following comprehensive configuration example:

- [URL Filter Client \(Firewall\) Configuration Example, page 12](#)

URL Filter Client (Firewall) Configuration Example

The following example shows how to configure the Cisco IOS firewall (also known as the URL filter client [UFC]) for N2H2 URL filtering:

Topology:

```

End User-----LAN-----Fa0/0 -- Firewall -- S2/0----- Internet ---- Web Server
                        |
                        | Router
N2H2
Server -----+

```

Router Configuration:

Example 1:

```

hostname fw9-7200b
!
!-----
! The following commands define the inspection rule "myfw," allowing
! the specified protocols to be inspected. Note that the "urlfilter"
! keyword entered for HTTP protocol enables URL filtering on HTTP
! traffic that are bound to this inspection.
!-----
!
ip inspect name myfw http urlfilter
ip inspect name myfw ftp
ip inspect name myfw smtp
ip inspect name myfw h323
!
!-----
! The following command sets the URL filtering cache table size to 12000.
!-----
ip urlfilter cache 12000
!
!-----
! The following commands configure three exclusive domains--
! two partial domains and one complete domain.
!-----
ip urlfilter exclusive-domain permit .weapons.com
ip urlfilter exclusive-domain deny .nbc.com
ip urlfilter exclusive-domain permit www.cisco.com
!
!-----
! The following two commands enable URL filtering Audit Trail and
! Alert messages.
!-----
ip urlfilter audit-trail
ip urlfilter alert
!
!-----
! The command configures the N2H2 URL filtering server installed
! on 192.168.3.1.
!-----
ip urlfilter server vendor n2h2 192.168.3.1
!
!-----
! Create Access Control List 102:
! ACL 102 denies all IP protocol traffic except for ICMP traffic.
! This means that only the return traffic for protocols defined in the
! inspection rule and the ICMP traffic is allowed access through the

```

```

! interface where this rule is applied.
!
! Note that ACL is given here for an example; it is not relevant
! to the URL filtering. The URL filtering will work without ACL also.
!-----
!
access-list 102 permit icmp any any
access-list 102 deny tcp any any
access-list 102 deny udp any any
access-list 102 deny ip any any
!
!
interface FastEthernet0/0
ip address 192.168.3.254 255.255.255.0
ip nat inside
no ip route-cache
no ip mroute-cache
!
interface Ethernet1/0
no ip route-cache
no ip mroute-cache
shutdown
duplex half
!
interface Ethernet1/1
no ip address
no ip mroute-cache
shutdown
duplex half
!
!-----
! The ACL and CBAC inspection rules are applied to the Serial2/0 interface.
! In this example, the ACL is applied IN, meaning that it applies to traffic
! inbound from the internet. The CBAC inspection rule myfw is applied OUT,
! meaning that CBAC inspects the traffic that goes out through the interface
! and controls return traffic to the router for an existing connection.
!-----
interface Serial2/0
ip address 10.6.9.7 255.255.0.0
ip access-group 102 in
ip nat outside
ip inspect myfw out
no ip directed-broadcast
no ip mroute-cache
!
ip nat inside source static 192.168.3.1 10.6.243.1
ip nat inside source static 192.168.3.2 10.6.243.2
ip nat inside source static 192.168.3.3 10.6.243.3
ip classless
ip route 192.168.0.30 255.255.255.255 10.6.0.1
!
!
line con 0
exec-timeout 0 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
password letmein
login
!
end

```

Example 2:

```
! In the above example, the CBAC can also be configured on the inbound
! FastEthernet0/0 interface as IN, in which case the CBAC inspects all
! the traffic that comes in on FastEthernet0/0 and controls return traffic
! that leaves out of this interface for an existing connection.
```

```
interface FastEthernet0/0
ip address 192.168.3.254 255.255.255.0
ip access-group 102 out
ip nat inside
ip inspect myfw in
no ip route-cache
no ip mroute-cache
!
!
hostname fw9-7200b
!
logging buffered 64000 debugging
enable secret 5 $1$qMOf$umPb75mb3sV27JpNbW//7.
!
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
ip cef
no ip domain lookup
!
ip inspect name test http urlfilter
ip urlfilter cache 5
ip urlfilter exclusive-domain permit .weapons.com
ip urlfilter exclusive-domain deny .nbc.com
ip urlfilter exclusive-domain permit www.cisco.com
ip urlfilter audit-trail
ip urlfilter alert
ip urlfilter server vendor n2h2 192.168.3.1
ip audit notify log
ip audit po max-events 100
ip port-map http port 8080
!
no voice hpi capture buffer
no voice hpi capture destination
!
mta receive maximum-recipients 0
!
interface FastEthernet0/0
ip address 192.168.3.254 255.255.255.0
ip access-group 101 out
ip nat inside
ip inspect test in
no ip route-cache
no ip mroute-cache
!
interface Ethernet1/0
ip address 10.6.9.7 255.255.0.0
ip nat outside
no ip route-cache
no ip mroute-cache
duplex half
!
interface Ethernet1/1
no ip address
no ip mroute-cache
shutdown
duplex half
```

```
!  
interface Ethernet1/2  
  no ip address  
  no ip mroute-cache  
  shutdown  
  duplex half  
!  
interface Ethernet1/3  
  no ip address  
  no ip mroute-cache  
  shutdown  
  duplex half  
!  
interface Serial2/0  
  no ip address  
  no ip mroute-cache  
  shutdown  
  dsu bandwidth 44210  
  framing c-bit  
  cablelength 10  
  serial restart_delay 0  
  fair-queue  
!  
ip nat pool devtest 10.6.243.21 10.6.243.220 netmask 255.255.0.0  
ip nat inside source list 1 pool devtest  
ip nat inside source static 192.168.3.1 10.6.243.1  
ip nat inside source static 192.168.3.2 10.6.243.2  
ip nat inside source static 192.168.3.3 10.6.243.3  
ip classless  
ip route 192.168.0.30 255.255.255.255 10.6.0.1  
no ip http server  
no ip http secure-server  
!  
ip pim bidir-enable  
!  
!  
access-list 101 deny tcp any any  
access-list 101 deny udp any any  
access-list 101 permit ip any any  
access-list 102 deny tcp any any  
access-list 102 deny udp any any  
access-list 102 permit ip any any  
dialer-list 1 protocol ip permit  
dialer-list 1 protocol ipx permit  
!  
!  
call rsvp-sync  
!  
!  
mgcp profile default  
!  
dial-peer cor custom  
!  
!  
!gatekeeper  
  shutdown  
!  
!  
line con 0  
  exec-timeout 0 0  
  stopbits 1  
line aux 0  
  stopbits 1  
line vty 0 4
```

```
password letmein
login
!
exception core-file sisu-devtest/coredump/fw9-7200b.core
exception dump 192.168.0.1
no scheduler max-task-time
!
end
```

Additional References

For additional information related to the Firewall N2H2 Support feature, refer to the following references:

- [Related Documents, page 17](#)
- [Standards, page 17](#)
- [MIBs, page 17](#)
- [RFCs, page 18](#)
- [Technical Assistance, page 18](#)

Related Documents

Related Topic	Document Title
Websense URL filtering information	<i>Firewall Websense URL Filtering</i> , Cisco IOS Release 12.2(15)T feature module
Additional Cisco IOS firewall configuration tasks and information	<i>The part “Traffic Filtering and Firewalls” in the Cisco IOS Security Configuration Guide, Release 12.2</i>
Additional Cisco IOS firewall commands	<i>The part “Traffic Filtering and Firewalls” in the Cisco IOS Security Command Reference, Release 12.2</i>
Cisco IOS firewall configuration	The chapter “Cisco IOS Firewall Overview” in the <i>Cisco IOS Security Configuration Guide, Release 12.2</i>

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

RFCs ¹	Title
RFC 1945	<i>Hypertext Transfer Protocol — HTTP/1.0</i>
RFC 2616	<i>Hypertext Transfer Protocol — HTTP/1.1</i>

1. Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

New Commands

- **clear ip urlfilter cache**
- **debug ip urlfilter**
- **ip urlfilter alert**
- **ip urlfilter allowmode**
- **ip urlfilter audit-trail**
- **ip urlfilter cache**
- **ip urlfilter exclusive-domain**
- **ip urlfilter max-request**
- **ip urlfilter max-resp-pak**
- **ip urlfilter server vendor**
- **ip urlfilter urlf-server-log**
- **show ip urlfilter cache**
- **show ip urlfilter config**
- **show ip urlfilter statistics**

Modified Command

- `ip inspect name`

Glossary

ACL—Access Control List.

CSIS—Cisco Secure Integrated Software. CSIS is a content-based firewall that currently inspects application data, checks for protocol conformance, extracts the relevant port information to create dynamic access list entries that successfully allows return traffic, and closes the ports at the end of the session.

ICMP—Internet Control Message Protocol. ICMP is a network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. ICMP is documented in RFC 792.

UFC—URL filter client. UFC is a separate process that accepts URLs from CSIS, forwards the URL to the Websense server, and process the replies from the vendor server (Websense or N2H2).

UFS—URL filter server. UFS is a generic name given to the vendor server (Websense or N2H2), which processes URLs and decides whether to allow or deny web traffic based on a given policy.

**Note**

Refer to the [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Firewall Stateful Inspection of ICMP

The Firewall Stateful Inspection of ICMP feature addresses the limitation of qualifying Internet Control Management Protocol (ICMP) messages into either a malicious or benign category by allowing the Cisco IOS firewall to use stateful inspection to “trust” ICMP messages that are generated within a private network and to permit the associated ICMP replies. Thus, network administrators can debug network issues by using ICMP without concern that possible intruders may enter the network.

Feature Specifications for the Firewall Stateful Inspection of ICMP feature

Feature History

Release	Modification
12.2(11)YU	This feature was introduced.
12.2(15)T	This feature was integrated into Cisco IOS Release 12.2(15)T.

Supported Platforms

For platforms supported in Cisco IOS Release 12.2(11)YU and 12.2(15)T, consult Cisco Feature Navigator.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions for Firewall Stateful Inspection of ICMP, page 2](#)
- [Information About Firewall Stateful Inspection of ICMP, page 2](#)
- [How to Use Firewall Stateful Inspection of ICMP, page 3](#)
- [Configuration Examples for Stateful Inspection of ICMP, page 6](#)
- [Additional References, page 7](#)
- [Command Reference, page 9](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Glossary, page 10](#)

Restrictions for Firewall Stateful Inspection of ICMP

- To enable this feature, your Cisco IOS image must contain the Cisco IOS firewall.
- This feature does not work for the User Datagram Protocol (UDP) traceroute, in which UDP datagrams are sent instead of ICMP packets. The UDP traceroute is typically the default for UNIX systems. To use ICMP inspection with a UNIX host, use the “I” option with the traceroute command. This functionality will cause the UNIX host to generate ICMP traceroute packets, which will be inspected by the Cisco IOS firewall ICMP.

Information About Firewall Stateful Inspection of ICMP

The following sections provide information about Cisco IOS Firewall Stateful Inspection of ICMP:

- [Feature Design of Firewall Stateful Inspection of ICMP, page 2](#)
- [ICMP Inspection Checking, page 3](#)

Feature Design of Firewall Stateful Inspection of ICMP

ICMP is used to report errors and information about a network. It is a useful tool for network administrators who are trying to debug network connectivity issues. Unfortunately, intruders can also use ICMP to discover the topology of a private network. To guard against a potential intruder, ICMP messages can be blocked from entering a private network; however, a network administrator may then be unable to debug the network. Although a Cisco IOS router can be configured using access lists to selectively allow certain ICMP messages through the router, the network administrator must still guess which messages are potentially malicious and which messages are benign. With the introduction of this feature, a user can now configure a Cisco IOS firewall for stateful inspection to “trust” that the ICMP messages are generated within the private network and to permit the associated ICMP replies.



Note

Access lists can still be used to allow unsolicited error messages along with Cisco IOS firewall inspection. Access lists complement Cisco IOS firewall ICMP inspection.

Stateful inspection of ICMP packets is limited to the most common types of ICMP messages that are useful to network administrators who are trying to debug their networks. That is, ICMP messages that do not provide a valuable tool for the internal network administrator will not be allowed. For the Cisco IOS firewall-supported ICMP message request types, see [Table 29](#).

Table 29 *ICMP Packet Types Supported by CBAC*

ICMP Packet Type	Name	Description
0	Echo Reply	Reply to Echo Request (Type 8)
3	Destination Unreachable	Possible reply to any request
		Note This packet is included because it is a possible response to any ICMP packet request.

Table 29 *ICMP Packet Types Supported by CBAC*

ICMP Packet Type	Name	Description
8	Echo Request	Ping or traceroute request
11	Time Exceeded	Reply to any request if the time to live (TTL) packet is 0
13	Timestamp Request	Request
14	Timestamp Reply	Reply to Timestamp Request (type 13)

**Note**

ICMP packet types 0 and 8 are used for pinging: the source sends out an Echo Request packet, and the destination responds with an Echo Reply packet.

Packet types 0, 8, and 11 are used for ICMP traceroute: Echo Request packets are sent out starting with a TTL packet of 1, and the TTL is incremented for each hop. The intermediate hops respond to the Echo Request packet with a Time Exceeded packet; the final destination responds with an Echo Reply packet.

ICMP Inspection Checking

Return packets are checked by the inspect code, not by ACLs. The inspect code tracks each destination address from outgoing packets and checks each return packet. For ECHO REPLY and TIMESTAMP REPLY packets, the return address is checked. For UNREACHABLE and TIME EXCEEDED packets, the intended destination address is extracted from the packet data and checked.

For more information, see [Checking for ICMP Inspection Example, page 7](#).

How to Use Firewall Stateful Inspection of ICMP

This section contains the following procedures:

- [Configuring Firewall Stateful Inspection for ICMP, page 3](#)
- [Verifying Firewall and ICMP Session Information, page 4](#)
- [Monitoring Firewall and ICMP Session Information, page 5](#)

Configuring Firewall Stateful Inspection for ICMP

To enable the Cisco IOS Firewall to start inspection ICMP messages, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip inspect name *inspection-name* icmp [alert {on | off}] [audit-trail {on | off}] [timeout *seconds*]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip inspect name <i>inspection-name</i> icmp [alert {on off}] [audit-trail {on off}] [timeout <i>seconds</i>] Example: Router(config)# ip inspect name test icmp alert on audit-trail on timeout 30	Turns on inspection for ICMP. <ul style="list-style-type: none"> alert—Alert messages are generated. This function is on by default. audit-trail—Audit trail messages are generated. This function is off by default. timeout—Overrides the global channel inactivity timeout value. The default value of the <i>seconds</i> argument is 10.

Verifying Firewall and ICMP Session Information

To display active ICMP session and IP access list information, perform the following optional steps:

SUMMARY STEPS

1. **enable**
2. **show ip inspect session [detail]**
3. **show ip access-list**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show ip inspect session [detail] Example: Router# show ip inspect session	(Optional) Displays existing sessions that are currently being tracked and inspected by the Cisco IOS firewall. <ul style="list-style-type: none"> The optional detail keyword causes additional details about these sessions to be shown.
Step 3	show ip access-list Example: Router# show ip access-list	(Optional) Displays the contents of all current IP access lists. For a sample output example, see the section “ICMP Session Verification Example.”

Monitoring Firewall and ICMP Session Information

To monitor debugging messages related to ICMP inspection, perform the following optional steps:



Note

Effective with Cisco IOS Release 12.4(20)T, the **debug ip inspect** command is replaced by the **debug policy-firewall** command. See the *Cisco IOS Debug Command Reference* for more information.

SUMMARY STEPS

1. enable
2. debug ip inspect icmp

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	debug ip inspect icmp Example: Router# debug ip inspect icmp	(Optional) Displays the operations of the ICMP inspection engine for debugging purposes. For an example of sample output, see the command debug ip inspect in the Command Reference section.

Configuration Examples for Stateful Inspection of ICMP

This section provides the following configuration examples:

- [Firewall Stateful Inspection for ICMP Configuration Example, page 6](#)
- [Checking for ICMP Inspection Example, page 7](#)
- [ICMP Session Verification Example, page 7](#)

Firewall Stateful Inspection for ICMP Configuration Example

The default ICMP timeout is deliberately short (10 seconds) due to the security hole that is opened by allowing ICMP packets with a wild-carded source address back into the inside network. The timeout will occur 10 seconds after the last outgoing packet from the originating host. For example, if you send a set of 10 ping packets spaced 1 second apart, the timeout will expire in 20 seconds or 10 seconds after the last outgoing packet. However, the timeout is not extended for return packets. If a return packet is not seen within the timeout window, the hole will be closed and the return packet will not be allowed in. Although the default timeout can be made longer if desired, it is recommended that this value be kept relatively short.

The following example shows how to configure a firewall for stateful inspection of ICMP packets:

```
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname UUT
!
ip subnet-zero
no ip domain lookup
!
ip inspect audit-trail
ip inspect name test icmp alert on audit-trail on timeout 30
!
interface Ethernet0
ip address 192.168.10.2 255.255.255.0
ip inspect test in
!
interface Ethernet1
ip address 192.168.20.2 255.255.255.0
ip access-group 101 in
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.20.3
no ip http server
!
access-list 101 deny ip any any
!
line con 0
exec-timeout 0 0
!
end
```


Checking for ICMP Inspection Example

In the following example, three destinations were pinged. The example shows that the inspect code tracked each destination address in the inspect session information.

```
fw_1751#sh ip insp sess detail
Established Sessions
Session 813A1808 (192.168.156.5:0)=>(0.0.0.0:0) icmp SIS_OPEN
  Created 00:04:20, Last heard 00:00:00
  Destinations: 3
    Dest addr [192.168.131.3]
    Dest addr [192.168.131.7]
    Dest addr [192.168.131.31]
  Bytes sent (initiator:responder) [8456:5880] acl created 4
  Inbound access-list 102 applied to interface Ethernet0/0
  Inbound access-list 102 applied to interface Ethernet0/0
  Inbound access-list 102 applied to interface Ethernet0/0
  Inbound access-list 102 applied to interface Ethernet0/0
```

ICMP Session Verification Example

The following example is sample output from the **show ip access-list** command. In this example, Access Control Lists (ACLs) are created for an ICMP session on which only ping packets were issued from the host.

```
Router# show ip access-list 101

Extended IP access list 101
  permit icmp any host 192.168.133.3 time-exceeded
  permit icmp any host 192.168.133.3 unreachable
  permit icmp any host 192.168.133.3 timestamp-reply
  permit icmp any host 192.168.133.3 echo-reply (4 matches)
```

Additional References

For additional information related to Firewall Stateful Inspection of ICMP, refer to the following references:

- [Related Documents, page 8](#)
- [Standards, page 8](#)
- [MIBs, page 8](#)
- [RFCs, page 9](#)
- [Technical Assistance, page 9](#)

Related Documents

Related Topic	Document Title
CBAC information and configuration tasks	<i>The chapter “Configuring Context-based Access Control” in the <i>Cisco IOS Security Configuration Guide, Release 12.2</i></i>
Additional CBAC commands	<i>The chapter “Context-based Access Control Commands” in the <i>Cisco IOS Security Command Reference, Release 12.2</i></i>

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

RFCs ¹	Title
RFC 792	<i>Internet Control Message Protocol</i>
RFC 950	<i>Internet Standard Subnetting Procedure</i>
RFC 1700	Assigned Numbers

1. Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug ip inspect**
- **ip inspect name**

Glossary

ACL—access control list. An ACL is a list kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).

CBAC—Context-Based Access Control. CBAC is the name given to the Cisco IOS Firewall subsystem.

firewall—A firewall is a networking device that controls access to the network assets of your organization. Firewalls are positioned at the entrance points into your network. If your network has multiple entrance points, you must position a firewall at each point to provide effective network access control.

The most basic function of a firewall is to monitor and filter traffic. Firewalls can be simple or elaborate, depending on your network requirements. Simple firewalls are usually easier to configure and manage. However, you might require the flexibility of a more elaborate firewall.

ICMP—Internet Control Message Protocol. An ICMP is a network layer Internet protocol that reports errors and provides other information relevant to IP packet processing.

RPC—remote-procedure call. A RPC is the technological foundation of client or server computing. RPCs are procedure calls that are built or specified by clients and are executed on servers, with the results returned over the network to the clients.

RTSP—Real Time Streaming Protocol. RTSP enables the controlled delivery of real-time data, such as audio and video. Sources of data can include both live data feeds, such as live audio and video, and stored content, such as prerecorded events. RTSP is designed to work with established protocols, such as RTP and HTTP.

SIP—Session Initiation Protocol. SIP is a protocol developed by the IETF MUSIC Working Group as an alternative to H.323. SIP features are compliant with IETF RFC 2543, published in March 1999. SIP equips platforms to signal the setup of voice and multimedia calls over IP networks.

SMTP—simple mail transfer protocol. SMTP is an Internet protocol providing e-mail services.

UDP—User Datagram Protocol. A UDP is a connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

**Note**

Refer to the [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Firewall Support for SIP

The Firewall Support for SIP feature integrates Cisco IOS firewalls, Voice over IP (VoIP) protocol, and Session Initiation Protocol (SIP) within a Cisco IOS-based platform, enabling better network convergence.



Note

Some Cisco IOS versions earlier than 12.2(11)YU and 12.2(15)T may accept the configuration commands for SIP that are shown in this document; however, those earlier versions will not function properly.

Feature Specifications for Firewall Support for SIP

Feature History

Release	Modification
12.2(11)YU	This feature was introduced.
12.2(15)T	This feature was integrated into Cisco IOS Release 12.2(15)T.

Supported Platforms

For platforms supported in Cisco IOS Releases 12.2(11)YU and 12.2(15)T, consult Cisco Feature Navigator.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions for Firewall Support for SIP, page 2](#)
- [Information About Firewall Support for SIP, page 2](#)
- [How to Configure Your Firewall for SIP, page 8](#)
- [Configuration Examples for Firewall SIP Support, page 11](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Additional References, page 11](#)
- [Command Reference, page 13](#)

Restrictions for Firewall Support for SIP

DNS Name Resolution

Although SIP methods can have Domain Name System (DNS) names instead of raw IP addresses, this feature currently does not support DNS names.

SIP UDP Support Only

This feature supports only the SIP User Datagram Protocol (UDP) format for signaling; the TCP format is not supported.

SIP Abbreviated Header

This feature does not support the compact form of SIP header fields.

Earlier Versions of Cisco IOS

Some Cisco IOS versions earlier than 12.2(11)YU and 12.2(15)T may accept the configuration commands for SIP that are shown in this document; however, those earlier versions will not function properly.

Information About Firewall Support for SIP

To configure the Cisco IOS Firewall Support for SIP feature, you must understand the following concepts:

- [Firewall and SIP Overviews, page 2](#)
- [Firewall for SIP Functionality Description, page 5](#)
- [SIP Message Treatment by the Firewall, page 6](#)
- [Call Database, page 7](#)

Firewall and SIP Overviews

This section contains the following concepts:

- [Cisco IOS Firewall, page 2](#)
- [SIP \(Session Initiation Protocol\), page 3](#)

Cisco IOS Firewall

The Cisco IOS firewall extends the concept of static access control lists (ACLs) by introducing dynamic ACL entries that open on the basis of the necessary application ports on a specific application and close these ports at the end of the application session. The Cisco IOS firewall achieves this functionality by inspecting the application data, checking for conformance of the application protocol, extracting the

relevant port information to create the dynamic ACL entries, and closing these ports at the end of the session. The Cisco IOS firewall is designed to easily allow a new application inspection whenever support is needed.

SIP (Session Initiation Protocol)

SIP is an ASCII-based, application-layer control protocol that can be used to establish, maintain, and terminate calls between two or more endpoints. Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.

SIP Messages

SIP has two types of messages—requests and responses—that have the following generic structure:

```
generic-message = Request-Line | Status-Line
                  * ( general-header | request-header
                    | response-header | entity-header )
                  CRLF
                  [ message-body]
```



Note

Any of these message components may contain embedded IP addresses.

[Table 30](#) identifies the six available SIP request messages.

Table 30 *SIP Request Messages*

SIP Message	Purpose
ACK	Confirms receipt of a final response to INVITE
BYE	Is sent by either side to end the call
CANCEL	Is sent to end a call that has not yet been connected
INVITE	Is a request from a User Agent Client (UAC) to initiate a session
OPTIONS	Are sent to query capabilities of the user agents and network servers
REGISTER	Is sent by the client to register the address with a SIP proxy

[Table 31](#) identifies the available SIP response methods.

Table 31 *SIP Response Messages*

SIP Message	Purpose
1xx Informational	<ul style="list-style-type: none"> • 100 = Trying • 180 = Ringing • 181 = Call Is Being Forwarded • 182 = Queued • 183 = Session Progress
2xx Successful	<ul style="list-style-type: none"> • 200 = OK
3xx Redirection	<ul style="list-style-type: none"> • 300 = Multiple Choices • 301 = Moved Permanently • 302 = Moved Temporarily • 303 = See Other • 305 = Use Proxy • 380 = Alternative Service
4xx Request Failure	<ul style="list-style-type: none"> • 400 = Bad Request • 401 = Unauthorized • 402 = Payment Required • 403 = Forbidden • 404 = Not Found • 405 = Method Not Allowed • 406 = Not Acceptable • 407 = Proxy Authentication Required • 408 = Request Timeout • 409 = Conflict • 410 = Gone • 411 = Length Required • 413 = Request Entity Too Large • 414 = Request URI Too Large • 415 = Unsupported Media Type • 420 = Bad Extension • 480 = Temporarily Not Available • 481 = Call Leg/Transaction Does Not Exist
4xx Request Failure (continued)	<ul style="list-style-type: none"> • 482 = Loop Detected • 483 = Too Many Hops • 484 = Address Incomplete • 485 = Ambiguous • 486 = Busy Here

Table 31 **SIP Response Messages (continued)**

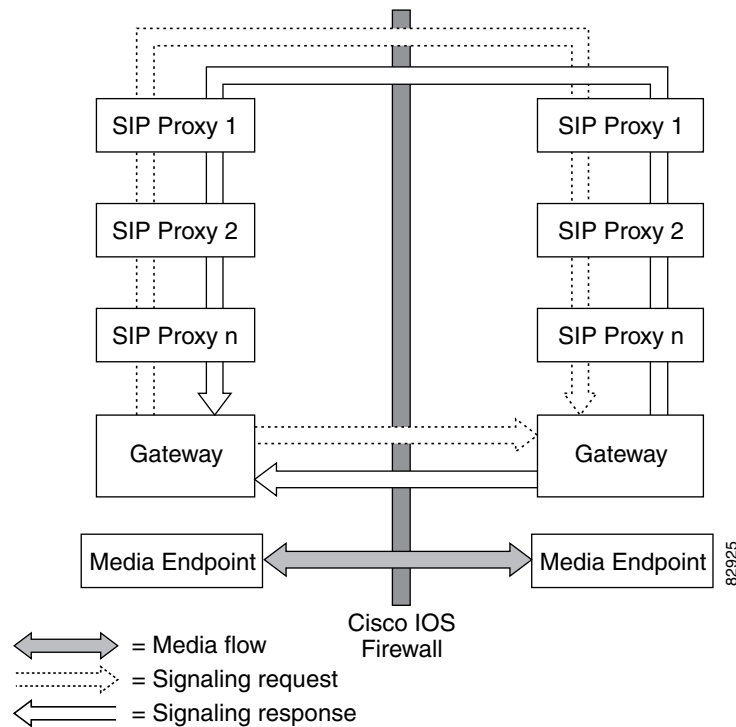
SIP Message	Purpose
5xx Server Failure	<ul style="list-style-type: none">• 500 = Internal Server Error• 501 = Not Implemented• 502 = Bad Gateway• 503 = Service Unavailable• 504 = Gateway Timeout• 505 = SIP Version Not Supported
6xx Global Failure	<ul style="list-style-type: none">• 600 = Busy Anywhere• 603 = Decline• 604 = Does Not Exist Anywhere• 606 = Not Acceptable

Firewall for SIP Functionality Description

The Firewall for SIP Support feature allows SIP signaling requests to traverse directly between gateways or through a series of proxies to the destination gateway or phone. After the initial request, if the Record-Route header field is not used, subsequent requests can traverse directly to the destination gateway address as specified in the Contact header field. Thus, the Cisco IOS firewall is aware of all surrounding proxies and gateways and allows the following functionality:

- SIP signaling responses can travel the same path as SIP signaling requests.
- Subsequent signaling requests can travel directly to the endpoint (destination gateway).
- Media endpoints can exchange data between each other.

See [Figure 28](#) for a sample topology that displays these functionalities.

Figure 28 Cisco IOS Firewall for SIP Awareness Sample Topology

SIP Message Treatment by the Firewall

See [Table 32](#) for information on the treatment of SIP methods by the Cisco IOS firewall.

Table 32 Treatment of SIP Methods by the Cisco IOS Firewall

SIP Message	Purpose
200 OK	Signifies the end of the call creation phase. The packet is checked for validity against the call database, and the contact information of the server is taken from it. Temporary call-flow-based openings in the firewall are created for allowing the BYE message, which can be initiated from the inside or outside.
200 OK for BYE	Signifies the graceful termination of the call and is in response to the BYE message. The same action as the CANCEL message is taken.
ACK	Signifies that the message is passed after checking for validity.
BYE	Signifies the intent to terminate the call. The database state is updated and temporary openings in the firewall are created for response to the BYE message.
CANCEL	Signifies abnormal data termination. The signaling sessions, media sessions, pregenerated temporary openings in the firewall, and the call database entry for the call are removed.

Table 32 *Treatment of SIP Methods by the Cisco IOS Firewall (continued)*

SIP Message	Purpose
INVITE	Occurs typically at the start of the call. The firewall will create a database entry upon receipt of this method and fill the database with relevant information extracted from this message. Temporary openings in the firewall will allow for a series of responses to the INVITE request. The temporary openings will be call-flow sensitive and will allow for responses for a fixed amount of time (t = 30 secs).
NO MATCH	Signifies a signaling message that is not present in the database.
Other Methods	Signifies that the message is passed if the call ID is present in the call database.
REGISTER	Results in the creation of an entry in the call database. Time-based, flow-control ACL firewall openings will allow for the response to the REGISTER and subsequent INVITE messages.
SESSION PROGRESS	Contains a response to the INVITE message, and it is a packet during the call creation phase. The packet is checked against the call database for validity of call ID and the media ports; the server proxy information is gathered from the packet. Media channels should be created in this phase.

Call Database

A call database, which contains the details of a call leg, is maintained for all call flows. A call database is created and maintained because there can be numerous signaling sessions for each call. [Table 33](#) identifies the information available in the call database.

Table 33 *Call Database Information*

Type	Purpose
call_int_over	Checks to see whether or not call initialization is over, and if so, checks to see if the call is in the teardown phase
C con ip & C con port	Signifies the IP address and port in the contact field of the initiator; for example, "Contact:<sip:1111@172.16.0.3:5060;user=phone>"
C media ip & C media port	Signifies the IP address in the media field of the initiator; for example, "c=IN IP4 172.16.0.3"
C media port	Signifies the port in the media field of the initiator; for example, "m=audio 20758 RTP/AVP 0"
C src ip & C src port	Signifies the actual IP address and port of the initiator
C via ip & C via port	Signifies the IP address and port in the via field of the initiator (the first via line); for example, "Via: SIP/2.0/UDP 172.16.0.3:5060"
current sip state	Is the current state of the call (which helps to avoid retransmission)
from/to/callid	Is extracted from the "INVITE" SIP request message to identify the call
media header	Keeps the list of media sessions for the call

Table 33 **Call Database Information (continued)**

Type	Purpose
media opened	Signifies multiple messages that may have media information, so you need to check to see whether or not the media has been opened for the call
prev sip state	Signifies the previous state of the call (which helps to avoid retransmission)
S con ip & S con port	Signifies the IP address and port in the contact field for the responder
S media ip	Signifies the IP address in the media field for the responder
S media port	Signifies the port in the media field for the responder
S src ip & S src port	Signifies the actual IP address and port of the responder
S via ip & S via port	Signifies the IP address and port in the via field for the responder
signal header	Keeps the list of signaling sessions for the call
sip_proxy_traversed	Makes the firewall topologically aware of whether the call has traversed through proxies

How to Configure Your Firewall for SIP

To configure a Cisco IOS Firewall for SIP support, perform the following tasks:

- [Configuring Firewall for SIP Support, page 8](#) (required)
- [Verifying Firewall for SIP Support, page 9](#) (optional)
- [Monitoring Firewall for SIP Support, page 10](#) (optional)

Configuring Firewall for SIP Support

To enable a firewall to support SIP, use the following commands.

Prerequisite

Before you configure Cisco IOS firewall support for SIP on your router, you first need to configure access lists, whose purpose normally is to block SIP traffic from unprotected networks for which the firewall will create temporary openings for specific traffic. For information about configuring access lists and the **access-list** command, see the chapter “[Configuring IPsec Network Security](#)” in the *Cisco IOS Security Configuration Guide*, Release 12.2, and the *Cisco IOS Command Reference*, Release 12.2 T, respectively.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip inspect name** *inspection-name* **sip** [**alert {on | off}**] [**audit-trail {on | off}**] [**timeout** *seconds*]
4. **interface** *type number*
5. **ip inspect** *inspection-name* **{in | out}**

6. Repeat Steps 3 through 5 (Optional)

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip inspect name inspection-name sip [alert {on off}] [audit-trail {on off}] [timeout seconds] Example: Router(config)# ip inspect name voip sip	Turns on inspection for SIP. <ul style="list-style-type: none"> alert—Alert messages are generated. This function is on by default. audit-trail—Audit trail messages are generated. This function is off by default. timeout—Overrides the global channel inactivity timeout value.
Step 4	interface type number Example: Router(config)# interface FastEthernet 0/0	Configures an interface type and enters interface configuration mode.
Step 5	ip inspect inspection-name {in out} Example: Router(config-if)# ip inspect voip in	Applies inspection configurations to an interface and for a particular traffic direction.
Step 6	If SIP calls are coming from other interfaces, repeat Steps 3 through 5 and apply SIP inspections for the calls that are coming from those interfaces.	Note The inspection of protocols other than SIP may not be desirable for traffic that comes from external networks, so it may be necessary to configure an additional inspection rule specifying only SIP.

Verifying Firewall for SIP Support

To verify Cisco IOS firewall session information, perform the following optional steps:

SUMMARY STEPS

1. **enable**
2. **show ip inspect name inspection-name**
3. **show ip inspect session [detail]**
4. **show ip access-list**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show ip inspect name <i>inspection-name</i> Example: Router# show ip inspect name voip	(Optional) Displays the configured inspection rule.
Step 3	show ip inspect session [detail] Example: Router# show ip inspect session	(Optional) Displays existing sessions that are currently being tracked and inspected by the Cisco IOS firewall. <ul style="list-style-type: none"> The optional detail keyword causes additional details about these sessions to be shown.
Step 4	show ip access-list Example: Router# show ip access-list	(Optional) Displays the contents of all current IP access lists.

Monitoring Firewall for SIP Support

To monitor firewall events, perform the following optional steps:



Note

Effective with Cisco IOS Release 12.4(20)T, the **debug ip inspect** command is replaced by the **debug policy-firewall** command. See the *Cisco IOS Debug Command Reference* for more information.

SUMMARY STEPS

- enable
- debug ip inspect sip

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	debug ip inspect sip Example: Router# debug ip inspect sip	(Optional) Displays the operations of the SIP inspection engine for debugging purposes.

Configuration Examples for Firewall SIP Support

This section provides the following configuration example:

- [Firewall and SIP Configuration Example, page 11](#)

Firewall and SIP Configuration Example

The following example shows how to allow outside initiated calls and internal calls. For outside initiated calls, an ACL needs to be punched to allow for the traffic from the initial signaling packet from outside. Subsequent signaling and media channels will be allowed by the inspection module.

```
ip inspect name voip sip
interface FastEthernet0/0
  ip inspect voip in
!
!
interface FastEthernet0/1
  ip inspect voip in
  ip access-group 100 in
!
!
access-list 100 permit udp host <gw ip> any eq 5060
access-list 100 permit udp host <proxy ip> any eq 5060
access-list deny ip any any
```

Additional References

For additional information related to Firewall Support for SIP, refer to the following references:

- [Related Documents, page 12](#)
- [Standards, page 12](#)
- [MIBs, page 12](#)
- [RFCs, page 13](#)
- [Technical Assistance, page 13](#)

Related Documents

Related Topic	Document Title
Cisco IOS firewall information and configuration tasks	The chapter “ Configuring Context-Based Access Control ” in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.2
Cisco IOS firewall commands	The chapter “ Context-Based Access Control Commands ” in the <i>Cisco IOS Security Command Reference</i> , Release 12.2
SIP information and configuration tasks	The chapter “ Configuring Session Initiation Protocol for Voice over IP ” in the <i>Cisco IOS Voice, Video, and Fax Configuration Guide</i> , Release 12.2 and
Additional SIP Information	Guide to Cisco Systems' VoIP Infrastructure Solution for SIP
Access lists and the access-list command	The chapter “ Configuring IPSec Network Security ” in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.2, and the Cisco IOS Command Reference , Release 12.2, respectively.

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

RFCs ¹	Title
RFC 2543	SIP: Session Initiation Protocol

1. Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug ip inspect**
- **ip inspect name**

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Firewall Websense URL Filtering

First Published: December 23, 2002

Last Updated: July 31, 2008

The Firewall Websense URL Filtering feature enables your Cisco IOS firewall (also known as Cisco Secure Integrated Software [CSIS]) to interact with the Websense URL filtering software, thereby allowing you to prevent users from accessing specified websites on the basis of some policy. The Cisco IOS firewall works with the Websense server to know whether a particular URL should be allowed or denied (blocked).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Firewall Websense URL Filtering” section on page 17](#).

Use Cisco Feature Navigator to find information about platform support and Cisco IOS, Catalyst OS, and Cisco IOS XE software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Restrictions for Firewall Websense URL Filtering, page 2](#)
- [Information About Firewall Websense URL Filtering, page 3](#)
- [How to Configure Websense URL Filtering, page 6](#)
- [Configuration Examples for the Firewall and Webserver, page 13](#)
- [Additional References, page 16](#)
- [Glossary, page 18](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007, 2008 Cisco Systems, Inc. All rights reserved.

Restrictions for Firewall Websense URL Filtering

Websense Server Requirement

To enable this feature, you must have *at least* one Websense server; however, two or more Websense servers are preferred. Although there is no limit to the number of Websense servers you may have, and you can configure as many servers as you wish, only one server will be active at any given time—the primary server. URL look-up requests will be sent only to the primary server.

URL Filtering Support Restriction

This feature supports only one active URL filtering scheme at a time. (Before enabling Websense URL filtering, you should always ensure that there is not another URL filtering scheme configured, such as N2H2.)

Username Restriction

This feature does not pass the username and group information to the Websense server. However, the Websense server can work for user-based policies because it has another mechanism for getting the username to correspond to an IP address.

Exclusive Domain List Restriction

This feature does not resolve the domains before it searches an exclusive domain list. When a questionable URL is presented to the filtering server, this feature searches only for the value that was specified in the command-line interface (CLI). That is, if an exclusive domain list was configured via the **ip urlfilter exclusive-domain deny 198.168.1.1** command, a user entering `http://198.168.1.1` into a browser will be denied access. However, a user who is trying to access this same domain and who enters `http://www.cisco.com`, will be allowed access because 198.168.1.1 was specified via the CLI, not `www.cisco.com`.

PISA URL Filtering Restrictions — Cisco IOS Release 12.2(18)ZYA

- Only one inspection rule is supported.
- Only HTTP filtering is supported. (HTTPS and FTP filtering are not supported.)
- HTTP over ports used by static Network Based Application Recognition (NBAR) protocols are not supported.
- Context-based Access Control (CBAC) is not supported.
- Only Layer 3 SVIs, Layer 3 routed ports, and Layer 3 subinterfaces are supported.
- The **clear ip urlfilter cache** and **show ip urlfilter cache** commands are not supported.
- Only the Websense URL filtering server is supported. (N2H2/SmartFilter/Trend Micro filtering servers are not supported.)
- Usernames are not passed on from PISA to Websense.

Information About Firewall Websense URL Filtering

To configure the Firewall Websense URL Filtering feature, you should understand the following concepts:

- [Benefits of Firewall Websense URL Filtering, page 3](#)
- [Feature Design of Firewall Websense URL Filtering, page 4](#)
- [Supported Websense Server Features on a Cisco IOS Firewall, page 5](#)

Benefits of Firewall Websense URL Filtering

The Cisco IOS Firewall Websense URL Filtering feature provides an Internet management application that allows you to control web traffic for a given host or user on the basis of a specified security policy. In addition, the following functions are available in this feature:

Primary and Secondary Servers

When users configure multiple Websense servers, the firewall will use only one server at a time—the primary server; all other servers are called secondary servers. When the primary server becomes unavailable for any reason, it becomes a secondary server and one of the secondary servers becomes the primary server.

A firewall marks a primary server as down when sending a request to or receiving a response from the server fails. When a primary server goes down, the system will go to the beginning of the configured servers list and try to activate the first server on the list. If the first server on the list is unavailable, it will try the second server on the list; the system will keep trying to activate a server until it is successful or until it reaches the end of the server list. If the system reaches the end of the server list, it will set a flag indicating that all of the servers are down, and it will enter allow mode.

When all the servers are down and the system is in allow mode, a periodic event that occurs for each minute will trace through the server list, trying to bring up a server by opening a TCP connection. If the TCP connection is successfully opened, the server is considered to be up, and the system will return to operational mode.

IP Cache Table

This function provides an IP cache table that contains the IP addresses of web servers whose underlying URLs can be accessed by all users and hosts.

The caching algorithm involves three parameters—the maximum number of IP addresses that can be cached, an idle time, and an absolute time. The algorithm also involves two timers—idle timer and absolute timer. The idle timer is a small periodic timer (1 minute) that checks to see whether the number of cached IP addresses in the cache table exceeds 80 percent of the maximum limit. If the cached IP addresses have exceeded 80 percent, it will start removing idle entries; if it has not exceeded 80 percent, it will quit and wait for the next cycle. The absolute timer is a large periodic timer (1 hour) that is used to remove all of the elapsed entries. (The age of an elapsed entry is greater than the absolute time.) An elapsed entry will also be removed during cache lookup.

The idle time value is fixed at 10 minutes. The absolute time value is taken from the Websense look-up response, which is often greater than 15 hours. The absolute value for cache entry made out of exclusive-domains is 12 hours. The maximum number of cache entries is configurable.

To configure cache table parameters, use the **ip urlfilter cache** command.

Packet Buffering

This function allows you to increase the maximum number of HTTP responses that a Cisco IOS firewall can hold. If the HTTP responses arrive prior to a Websense server reply, this buffering scheme allows your firewall to store a maximum of 200 HTTP responses. (After 200 responses have been reached, the firewall will drop further responses.) The responses will remain in the buffer until an allow or deny message is received from Websense: if the status indicates that the URL is allowed, the firewall will release the HTTP responses in the buffer to the browser of the end user; if the status indicates that the URL is blocked, the firewall will discard the HTTP responses in the buffer and close the connection to both ends. This function prevents numerous HTTP responses from overwhelming your system.

To configure the maximum number of HTTP responses for your firewall, use the **ip urlfilter max-resp-pak** command.

Exclusive Domains

This function provides a configurable list of domain names so that the Cisco IOS firewall does not have to send a lookup request to the Websense server for the HTTP traffic that is destined for one of the domains in the exclusive list. Thus, the Websense server does not have to deal with look-up requests for HTTP traffic that is destined for a host that has already been marked as “allowed.”

Flexibility when entering domain names is also provided; that is, the user can enter the complete domain name or a partial domain name. If the user adds a complete domain name, such as “www.cisco.com,” to the exclusive domain list, all HTTP traffic whose URLs are destined for this domain (such as www.cisco.com/news and www.cisco.com/index) will be excluded from the Websense URL filtering policies, and based on the configuration, the URLs will be permitted or blocked (denied).

If the user adds only a partial domain name to the exclusive domain list, such as “.cisco.com,” all URLs whose domain names end with this partial domain name (such as www.cisco.com/products and www.cisco.com/eng) will be excluded from the Websense URL filtering policies, and based on the configuration, the URLs will be permitted or blocked (denied).

To configure an exclusive domain list, use the **ip urlfilter exclusive-domain** command.

Allow Mode

The system will go into allow mode when connections to all the Websense servers are down. The system will return to normal mode when a connection to at least one web Websense server is up. Allow mode directs your system to forward or drop all packets on the basis of the configurable allow mode setting. By default, allow mode is off, so all HTTP requests are forbidden if all Websense servers are down.

To configure allow mode for your system, use the **ip urlfilter allowmode** command.

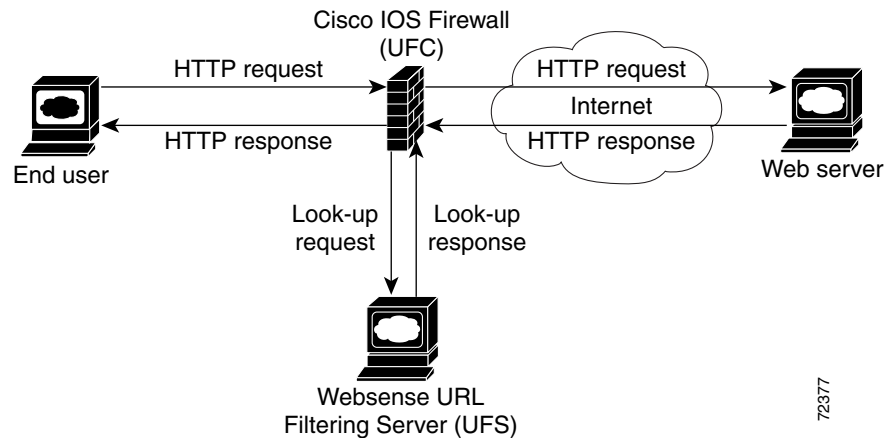
Feature Design of Firewall Websense URL Filtering



Note

This feature assumes that the Websense server will be part of a protected network and that requests from the Cisco IOS firewall will not travel over any unprotected network to reach the Websense server.

[Figure 29](#) and the corresponding steps explain a sample URL filtering network topology.

Figure 29 Firewall Websense URL Filtering Sample Topology

1. The end user browses a page on the web server, and the browser sends an HTTP request.
2. After the Cisco IOS firewall receives this request, it forwards the request to the web server while simultaneously extracting the URL and sending a look-up request to the Websense server.
3. After the Websense server receives the look-up request, it checks its database to see whether it should permit or deny the URL; it returns a permit or deny status via a look-up response to the Cisco IOS firewall.
4. After the Cisco IOS firewall receives this look-up response, it performs one of the following functions:
 - If the look-up response permits the URL, it sends the HTTP response to the end user.
 - If the look-up response denies the URL, the Websense server redirects the user to its own internal web server, which displays a message that describes the category under which the URL is blocked; thereafter, the connection is reset to both ends.

Supported Websense Server Features on a Cisco IOS Firewall

The Cisco IOS firewall supports all of the filtering and user authentication methods that are supported by the Websense server.

The following filtering methods are supported:

- Global filtering, which is applied to all users, groups, and IP addresses
- User- or group-based filtering, which is applied to a specific user or group
- Keyword-based filtering, which is applied on the basis of specific keywords (for example, a user can configure a policy for which all URLs with the keyword “dog” will be denied)
- Category-based filtering, which is applied on the basis of specific categories
- Customized filtering, which allows the user to apply a policy for customized URLs

The NT LAN Manager (NTLM) and Lightweight Directory Access Protocol (LDAP) user authentication methods are supported in this feature. Websense uses these methods to authenticate the user when the firewall does not pass the authenticated username along with the look-up request.

When the username is not passed along with the look-up request, the Websense server retrieves the username through one of the following methods:

- Manual authentication—Websense redirects the user to its own internal web server, which displays a challenge or response for the username and password. (This process is similar to when a user is blocked, but in this process, an authentication message is displayed instead of a blocked message.) Thereafter, Websense checks the NTLM or LDAP directory service to see if the username and password are a match. If there is a match, Websense associates the username with the source IP address and policies can be created for that username.
- Transparent ID (XID)—Websense has an agent that automatically associates users, when they log onto a Windows network, to their IP addresses. Unlike manual authentication, this method does not require an additional logon by the user. However, this method can be used only for Windows.

**Note**

Although Websense also supports user authentication via TACACS or RADIUS, this feature currently does not support these protocols for user authentication.

How to Configure Websense URL Filtering

To configure your Cisco IOS firewall to interact with at least one Websense server to provide URL filtering, configure the following procedures:

- [Configuring Firewall Websense URL Filtering, page 6](#) (required)
- [Verifying Cisco IOS Firewall and Websense URL Filtering, page 11](#) (optional)
- [Maintaining the Cache Table, page 12](#) (optional)
- [Monitoring the URL Filter Subsystems, page 13](#) (optional)

Configuring Firewall Websense URL Filtering

Websense is a third-party filtering software that can filter HTTP requests on the basis of the following policies: destination hostname, destination IP address, keywords, and username. The software maintains a URL database of more than 20 million sites organized into more than 60 categories and subcategories.

Prerequisites

Before enabling Websense URL filtering, you should always ensure that there is not another URL filtering scheme configured, such as N2H2. If you try to enter a new filtering scheme when one already exists, the new scheme will be ignored, and the system will display an error message that says, “different URL filtering scheme cannot co-exist.”

Restrictions

Enabling HTTP inspection (via the **ip inspect name** command) triggers the Java applet scanner, which is CPU intensive. The only way to stop the Java applet scanner is to specify the **java-list access-list** keyword and argument and configure a standard access list to allow any traffic. Configuring URL filtering without enabling the **java-list access-list** keyword and argument will severely impact performance.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip inspect name** *inspection-name* **http** [**java-list** *access-list*] [**urlfilter**] [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*]
4. **ip inspect** *inspection-name* {**in** | **out**}
5. **ip urlfilter server vendor** {**websense** | **n2h2**} *ip-address* [**port** *port-number*] [**timeout** *seconds*] [**retransmit** *number*]
6. **ip urlfilter alert**
7. **ip urlfilter audit-trail**
8. **ip urlfilter urlf-server-log**
9. **ip urlfilter exclusive-domain** {**permit** | **deny**} *domain-name*
10. **ip urlfilter cache** *number*
11. **ip urlfilter allowmode** [**on** | **off**]
12. **ip urlfilter max-resp-pak** *number*
13. **ip urlfilter max-request** *number*
14. **ip urlfilter truncate** {**script-parameters** | **hostname**}
15. **ip urlfilter mode** {**per-session** | **per-uri** | **per-uri-proxy-only**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
	Example: Router> enable	
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	

	Command or Action	Purpose
Step 3	<p>ip inspect name inspection-name http [java-list access-list] [urlfilter] [alert {on off}] [audit-trail {on off}] [timeout seconds]</p> <p>Example: Router(config)# ip inspect name fw_urlf http java-list 51 urlfilter timeout 30</p>	<p>Turns on HTTP inspection. The urlfilter keyword associates URL filtering with HTTP inspection.</p> <p>Note You may configure two or more inspections in a router, but URL filtering will work only with the inspections in which the urlfilter keyword is enabled.</p> <p>Note Enabling HTTP inspection with or without any options triggers the Java applet scanner, which is CPU intensive. The only way to stop the Java applet scanner is to specify the java-list access-list keyword and argument. Configuring URL filtering without enabling the java-list access-list keyword and argument will severely impact performance.</p>
Step 4	<p>ip inspect inspection-name {in out}</p> <p>Example: Router(config)# ip inspect fw_urlf in</p>	<p>Applies a set of inspection rules to an interface.</p> <ul style="list-style-type: none"> The in keyword applies the inspection rules to inbound traffic.
Step 5	<p>ip urlfilter server vendor {websense n2h2} ip-address [port port-number] [timeout seconds] [retransmit number]</p> <p>Example: Router(config)# ip urlfilter server vendor websense 10.201.6.202</p>	<p>Configures a Websense server to interact with the firewall to filter HTTP requests on the basis of a specified policy.</p> <ul style="list-style-type: none"> ip-address—IP address of the vendor server. port port-number—Port number that the vendor server listens on. The default port number is 15868. timeout seconds—Length of time that the firewall will wait for a response from the vendor server. The default timeout is 5 minutes. retransmit number—Number of times the firewall will retransmit the request when a response does not arrive. The default value is 2 times.
Step 6	<p>ip urlfilter alert</p> <p>Example: Router(config)# ip urlfilter alert</p>	<p>(Optional) Enables the system alert, which displays system messages such as a server entering allow mode or going down.</p> <ul style="list-style-type: none"> The system alert is enabled by default.
Step 7	<p>ip urlfilter audit-trail</p> <p>Example: Router(config)# ip urlfilter audit-trail</p>	<p>(Optional) Enables the logging of messages into the syslog server of router. This function is disabled by default.</p>
Step 8	<p>ip urlfilter urlf-server-log</p> <p>Example: Router(config)# ip urlfilter urlf-server-log</p>	<p>(Optional) Enables the logging of system messages on the URL filtering server (the Websense server).</p> <ul style="list-style-type: none"> This function is disabled by default.

	Command or Action	Purpose
Step 9	<p>ip urlfilter exclusive-domain {permit deny} <i>domain-name</i></p> <p>Example: Router(config)# ip urlfilter exclusive-domain permit www.cisco.com</p>	<p>(Optional) Adds a domain name to or from the exclusive domain list so that the firewall does not have to send look-up requests to the Websense server.</p> <ul style="list-style-type: none"> • permit—Permits all traffic destined for the specified domain name. • deny—Denies all traffic destined for the specified domain name. • <i>domain-name</i>—Domain name that is added or removed from the exclusive domain list.
Step 10	<p>ip urlfilter cache <i>number</i></p> <p>Example: Router(config)# ip urlfilter cache 4500</p>	<p>(Optional) Configures cache table parameters.</p> <ul style="list-style-type: none"> • <i>number</i>—Maximum number of destination IP addresses that can be cached into the cache table; the default is 5000.
Step 11	<p>ip urlfilter allowmode [on off]</p> <p>Example: Router(config)# ip urlfilter allowmode on</p>	<p>(Optional) Turns on the default mode of the filtering systems.</p> <ul style="list-style-type: none"> • on—Allows HTTP requests to pass to the end user if all Websense servers are down. • off—Blocks all HTTP requests if all Websense servers are down; off is the default setting.
Step 12	<p>ip urlfilter max-resp-pak <i>number</i></p> <p>Example: Router(config)# ip urlfilter max-resp-pak 150</p>	<p>(Optional) Configures the maximum number of HTTP responses that the firewall can keep in its packet buffer. The default value is 200 512-byte buffers.</p>
Step 13	<p>ip urlfilter max-request <i>number</i></p> <p>Example: Router(config)# ip urlfilter maxrequest 500</p>	<p>(Optional) Sets the maximum number of outstanding requests that can exist at any given time. If the maximum number of requests is reached, all subsequent URLs are dropped.</p> <ul style="list-style-type: none"> • The default value is 1000.

	Command or Action	Purpose
Step 14	ip urlfilter truncate {script-parameters hostname} Example: Router(config)# ip urlfilter truncate hostname	(Optional) Allows the URL filter to truncate long URLs to the server.
Step 15	ip urlfilter mode {per-session per-uri per-uri-proxy-only} Example: Router(config)# ip urlfilter mode per-uri	(Optional) Configures a URL filtering mode. <ul style="list-style-type: none"> • per-session—Filters the first URL in the HTTP session. • per-uri—Filters the first URL in each packet. • per-uri-proxy-only—Filters via the per-session keyword behavior for direct (non-proxy) requests. Filters via the per-uri keyword behavior for proxy requests. <p>Note This command is available only on the Catalyst 6500 with PISA in Cisco IOS Release 12.2(18)ZYA.</p>

Troubleshooting Tips

This feature introduces the following alert messages:

- “%URLF-3-SERVER_DOWN: Connection to the URL filter server 10.92.0.9 is down”

This level three LOG_ERR-type message is displayed when a configured UFS goes down. When this happens, the firewall will mark the configured server as secondary and try to bring up one of the other secondary servers and mark that server as the primary server. If there is no other server configured, the firewall will enter allow mode and display the “URLF-3-ALLOW_MODE” message.

- %URLF-3-ALLOW_MODE: Connection to all URL filter servers are down and ALLOW MODE is OFF

This LOG_ERR type message is displayed when all UFSs are down and the system enters allow mode.



Note Whenever the system goes into allow mode (all filter servers are down), a periodic keepalive timer will be triggered that will try to bring up a server by opening a TCP connection.

- “%URLF-5-SERVER_UP: Connection to an URL filter server 10.92.0.9 is made; the system is returning from ALLOW MODE”

This LOG_NOTICE-type message is displayed when the UFSs are detected as being up and the system is returning from allow mode.

- “%URLF-4-URL_TOO_LONG:URL too long (more than 3072 bytes), possibly a fake packet?”

This LOG_WARNING-type message is displayed when the URL in a look-up request is too long; any URL longer than 3K will be dropped.

- “%URLF-4-MAX_REQ: The number of pending request exceeds the maximum limit <1000>”

This LOG_WARNING-type message is displayed when the number of pending requests in the system exceeds the maximum limit and all further requests are dropped.

To display these alert messages, use the **ip urlfilter alert** command.

This feature introduces the following syslog messages:

- “%URLF-6-SITE_ALLOWED: Client 10.0.0.2:12543 accessed server 10.76.82.21:8080”

This message is logged for each request whose destination IP address is found in the cache. It includes the source IP address, source port number, destination IP address, and destination port number. The URL is not logged because the IP address of the request is found in the cache, so parsing the request and extracting the URL is a waste of time.

- “%URLF-4-SITE-BLOCKED: Access denied for the site ‘www.sports.com’; client 10.54.192.6:34557 server 172.24.50.12:80”

This message is logged when a request finds a match against one of the blocked domains in the exclusive-domain list or the corresponding entry in the IP cache.

- “%URLF-6-URL_ALLOWED: Access allowed for URL http://www.websense.com/; client 10.54.192.6:54123 server 192.168.0.1:80”

This message is logged for each URL request that is allowed by a UFS. It includes the allowed URL, source IP address, source port number, destination IP address, and destination port number. Longer URLs will be truncated to 300 bytes and then logged.

- “%URLF-6-URL_BLOCKED: Access denied URL http://www.google.com; client 12.54.192.6:54678 server 64.192.14.2:80”

This message is logged for each URL request that is blocked by a UFS. It includes the blocked URL, source IP address, source port number, destination IP address, and destination port number. Longer URLs will be truncated to 300 bytes and then logged.

To display these syslog messages, use the **ip urlfilter audit-trail** command.

Verifying Cisco IOS Firewall and Websense URL Filtering

To verify that the Firewall Websense URL Filtering feature is working, perform any of the following optional steps:

SUMMARY STEPS

1. **enable**
2. **show ip urlfilter cache**
3. **show ip urlfilter config**
4. **show ip urlfilter statistics**

DETAILED STEPS

Command or Action	Purpose
enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
show ip urlfilter cache Example: Router# show ip urlfilter cache	Displays the destination IP addresses that are cached into the cache table. Note This command is not supported on PISA in Cisco IOS Release 12.2(18)ZYA.
show ip urlfilter config Example: Router# show ip urlfilter config	Displays the size of the cache, the maximum number of outstanding requests, the allow mode state, and the list of configured Websense servers.
show ip urlfilter statistics Example: Router# show ip urlfilter statistics	Displays information such as the number of requests that are sent to the Websense server, the number of responses received from the Websense server, the number of pending requests in the system, the number of failed requests, the number of blocked URLs.

Maintaining the Cache Table

To clear the cache table of a specified address or of all IP addresses, perform the following optional steps.

SUMMARY STEPS

1. enable
2. clear ip urlfilter cache

DETAILED STEPS

Command or Action	Purpose
enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
clear ip urlfilter cache {ip-address all} Example: Router# clear ip urlfilter cache all	Clears the cache table. Note This command is not supported on PISA in Cisco IOS Release 12.2(18)ZYA.

Monitoring the URL Filter Subsystems

To monitor the URL filter subsystems, perform the following optional steps:

SUMMARY STEPS

1. **enable**
2. **debug ip urlfilter {func-trace | detailed | events}**

DETAILED STEPS

Command or Action	Purpose
enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
debug ip urlfilter {func-trace detailed events} Example: Router# debug ip urlfilter detailed	Enables debugging information of the URL filter subsystems. <ul style="list-style-type: none"> • func-trace—Prints a sequence of important functions that are called when configuring URL filtering. • detailed—Prints detailed information about various activities that occur during URL filtering. • events—Prints various events, such as queue event, timer event, and socket event.

Configuration Examples for the Firewall and Webserver

This section provides the following comprehensive configuration example:

- [URL Filter Client \(Firewall\) Configuration Example, page 13](#)

URL Filter Client (Firewall) Configuration Example

The following example shows how to configure the Cisco IOS firewall (also known as the URL filter client [UFC]) for Websense URL filtering:

```
hostname fw9-7200b
!
logging buffered 64000 debugging
enable secret 5 $1$qMOF$umPb75mb3sV27JpNbW//7.
!
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
ip cef
no ip domain lookup
!
ip inspect name test http urlfilter
ip urlfilter cache 5
ip urlfilter exclusive-domain permit .cat.com
```

```

ip urlfilter exclusive-domain deny .dog.com
ip urlfilter exclusive-domain permit www.store.com
ip urlfilter audit-trail
ip urlfilter alert
ip urlfilter server vendor websense 192.168.3.1
ip audit notify log
ip audit po max-events 100
ip port-map http port 8080
!
no voice hpi capture buffer
no voice hpi capture destination
!
mta receive maximum-recipients 0
!
interface FastEthernet0/0
 ip address 192.168.3.254 255.255.255.0
 ip access-group 101 out
 ip nat inside
 ip inspect test in
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet1/0
 ip address 10.6.9.7 255.255.0.0
 ip nat outside
 no ip route-cache
 no ip mroute-cache
 duplex half
!
interface Ethernet1/1
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
!
interface Ethernet1/2
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
!
interface Ethernet1/3
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
!
interface Serial2/0
 no ip address
 no ip mroute-cache
 shutdown
 dsu bandwidth 44210
 framing c-bit
 cablelength 10
 serial restart_delay 0
 fair-queue
!
ip nat pool devtest 10.6.243.21 10.6.243.220 netmask 255.255.0.0
ip nat inside source list 1 pool devtest
ip nat inside source static 192.168.3.1 10.6.243.1
ip nat inside source static 192.168.3.2 10.6.243.2
ip nat inside source static 192.168.3.3 10.6.243.3
ip classless
ip route 192.168.0.30 255.255.255.255 10.6.0.1

```

```
no ip http server
no ip http secure-server
!
ip pim bidir-enable
!
!
access-list 101 deny    tcp any any
access-list 101 deny    udp any any
access-list 101 permit  ip any any
access-list 102 deny    tcp any any
access-list 102 deny    udp any any
access-list 102 permit  ip any any
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!!
!
gatekeeper
shutdown
!
!
line con 0
  exec-timeout 0 0
  stopbits 1
line aux 0
  stopbits 1
line vty 0 4
  password letmein
  login
!
exception core-file sisu-devtest/coredump/fw9-7200b.core
exception dump 192.168.0.1
no scheduler max-task-time
!
end
```

Additional References

The following sections provide references related to the Firewall Websense URL Filtering feature

Related Documents

Related Topic	Document Title
N2H2 URL filtering	The chapter Firewall N2H2 Support , in the <i>Cisco IOS Security Configuration Guide</i>
Additional firewall commands	Cisco IOS Security Command Reference

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs ¹	Title
RFC 1945	Hypertext Transfer Protocol — HTTP/1.0
RFC 2616	Hypertext Transfer Protocol — HTTP/1.1

1. Not all supported RFCs are listed.

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Feature Information for Firewall Websense URL Filtering

[Table 34](#) lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

[Table 34](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 34 **Feature Information for Firewall Websense URL Filtering**

Feature Name	Releases	Feature Information
Firewall Websense URL Filtering	12.2(11)YU 12.2(15)T 12.2(18)ZYA	<p>This feature enables your Cisco IOS firewall to interact with the Websense URL filtering software, thereby allowing you to prevent users from accessing specified websites on the basis of some policy.</p> <p>In 12.2(18)ZYA, support was added on the Catalyst 6500 series of switches equipped with the PISA.</p> <p>The following commands were introduced or modified: clear ip urlfilter cache, debug ip urlfilter, ip inspect name, ip urlfilter alert, ip urlfilter allowmode, ip urlfilter audit-trail, ip urlfilter cache, ip urlfilter exclusive-domain, ip urlfilter max-request, ip urlfilter max-resp-pak, ip urlfilter server vendor, ip urlfilter urlf-server-log, show ip urlfilter cache, show ip urlfilter config, show ip urlfilter statistics.</p> <p>In Cisco IOS Release 12.2(18)ZYA, the following command was introduced: ip urlfilter mode</p>

Glossary

CSIS—Cisco Secure Integrated Software. CSIS is a content-based firewall that currently inspects application data, checks for protocol conformance, extracts the relevant port information to create dynamic access list entries that successfully allow return traffic, and closes the ports at the end of the session.

UFC—URL filter client. UFC is a separate process that accepts URLs from CSIS, forwards the URL to the Websense server, and processes the replies from the vendor server (Websense or N2H2).

UFS—URL filter server. UFS is a generic name given to the vendor server (Websense or N2H2), which processes URLs and decides whether to allow or deny web traffic on the basis of a given policy.



Note

Refer to the [Internetworking Terms and Acronyms](#) for terms not included in this glossary..

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007, 2008 Cisco Systems, Inc. All rights reserved.



Firewall Support of Skinny Client Control Protocol (SCCP)

The Firewall Support of Skinny Client Control Protocol (SCCP) feature enables Context-Based Access Control (CBAC) inspection to support the Voice over IP (VoIP) protocol, Skinny Client Control Protocol (SCCP). That is, CBAC inspects Skinny control packets that are exchanged between a Skinny client and the Call Manager (CM); CBAC then configures the router (also known as the Cisco IOS Firewall) to enable the Skinny data channels to traverse through the router.

Feature Specifications for the Firewall Support of Skinny Client Control Protocol (SCCP) Feature

Feature History

Release	Modification
12.3(1)	This feature was introduced.

Supported Platforms

For platforms supported in Cisco IOS Release 12.3(1), consult Cisco Feature Navigator.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Firewall Support of Skinny Client Control Protocol \(SCCP\), page 2](#)
- [Restrictions for Firewall Support of Skinny Client Control Protocol \(SCCP\), page 2](#)
- [Information About Firewall Support of Skinny Client Control Protocol \(SCCP\), page 2](#)
- [How to Configure Your Firewall for Skinny Support, page 4](#)
- [Configuration Examples for Firewall Skinny Support, page 8](#)
- [Additional References, page 10](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Command Reference, page 11](#)

Prerequisites for Firewall Support of Skinny Client Control Protocol (SCCP)

The Skinny inspection module is part of the inspection subsystem; thus, your router must be running an image that has firewall support.

Restrictions for Firewall Support of Skinny Client Control Protocol (SCCP)

This feature has the following restrictions:

- Skinny inspection will inspect only the SCCP sessions that have been established after the firewall is configured with Skinny inspection. That is, any SCCP sessions that were established through the firewall before the Skinny inspection was configured will not be inspected.
- This feature does not support Music on Hold (MOH) when a device other than the CM is the music server. (This feature does support MOH when the CM is the music server.)
- This feature does not address either the multicast functionality of SCCP or the functionality of multiple active calls on a single Skinny client.

This feature does not support the following Skinny and firewall configurations:

- The firewall and CM cannot be in the same router. Skinny inspection does not support this configuration because the current firewall implementation does not inspect sessions that start or terminate at the router. Thus, Skinny inspection will work only with an external CM.
- The CM and the Skinny client cannot be on three different networks that are separated at the firewall. The current firewall implementation does not inspect sessions that have devices residing on more than two distinct networks that are segregated at the firewall. That is, if there are more than two interfaces at the firewall, session inspection is not supported.

Information About Firewall Support of Skinny Client Control Protocol (SCCP)

To configure the Firewall Support of SCCP feature, you must understand the following concepts:

- [Context-Based Access Control Overview, page 3](#)
- [Skinny Overview, page 3](#)
- [CBAC and Skinny Functionality Overview, page 3](#)

Context-Based Access Control Overview

CBAC extends the concept of static access control lists (ACLs) by introducing dynamic ACL entries that open the necessary application ports on the basis of a specific application and close these ports at the end of the application session. CBAC achieves this functionality by inspecting the application data, checking for conformance of the application protocol, extracting the relevant port information to create the dynamic ACL entries, and closing these ports at the end of the session. CBAC is designed to easily allow a new application inspection whenever support is needed.

Skinny Overview

Skinny enables voice communication between two Skinny clients through the use of a CM. Typically, the CM provides service to the Skinny clients on TCP Port 2000. Initially, a Skinny client connects to the CM by establishing a TCP connection; the client will also establish a TCP connection with a secondary CM, if available. After the TCP connection is established, the client will register with the primary CM, which will be used as the controlling CM until it reboots or there is a keepalive failure. Thus, the Skinny TCP connection between the client and the CM exists forever and is used to establish calls coming to or from the client. If a TCP connection failure is detected, the secondary CM is used. All data channels established with the previous CM remain active and will be closed after the end parties hang up the call.

[Table 1](#) lists the set of messages that are necessary for the data sessions to open and close. Skinny inspection will examine the data sessions that are deemed for opening and closing the access list pin holes.

Table 1 *Skinny Data Session Messages*

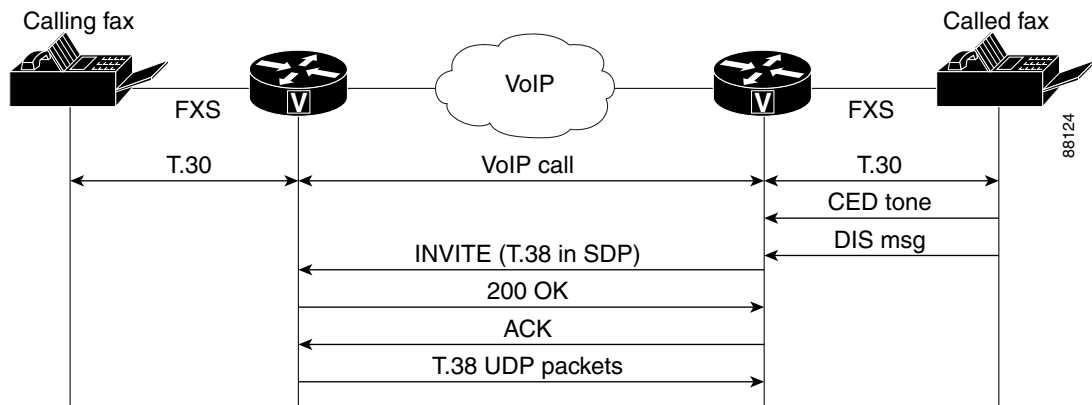
Skinny Inspection Message	Description
StationOpenReceiveChannelAckMessage	Contains the IP address and port information of the Skinny client sending this message. This message also contains the status of whether or not the client is willing to receive the voice traffic.
StationStartMediaTransmissionMessage	Contains the IP address and port information of the remote Skinny client.
StationCloseReceiveChannelMessage	CM instructs the Skinny client (on the basis of the information in this message) to close the receiving channel.
StationStopMediaTransmissionMessage	CM instructs the Skinny client (on the basis of the information in this message) to stop transmitting voice traffic.
StationStopSessionTransmissionMessage	CM instructs the Skinny client (on the basis of the information in this message) to end an indicated session.

CBAC and Skinny Functionality Overview

[Figure 1](#) depicts typical deployment solutions that are supported by CBAC inspection for Skinny. According to [Figure 1](#), a firewall with Skinny inspection can be configured on Cisco IOS Router A, Cisco IOS Router B, or both routers, thereby addressing the following three scenarios:

- A Cisco IOS router with a firewall on the customer premises equipment (CPE) side, supporting Skinny VoIP phone
- A Cisco IOS router with a firewall on the CM side
- A Cisco IOS router with a firewall at both ends of the connection

Figure 1 *CBAC Inspection for Skinny Sample Topology*



How to Configure Your Firewall for Skinny Support

To configure a Cisco IOS Firewall for SCCP support, perform the following tasks:

- [Configuring Basic Skinny CBAC Inspection, page 4](#)
- [Setting Skinny CBAC Session Timeouts, page 6](#)
- [Configuring Port to Application Mapping, page 6](#)
- [Verifying Cisco IOS Firewall for Skinny Support, page 7](#)
- [Monitoring Cisco IOS Firewall for Skinny Support, page 8](#)

Configuring Basic Skinny CBAC Inspection

Perform the following required steps to configure a basic Skinny CBAC configuration:

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **ip inspect name** *inspection-name protocol* [**alert** {on | off}] [**audit-trail** {on | off}] [**timeout** *seconds*]
4. **ip inspect name** *inspection-name protocol* [**alert** {on | off}] [**audit-trail** {on | off}] [**timeout** *seconds*] (Optional. Required if the TFTP server is outside the firewall.)
5. **interface** *type number*
6. **ip access-group** {*access-list-number*} {in | out}
7. **ip inspect** *inspection-name* {in | out}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip inspect name <i>inspection-name protocol</i> [alert {on off}] [audit-trail {on off}] [timeout <i>seconds</i>] Example: Router(config)# ip inspect name firewall skinny	Enables CBAC Skinny inspections.
Step 4	ip inspect name <i>inspection-name protocol</i> [alert {on off}] [audit-trail {on off}] [timeout <i>seconds</i>] Example: Router(config)# ip inspect name firewall tftp	(Optional. Required if the TFTP server is outside the firewall.) Defines a set of inspection rules.
Step 5	interface <i>type number</i> Example: Router(config)# interface FastEthernet 0/0	Configures an interface type and enters interface configuration mode.
Step 6	ip access-group { <i>access-list-number</i> } {in out} Example: Router(config-if)# ip access-group 100 in	Control access to an interface. Number of the access list that is blocking incoming traffic.
Step 7	ip inspect <i>inspection-name</i> {in out} Example: Router(config-if)# ip inspect firewall out	Applies a set of inspection rules to an interface.

Setting Skinny CBAC Session Timeouts

Session timeouts are triggered when traffic is not seen on a particular session for a configured amount of time. (This value is configured via the **ip inspect name** command.) After the inactivity timeout is triggered, the firewall will clean up the session and deallocate all of the session data.

You must set the inactivity timeout value for Skinny to a greater value than the keepalive timeout value that is configured between the CM and Skinny clients. Otherwise, the Skinny connection may become inaccessible for inspection because the firewall might delete the session-related information due to inactivity.

After the inactivity timeout is triggered, the inspection module will send reset (RST packets) to both ends of the connection. Any data channels that are associated with the control channel will not be closed. After both end parties hang up, there will not be any traffic on the data channels and the connection will eventually timeout.



Note

If the inactivity timeout of the control channel that is connected to the primary CM is less than the keepalive timeout that is sent by the CM to the Skinny client, the firewall will set the inactivity timeout to three times the keepalive timeout. If a timeout is not configured, the default value of 3600 seconds will be used.

Configuring Port to Application Mapping

By default, the Skinny inspection will inspect SCCP messages to or from the CM on TCP port 2000. If you prefer to configure the CM to use a different port, the port to application mapping (PAM) feature should be used to specify the desired port to the Cisco IOS firewall. Thus, the firewall will inspect the SCCP messages in the desired port and in port 2000. To configure the CM to use a different port via PAM, use the **ip port-map** command.

Prerequisites

Before you can configure PAM, you must first configure the steps in the section, “[Configuring Basic Skinny CBAC Inspection](#).”

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip port map** *appl_name* **port** *port_num* [**list** *acl_num*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip port map <i>appl_name</i> port <i>port_num</i> [list <i>acl_num</i>] Example: Router(config)# ip port map skinny port 2100	(Optional) Creates a port to address mapping for SCCP. This command allows you to indicate additional ports that need to be monitored for SCCP.

Verifying Cisco IOS Firewall for Skinny Support

To display active Skinny session information, perform the following optional steps:

SUMMARY STEPS

1. **enable**
2. **show ip inspect** {**name** *inspection-name* | **config** | **interfaces** | **session** [**detail**] | **all**}
3. **show ip access-list**
4. **show ip port-map** [*appl_name* | **port** *port_num*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show ip inspect { name <i>inspection-name</i> config interfaces session [detail] all } Example: Router# show ip inspect session detail	(Optional) Displays existing sessions that are currently being tracked and inspected by CBAC. The optional detail keyword causes additional details about these sessions to be shown.

	Command or Action	Purpose
Step 3	show ip access-list Example: Router# show ip access-list	(Optional) Displays the contents of all current IP access lists, which includes the dynamic access lists created by Skinny inspection.
Step 4	show ip port-map [appl_name port port_num] Example: Router# show ip port-map skinny	(Optional) Displays information about the active port to application mappings on the router. Use this command to view Skinny port map information. <ul style="list-style-type: none"> <i>appl_name</i>—Displays Skinny-specific PAM information. (You must specify the <i>skinny</i> argument.)

Monitoring Cisco IOS Firewall for Skinny Support



Note

Effective with Cisco IOS Release 12.4(20)T, the **debug ip inspect** command is replaced by the **debug policy-firewall** command. See the *Cisco IOS Debug Command Reference* for more information.

To monitor debugging messages related to Skinny inspection, perform the following optional steps:

SUMMARY STEPS

1. **enable**
2. **debug ip inspect {sccp | detailed}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	debug ip inspect {sccp detailed} Example: Router# debug ip inspect sccp	(Optional) Displays and logs the debugging messages related to SCCP inspection.

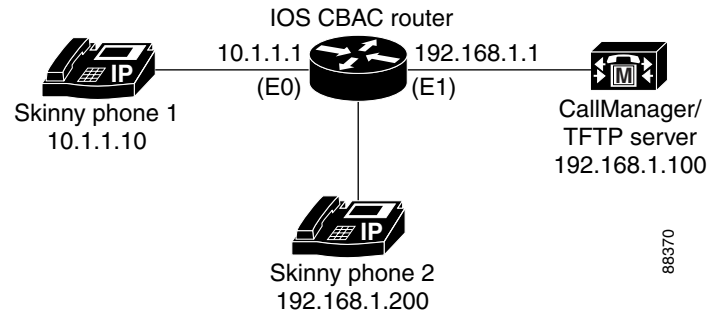
Configuration Examples for Firewall Skinny Support

This section provides the following configuration example:

- [Firewall and Skinny Configuration Example, page 9](#)

Firewall and Skinny Configuration Example

Figure 2 *Skippy and CBAC Configuration*



The following is an example of how to configure a Cisco IOS firewall for Skinny support and includes PAM (see [Figure 2](#)):

```
! Define the name of the router as "CBAC-Firewall."
!
host CBAC-Firewall
!
! Create a DHCP server process to offer out 10.1.1.x addresses on the
! inside network. Option 150 is used by Cisco IP phones as where to
! look for their configuration file. A default router is required so that all
! the IP phones can talk to networks other than just to the local 10.1.1.x.
!
ip dhcp pool localnetwork
  network 10.1.1.0 255.255.255.0
  option 150 ip 192.168.1.100
  default-router 10.1.1.1
!
! Prevent the DHCP server process from assigning 10.1.1.1 -.9 as an IP
! address on the local network. This is done to hold the addresses .2 - .9 as static-
! defined addresses.
!
ip dhcp excluded-address 10.1.1.1 10.1.1.9
!
! Define firewall rules to all Skinny traffic in/out along with TFTP
! services.
!
ip inspect name fwout tftp
ip inspect name fwout skinny
!
! Prevent any traffic from coming in.
!
access-list 100 deny ip any any
!
interface ethernet 1
  ip access-group 100 in
  ip inspect firewall out
```

If the CallManager is requiring Skinny registration to happen on port tcp/2100, you will still need the above configuration plus the following additional step.

```
ip port map skinny port 2100
```

Additional References

The following sections provide additional references related to the Firewall Support of Skinny Client Control Protocol (SCCP) feature:

- [Related Documents, page 11](#)
- [Standards, page 11](#)
- [MIBs, page 11](#)
- [RFCs, page 11](#)
- [Technical Assistance, page 11](#)

Related Documents

Related Topic	Document Title
Additional CBAC information and configuration tasks	<i>The chapter “Configuring Context-based Access Control” in the Cisco IOS Security Configuration Guide, Release 12.3</i>
CBAC commands	<i>Cisco IOS Security Command Reference, Release 12.3</i>
PAM information and configuration tasks	<i>The chapter “Configuring Port to Application Mapping” in the Cisco IOS Security Configuration Guide, Release 12.3</i>

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs ¹	Title
None	—

1. Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this

module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug ip inspect**
- **ip inspect name**
- **ip port-map**

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Granular Protocol Inspection

The Granular Protocol Inspection feature adds flexibility to the Cisco IOS Firewall by allowing it to perform a higher degree of inspection of TCP and User Data Protocol (UDP) traffic for most RFC 1700 application types.

Feature History for Granular Protocol Inspection

Release	Modification
12.3(14)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Granular Inspection Protocol, page 1](#)
- [Restrictions for Granular Inspection Protocol, page 2](#)
- [Information About Granular Protocol Inspection, page 2](#)
- [How to Configure Granular Protocol Inspection, page 5](#)
- [Configuration Examples for Granular Protocol Inspection, page 9](#)
- [Additional References, page 12](#)
- [Command Reference, page 13](#)
- [Glossary, page 14](#)

Prerequisites for Granular Inspection Protocol

- Cisco IOS Firewall software must be installed in your network.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- Access control lists (ACLs) must be applied to specified interfaces to enable the existing firewall software to function properly.

Restrictions for Granular Inspection Protocol

Port ranges cannot be specified directly in the **ip inspect name** command; use the port-to-application mapping (PAM) table.

Information About Granular Protocol Inspection

To use the Granular Protocol Inspection feature, you need to understand the following concepts:

- [Cisco IOS Firewall, page 3](#)
- [Granular Protocol Inspection, page 3](#)
- [Benefits, page 4](#)

Cisco IOS Firewall

The Cisco IOS Firewall is a security-specific option that provides inspection firewall functionality and intrusion detection for every network perimeter. By delivering state-of-the-art security features such as stateful, application-based filtering; dynamic per-user authentication and authorization; and URL filtering, the Cisco IOS Firewall adds greater depth and flexibility to existing Cisco IOS security solutions including authentication, encryption, and failover.

A firewall is a physical software or hardware barrier between one part of an internal network used to control access to and from external networks. This barrier is unique because it allows predefined traffic to pass through the firewall while being monitored for protocol anomalies. The difficult part is determining the criteria by which the packets are granted or denied access through the device.

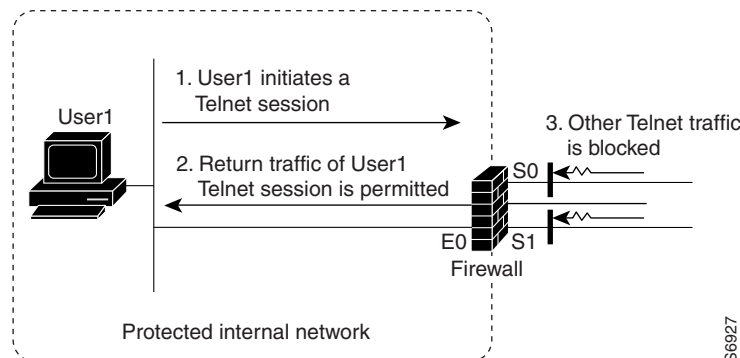
As mentioned, a firewall blocks traffic and permits other types of traffic to traverse. Firewalls are not just access control lists (ACLs); rather, they are a stateful inspection application.

Granular Protocol Inspection

The Cisco IOS Firewall performs inspections for TCP and UDP traffic. For example, TCP inspections include Telnet traffic (port 23, by default) as well as all other applications on TCP such as Hypertext Transfer Protocol (HTTP), e-mail, instant message (IM) chatter, and so on. Therefore, there is no easy way to inspect Telnet traffic alone and deny all other TCP traffic.

The Granular Protocol Inspection feature allows you to specify TCP or UDP ports using the PAM table. As a result, the Cisco IOS Firewall can restrict traffic inspections to specific applications, thereby permitting a higher degree of granularity in selecting which protocols are to be permitted and denied as shown in [Figure 32](#).

Figure 32 **Sample Topology**



Benefits

The Granular Protocol Inspection feature provides the following benefits:

- Greater flexibility by allowing more granularity in the selection of protocols to be inspected
- Ease of use by providing for group inspection of multiple ports into a single, user-defined application keyword
- Enhanced functionality with the addition of more well-known ports, user-defined applications, and user-defined port ranges
- Improved performance and reduced CPU load resulting from focused inspection selections

How to Configure Granular Protocol Inspection

This section contains the following procedures:

- [Defining Applications, page 5](#) (required)
- [Setting Up Inspection Rules, page 6](#) (required)
- [Verifying the Configuration, page 7](#) (optional)

Defining Applications

Perform the following task to define your applications in the PAM table by using the **ip port-map** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip port-map** *appl-name* **port** [**tcp** | **udp**] [*port_num* | **from** *begin_port_num* **to** *end_port_num*] [*list acl-num*] [**description** *description_string*]
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip port-map <i>appl-name</i> port [tcp udp] [<i>port_num</i> from <i>begin_port_num</i> to <i>end_port_num</i>] [list <i>acl-num</i>] [description <i>description_string</i>] Example: Router(config)# ip port-map user-10 port udp from 3400 to 3433 list 22 description "test application"	Establishes PAM entries. Note When defining a user application in the PAM table, you must enter the prefix user- ; otherwise, the following error message appears: "Unable to add port-map entry. Names for user-defined applications must start with 'user-'." Note Write the text string in the following format: " <i>C description_string C</i> ," where " <i>C</i> " is a delimiting character.
Step 4	exit Example: Router(config)# exit	Exits global configuration mode.

Setting Up Inspection Rules

Perform the following task to set up your inspection rules by using the **ip inspect name** command.

SUMMARY STEPS

- enable**
- configure terminal**
- ip inspect name** *inspection-name* *protocol* [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*]
- exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip inspect name inspection-name protocol [alert {on off}] [audit-trail {on off}] [timeout seconds] Example: Router(config)# ip inspect name abc user-10	Defines inspection rules. Note Replace the <i>protocol</i> argument with the application (PAM entry) that you just defined in the previous step. In this example, it is <i>user-10</i> .
Step 4	exit Example: Router(config)# exit	Exits global configuration mode.

Verifying the Configuration

Perform the following task to verify your applications and inspection rules.

SUMMARY STEPS

1. enable
2. show ip port-map [appl-name | port port-num [detail]]
3. exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	show ip port-map [<i>appl-name</i> port <i>port-num</i> [detail]] Example: Router# show ip port-map port 70 detail	Establishes PAM entries.
Step 3	exit Example: Router# exit	(Optional) Exits privileged EXEC mode.

Configuration Examples for Granular Protocol Inspection

This section contains the following configuration examples:

- [Defining an Application for the PAM Table: Example, page 9](#)
- [Setting Up an Inspection Rule: Example, page 9](#)
- [Verifying the Configuration: Example, page 10](#)

Defining an Application for the PAM Table: Example

In the following example from the **ip port-map** command, a user-defined application named user-10 is defined in the PAM table for five ports using the TCP protocol. Standard access list 77 is applied to define host-specific port mapping and “TEST STRING” is the description.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)# ip port-map user-10 port tcp 4000 5000 6000 7000 8000 list 77 description
"TEST STRING"
```

```
Router(config)# end
```

Setting Up an Inspection Rule: Example

The following example from the **ip inspect name** command, lists user-10 as an application with the description “TEST STRING.”

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)# ip inspect name abc ?
```

bootpc	Bootstrap Protocol Client
bootps	Bootstrap Protocol Server
cisco-fna	Cisco FNATIVE
cisco-sys	Cisco SYSMAINT
cisco-tna	Cisco TNATIVE
cuseeme	CUSEeMe Protocol
echo	Echo port
esmtpt	Extended SMTP
finger	Finger
fragment	IP fragment inspection
ftp	File Transfer Protocol
gopher	Gopher
gtpv0	GPRS Tunneling Protocol Version 0
gtpv1	GPRS Tunneling Protocol Version 1
h323	H.323 Protocol (e.g, MS NetMeeting, Intel Video Phone)
http	HTTP Protocol
icmp	ICMP Protocol
imap	IMAP Protocol
imap3	Interactive Mail Access Protocol 3
kerberos	Kerberos
ldap	Lightweight Directory Access Protocol
netbios-dgm	NETBIOS Datagram Service
netshow	Microsoft NetShow Protocol

```

nntp          Network News Transport Protocol
parameter    Specify inspection parameters
pop3         POP3 Protocol
pwdgen       Password Generator Protocol
rcmd         R commands (r-exec, r-login, r-sh)
realaudio    Real Audio Protocol
rpc          Remote Procedure Call Protocol
rtsp         Real Time Streaming Protocol
secure-http  Secure Hypertext Transfer Protocol
sip          SIP Protocol
skinny       Skinny Client Control Protocol
smtp         Simple Mail Transfer Protocol
snmp         Simple Network Management Protocol
snmptrap     SNMP Trap
sqlnet       SQL Net Protocol
sqlsrv       SQL Service
streamworks  StreamWorks Protocol
tacacs       Login Host Protocol (TACACS)
tacacs-ds    TACACS-Database Service
tcp          Transmission Control Protocol
telnet       Telnet
tftp         TFTP Protocol
udp          User Datagram Protocol
vdolive      VDOLive Protocol
user-10      TEST STRING<----- !user-defined application!

```

In the following example from the **ip inspect name** command, an inspection rule is established for user-10:

```

Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# ip inspect name abc user-10

Router(config)# end

```

Verifying the Configuration: Example

The following example verifies your port-map configuration:

```

Router# show running-config | include port-map

ip port-map user-10 port tcp 4000 5000 6000 7000 8000 list 77 description "TEST STRING"

```

The following example verifies your inspection rule configuration:

```

Router# show running-config | include inspect

ip inspect name abc user-10

```

The following example displays information about the user-defined application called user-10.

```
Router# show ip port-map user-10
```

```
Host specific:      user-10                tcp port 4000...8000      in list 77      user defined
```

The following example displays detailed information about the user-defined application called user-10.

```
Router# show ip port-map user-10 detail
```

```
IP port-map entry for application 'user-10':
```

```
tcp 4000...8000                list 77 "TEST STRING"                user defined
```

Additional References

The following sections provide references related to the Granular Protocol Inspection feature.

Related Documents

Related Topic	Document Title
Security commands: complete command syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS Security Command Reference , Release 12.3 T
Security features including firewalls and authentication	Cisco IOS Security Configuration Guide , Release 12.3

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **ip inspect name**
- **ip port-map**
- **show ip port-map**

Glossary

CBAC—Context-Based Access Control. A protocol that provides internal users with secure access control for each application and for all traffic across network perimeters. CBAC enhances security by scrutinizing both source and destination addresses and by tracking each application's connection status.

firewall—A router or access server, or several routers or access servers, designated as a buffer between any connected public networks and a private network. A firewall router uses access lists and other methods to ensure the security of the private network.

granular—Degree of componentization. Small, fine-grained components provide greater flexibility in assembling the right combination of functionality, but can be difficult to manage.

inspection rule—A rule that specifies what IP traffic (which application-layer protocols) will be inspected by CBAC at an interface.

PAM—port-to-application mapping. A flexible, per-application port mapping capability that allows the Cisco IOS Firewall to support applications running on nonstandard ports. This feature allows network administrators to customize access control for specific applications and services, in order to meet their distinct network needs.

traffic inspection—A way that CBAC inspects traffic that travels through the firewall to discover and manage state information for TCP and UDP sessions. This state information is used to create temporary openings in the firewall's access lists to allow return traffic and additional data connections for permissible sessions (sessions that originated from within the protected internal network).

UDP—User Data Protocol. A connectionless service—there are no actual sessions, so the software approximates sessions by examining the information in the packet and determining if the packet is similar to other UDP packets (for example, similar source/destination addresses and port numbers) and if the packet was detected soon after another similar UDP packet. "Soon" means within the configurable UDP idle timeout period.

**Note**

Refer to [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



H.323 RAS Support in Cisco IOS Firewall

First Published: November 17, 2006

Last Updated: November 17, 2006

This feature introduces support for H.225 Registration, Admission, and Status (RAS) signaling in Cisco IOS firewalls. RAS is a signaling protocol that is used between endpoints (such as gateways) and gatekeepers.

The H.225 standard is used by H.323 for call setup. H.255 includes RAS control, which is used to communicate with the gatekeeper. A RAS signaling channel enables connections between the gatekeeper and H.323 endpoints.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for H.323 RAS Support in Cisco IOS Firewall”](#) section on page 8.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Restrictions for H.323 RAS Support in Cisco IOS Firewall, page 2](#)
- [How to Configure a Firewall Policy for H.323 RAS Protocol Inspection, page 2](#)
- [Configuration Examples for H.225 RAS Protocol Inspection, page 6](#)
- [Additional References, page 6](#)
- [Command Reference, page 7](#)
- [Feature Information for H.323 RAS Support in Cisco IOS Firewall, page 8](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Restrictions for H.323 RAS Support in Cisco IOS Firewall

H.225 RAS inspection is supported only with zone-based policy firewall inspection.

How to Configure a Firewall Policy for H.323 RAS Protocol Inspection

This section contains the following configuration tasks:

- [Configuring a Class Map for H.323 RAS Protocol Inspection, page 2](#)
- [Creating a Policy Map for H.323 RAS Protocol Inspection, page 3](#)

Configuring a Class Map for H.323 RAS Protocol Inspection

Use this task to configure a class map for classifying network traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type inspect** [**match any** | **match all**] *class-map-name*
4. **match access-group** { *access-group* | **name** *access-group-name* }
5. **match protocol** *protocol-name* [**signature**]
6. **match class-map** *class-map-name*
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	class-map type inspect [match-any match-all] <i>class-map-name</i> Example: Router(config)# class-map type inspect match-all c1	Creates a Layer 3 or Layer 4 inspect type class map and enters class-map configuration mode.
Step 4	match access-group { <i>access-group</i> name <i>access-group-name</i> } Example: Router(config-cmap)# match access-group 101	(Optional) Configures the match criterion for a class map based on the access control list (ACL) name or number.
Step 5	match protocol <i>protocol-name</i> [signature] Example: Router(config-cmap)# match protocol h225ras	Configures the match criterion for a class map on the basis of a specified protocol. Note You should specify the h225ras keyword to create a class-map for H.225 RAS protocol classification. For a list of supported protocols, use the command-line interface (CLI) help option (?) on your platform.
Step 6	match class-map <i>class-map-name</i> Example: Router(config-cmap)# match class-map c1	(Optional) Specifies a previously defined class as the match criterion for a class map.
Step 7	exit Example: Router(config-cmap)# exit	Returns to global configuration mode.

Creating a Policy Map for H.323 RAS Protocol Inspection

Use this task to create a policy map for a firewall policy that will be attached to zone pairs.

**Note**

If you are creating an inspect type policy map, only the following actions are allowed: drop, inspect, police, and pass.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *policy-map-name*
4. **class type inspect** *class-name*
5. **inspect** [*parameter-map-name*]
6. **police rate** *bps* **burst** *size*
7. **drop** [log]
8. **pass**
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy-map type inspect <i>policy-map-name</i> Example: Router(config)# policy-map type inspect p1	Creates a Layer 3 and Layer 4 inspect type policy map and enters policy-map configuration mode.
Step 4	class type inspect <i>class-name</i> Example: Router(config-pmap)# class type inspect c1	Specifies the traffic (class) on which an action is to be performed and enters policy-map class configuration mode.
Step 5	inspect [<i>parameter-map-name</i>] Example: Router(config-pmap-c)# inspect inspect-params	Enables Cisco IOS stateful packet inspection.
Step 6	police rate <i>bps</i> <i>burst size</i> Example: Router(config-pmap-c)# police rate 2000 burst 3000	(Optional) Limits traffic matching within a firewall (inspect) policy.
Step 7	drop [log] Example: Router(config-pmap-c)# drop	(Optional) Drops packets that are matched with the defined class. Note The actions drop and pass are exclusive, and the actions inspect and drop are exclusive; that is, you cannot specify both of them.
Step 8	pass Example: Router(config-pmap-c)# pass	(Optional) Allows packets that are matched with the defined class.
Step 9	exit Example: Router(config-pmap-c)# exit	Returns to policy-map configuration mode.

What to Do Next

After configuring an H.323 RAS protocol firewall policy, you want to attach the policy to a zone pair. For information on completing this task, see the [“Zone-Based Policy Firewall”](#) module.

Configuration Examples for H.225 RAS Protocol Inspection

This section contains the following configuration example:

- [H.323 RAS Protocol Inspection Configuration: Example, page 6](#)

H.323 RAS Protocol Inspection Configuration: Example

The following example shows how to configure an H.323 RAS protocol inspection policy:

```
class-map type inspect match-any c1
  match protocol h323
  match protocol h225ras
class-map type inspect match-all c2
  match protocol icmp
!
policy-map type inspect p1
  class type inspect c1
  inspect
  class class-default
  drop
policy-map type inspect p2
  class type inspect c2
  inspect
  class class-default
  drop
!
zone security z1
  description One-Network zone
zone security z2
  description Two-Network zone
zone-pair security zp source z1 destination z2
  service-policy type inspect p1
zone-pair security zp-rev source z2 destination z1
  service-policy type inspect p2
!
interface FastEthernet1/0
  ip address 10.0.0.0 255.255.0.0
  zone-member security z1
  duplex auto
  speed auto
!
interface FastEthernet1/1
  ip address 10.0.1.1 255.255.0.0
  zone-member security z2
  duplex auto
  speed auto
```

Additional References

The following sections provide references related to the H.323 RAS Support in Cisco IOS Firewall feature.

Related Documents

Related Topic	Document Title
Zone-based policy information: configurations, examples, descriptions	Zone-Based Policy Firewall , Cisco IOS Release 12.4(9)T Zone-Based Policy Firewall Design Guide
Zone-based policy configuration commands	Cisco IOS Security Command Reference

MIBs

MIB	MIBs Link
No new or modified MIBs are supported.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and technical documentation. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **match protocol (zone)**

Feature Information for H.323 RAS Support in Cisco IOS Firewall

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for H.323 RAS Support

Feature Name	Releases	Feature Information
H.323 RAS Support in Cisco IOS Firewall	12.4(11)T	This feature introduces support for H.255 Registration, Admission, and Status (RAS) signaling in Cisco IOS firewalls.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



HTTP Inspection Engine

The HTTP Inspection Engine feature allows users to configure their Cisco IOS Firewall to detect and prohibit HTTP connections—such as tunneling over port 80, unauthorized request methods, and non-HTTP compliant file transfers—that are not authorized within the scope of the security policy configuration. Tunneling unauthorized protocols through port 80 and over HTTP exposes a network to significant security risks.

The Cisco IOS Firewall can now be configured with a security policy that adheres to the following tasks:

- Allowing specific traffic targeted for port 80 to traverse the firewall. The traffic is inspected for protocol conformance and for the types of HTTP commands that are allowed or disallowed.
- Denying specific traffic targeted for port 80 that does not comply to HTTP traffic standards. The firewall is enabled to drop the packet, reset the connection, and send a syslog message, as appropriate.

Feature History for HTTP Inspection Engine

Release	Modification
12.3(14)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions for HTTP Inspection Engine, page 2](#)
- [Information About HTTP Inspection Engine, page 2](#)
- [How to Define and Apply an HTTP Application Policy to a Firewall for Inspection, page 2](#)
- [Configuration Examples for Setting Up an HTTP Inspection Engine, page 10](#)
- [Additional References, page 11](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Command Reference, page 12](#)

Restrictions for HTTP Inspection Engine

The Cisco 831 router with 48M RAM does not have enough memory to support this feature.

Information About HTTP Inspection Engine

Before configuring an application firewall to detect and police specific traffic targeted for port 80, you should understand the following concepts:

- [What Is a Security Policy?, page 2](#)
- [Cisco IOS HTTP Application Policy Overview, page 2](#)

What Is a Security Policy?

The application firewall uses a security policy, which consists of a collection of static signatures, to detect security violations. A static signature is a collection of parameters that specify protocol conditions that must be met before an action is taken. (For example, a signature may specify that an HTTP data stream containing the POST method must reset the connection.) These protocol conditions and reactions are defined by the end user via the command-line interface (CLI) to form a security policy.

Cisco IOS HTTP Application Policy Overview

HTTP uses port 80 to transport Internet web services, which are commonly used on the network and rarely challenged with regards to their legitimacy and conformance to standards. Because port 80 traffic is typically allowed through the network without being challenged, many application developers are leveraging HTTP traffic as an alternative transport protocol in which to enable their application to travel through or even bypass the firewall.

Most firewalls provide only packet filtering capabilities that simply permit or deny port 80 traffic without inspecting the data stream; the Cisco IOS application firewall for HTTP performs packet inspection as follows:

- Detects HTTP connections that are not authorized within the scope of the security policy configuration.
- Detects users who are tunneling applications through port 80.

If the packet is not in compliance with the HTTP protocol, it will be dropped, the connection will be reset, and a syslog message will be generated, as appropriate.

How to Define and Apply an HTTP Application Policy to a Firewall for Inspection

This section contains the following procedures:

- [Defining an HTTP Application Policy, page 3](#)

- [Applying an HTTP Application Policy to a Firewall for Inspection, page 7](#)

Defining an HTTP Application Policy

Use this task to create an HTTP application firewall policy.

Restrictions

Although application firewall policies are defined in global configuration mode, only one global policy for a given protocol is allowed per interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **appfw policy-name** *policy-name*
4. **application** *protocol*
5. **strict-http action** {reset | allow} [alarm]
6. **content-length** {min *bytes* max *bytes* | min *bytes* | max *bytes*} **action** {reset | allow} [alarm]
7. **content-type-verification** [match-req-resp] **action** {reset | allow} [alarm]
8. **max-header-length** {request *bytes* response *bytes*} **action** {reset | allow} [alarm]
9. **max-uri-length** *bytes* **action** {reset | allow} [alarm]
10. **request-method** {rfc *rfc-method* | extension *extension-method*} **action** {reset | allow} [alarm]
11. **port-misuse** {p2p | tunneling | im | default} **action** {reset | allow} [alarm]
12. **transfer-encoding type** {chunked | compress | deflate | gzip | identity | default} **action** {reset | allow} [alarm]
13. **timeout** *seconds*
14. **audit-trail** {on | off}
15. **exit**
16. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	appfw policy-name policy-name Example: Router(config)# appfw policy-name mypolicy	Defines an application firewall policy and puts the router in application firewall policy configuration mode.
Step 4	application protocol Example: Router(cfg-appfw-policy)# application http	Allows you to configure inspection parameters for a given protocol. Currently, only HTTP traffic can be inspected. <ul style="list-style-type: none"> <i>protocol</i> —Specify the http keyword. This command puts you in <i>appfw-policy-protocol</i> configuration mode, where “ <i>protocol</i> ” is dependent upon the specified protocol. Because only HTTP can be specified, the configuration mode is <i>appfw-policy-http</i> .
Step 5	strict-http action {reset allow} [alarm] Example: Router(cfg-appfw-policy-http)# strict-http action allow alarm	(Optional) Allows HTTP messages to pass through the firewall or resets the TCP connection when HTTP noncompliant traffic is detected.
Step 6	content-length {min bytes max bytes min bytes max bytes} action {reset allow} [alarm] Example: Router(cfg-appfw-policy-http)# content-length max 1 action allow alarm	(Optional) Permits or denies HTTP traffic through the firewall on the basis of message size. <ul style="list-style-type: none"> min max bytes—Minimum or maximum content length, in bytes, allowed per message. Number of bytes range: 0 to 65535.
Step 7	content-type-verification [match-req-resp] action {reset allow} [alarm] Example: Router(cfg-appfw-policy-http)# content-type-verification match-req-resp action allow alarm	(Optional) Permits or denies HTTP traffic through the firewall on the basis of content message type.
Step 8	max-header-length {request bytes response bytes} action {reset allow} [alarm] Example: Router(cfg-appfw-policy-http)# max-header-length request 1 response 1 action allow alarm	(Optional) Permits or denies HTTP traffic on the basis of the message header length. <ul style="list-style-type: none"> <i>bytes</i>—Number of bytes ranging from 0 to 65535.

	Command or Action	Purpose
Step 9	max-uri-length <i>bytes</i> action { reset allow } [alarm] Example: Router(cfg-appfw-policy-http)# max-uri-length 1 action allow alarm	(Optional) Permits or denies HTTP traffic on the basis of the URI length in the request message.
Step 10	request method { rfc <i>rfc-method</i> extension <i>extension-method</i> } action { reset allow } [alarm] Example: Router(cfg-appfw-policy-http)# request-method rfc default action allow alarm	(Optional) Permits or denies HTTP traffic according to either the request methods or the extension methods. <ul style="list-style-type: none"> • rfc—Specifies that the supported methods of RFC 2616, <i>Hypertext Transfer Protocol—HTTP/1.1</i>, are to be used for traffic inspection. • <i>rfc-method</i>—Any one of the following RFC 2616 methods can be specified: connect, default, delete, get, head, options, post, put, trace. • extension—Specifies that the extension methods are to be used for traffic inspection. • <i>extension-method</i>—Any one of the following extension methods can be specified: copy, default, edit, getattribute, getproperties, index, lock, mkdir, move, revadd, revlabel, revlog, save, setattribute, startrev, stoprev, unedit, unlock.
Step 11	port-misuse { p2p tunneling im default } action { reset allow } [alarm] Example: Router(cfg-appfw-policy-http)# port-misuse default action allow alarm	(Optional) Permits or denies HTTP traffic through the firewall on the basis of specified applications in the HTTP message. <ul style="list-style-type: none"> • p2p—Peer-to-peer protocol applications subject to inspection: Kazaa and Gnutella. • tunneling—Tunneling applications subject to inspection: HTTPPort/HTTPHost, GNU Httptunnel, GotoMyPC, Firethru, Http-tunnel.com Client • im—Instant messaging protocol applications subject to inspection: Yahoo Messenger. • default—All applications are subject to inspection.

	Command or Action	Purpose
Step 12	<p>transfer-encoding type {chunked compress deflate gzip identity default} action {reset allow} [alarm]</p> <p>Example: Router(cfg-appfw-policy-http)# transfer-encoding type default action allow alarm</p>	<p>(Optional) Permits or denies HTTP traffic according to the specified transfer-encoding of the message.</p> <ul style="list-style-type: none"> • chunked—Encoding format (specified in RFC 2616, <i>Hypertext Transfer Protocol—HTTP/1</i>) in which the body of the message is transferred in a series of chunks; each chunk contains its own size indicator. • compress—Encoding format produced by the UNIX “compress” utility. • deflate—“ZLIB” format defined in RFC 1950, <i>ZLIB Compressed Data Format Specification version 3.3</i>, combined with the “deflate” compression mechanism described in RFC 1951, <i>DEFLATE Compressed Data Format Specification version 1.3</i>. • gzip—Encoding format produced by the “gzip” (GNU zip) program. • identity—Default encoding, which indicates that no encoding has been performed. • default—All of the transfer encoding types.
Step 13	<p>timeout <i>seconds</i></p> <p>Example: Router(cfg-appfw-policy-http)# timeout 60</p>	<p>(Optional) Overrides the global TCP idle timeout value for HTTP traffic.</p> <p>Note If this command is not issued, the default value specified via the ip inspect tcp idle-time command will be used.</p>
Step 14	<p>audit-trail {on off}</p> <p>Example: Router(cfg-appfw-policy-http)# audit-trail on</p>	<p>(Optional) Turns audit trail messages on or off.</p> <p>Note If this command is not issued, the default value specified via the ip inspect audit-trail command will be used.</p>
Step 15	<p>exit</p> <p>Example: Router(cfg-appfw-policy-http)# exit</p>	Exits cfg-appfw-policy-http configuration mode.
Step 16	<p>exit</p> <p>Example: Router(cfg-appfw-policy)# exit</p>	Exits cfg-appfw-policy configuration mode.

What to Do Next

After you have successfully defined an application policy for HTTP traffic inspection, you must apply the policy to an inspection rule. Thereafter, the inspection rule must be applied to an interface. For information on completing this task, see the section “[Applying an HTTP Application Policy to a Firewall for Inspection.](#)”

Applying an HTTP Application Policy to a Firewall for Inspection

Use this task to apply an HTTP application policy to an inspection rule, followed by applying the inspection rule to an interface.

**Note**

An application policy can coexist with other inspection protocols (for example, an HTTP policy and an FTP policy can coexist).

Prerequisites

You must have already defined an application policy (as shown in the section “[Defining an HTTP Application Policy](#)”).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip inspect name** *inspection-name* **appfw** *policy-name*
4. **ip inspect name** *inspection-name* **http** [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*]
5. **interface** *type number*
6. **ip inspect** *inspection-name* {**in** | **out**}
7. **exit**
8. **exit**
9. **show appfw configuration** [*name*]
or
show ip inspect {**name** *inspection-name* | **config** | **interfaces** | **session** [**detail**] | **statistics** | **all**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip inspect name inspection-name appfw policy-name Example: Router(config)# ip inspect name firewall appfw mypolicy	Defines a set of inspection rules for the application policy. <ul style="list-style-type: none"> <i>policy-name</i>—Must match the policy name specified via the appfw policy-name command.
Step 4	ip inspect name inspection-name http [alert {on off}] [audit-trail {on off}] [timeout seconds] Example: Router(config)# ip inspect name firewall http	Defines a set of inspection rules that is to be applied to all HTTP traffic. <ul style="list-style-type: none"> The <i>inspection-name</i> argument must match the <i>inspection-name</i> argument specified in Step 3.
Step 5	interface type number Example: Router#(config)# interface FastEthernet0/0	Configures an interface type and enters interface configuration mode.
Step 6	ip inspect inspection-name {in out} Example: Router#(config-if)# ip inspect firewall in	Applies the inspection rules (defined in Step 3 and Step 4) to all traffic entering the specified interface. <ul style="list-style-type: none"> The <i>inspection-name</i> argument must match the inspection name defined via the ip inspect name command.
Step 7	exit Example: Router#(config-if)# exit	Exits interface configuration mode.

	Command or Action	Purpose
Step 8	exit Example: Router(config)# exit	Exits global configuration mode.
Step 9	show appfw configuration [name] Example: Router# show appfw configuration or show ip inspect {name inspection-name config interfaces session [detail] statistics all} Example: Router# show ip inspect config	(Optional) Displays application firewall policy configuration information. (Optional) Displays firewall-related configuration information.

Troubleshooting Tips

To help troubleshoot the application firewall configuration, issue the following application-firewall specific debug command: **debug appfw {application protocol | function-trace | object-creation | object-deletion | events | timers | detailed}**.

The following sample configuration shows how to configure an HTTP policy with application firewall debugging enabled:

```
Router(config)# appfw policy-name myPolicyAPPPFW FUNC:appfw_policy_find
APPPFW FUNC:appfw_policy_find -- Policy myPolicy is not found
APPPFW FUNC:appfw_policy_alloc
APPPFW FUNC:appfw_policy_alloc -- policy_alloc 0x65727278
APPPFW FUNC:appfw_policy_alloc -- Policy 0x65727278 is set to valid
APPPFW FUNC:appfw_policy_alloc -- Policy myPolicy has been created
APPPFW FUNC:appfw_policy_command -- memlock policy 0x65727278

! Debugging sample for application (HTTP) creation

Router(cfg-appfw-policy)# application httpAPPPFW FUNC:appfw_http_command
APPPFW FUNC:appfw_http_appl_find
APPPFW FUNC:appfw_http_appl_find -- Application not found
APPPFW FUNC:appfw_http_appl_alloc
APPPFW FUNC:appfw_http_appl_alloc -- appl_http 0x64D7A25C
APPPFW FUNC:appfw_http_appl_alloc -- Application HTTP parser structure 64D7A25C created

! Debugging sample for HTTP-specific application inspection
Router(cfg-appfw-policy-http)#
Router(cfg-appfw-policy-http)# strict-http action reset alarm
APPPFW FUNC:appfw_http_subcommand
APPPFW FUNC:appfw_http_subcommand -- strict-http cmd turned on

Router# debug appfw detailed

APPPFW Detailed Debug debugging is on
fw7-7206a#debug appfw object-creation
APPPFW Object Creations debugging is on
fw7-7206a#debug appfw object-deletion
APPPFW Object Deletions debugging is on
```

Configuration Examples for Setting Up an HTTP Inspection Engine

This section contains the following configuration example:

- [Setting Up and Verifying an HTTP Inspection Engine: Example, page 10](#)

Setting Up and Verifying an HTTP Inspection Engine: Example

The following example show how to define the HTTP application firewall policy “mypolicy.” This policy includes all supported HTTP policy rules. This example also includes sample output from the **show appfw configuration** and **show ip inspect config** commands, which allow you to verify the configured setting for the application policy.

```
! Define the HTTP policy.
appfw policy-name mypolicy
  application http
    strict-http action allow alarm
    content-length maximum 1 action allow alarm
    content-type-verification match-req-rsp action allow alarm
    max-header-length request 1 response 1 action allow alarm
    max-uri-length 1 action allow alarm
    port-misuse default action allow alarm
    request-method rfc put action allow alarm
    transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
  ip inspect firewall in
!
!
! Issue the show appfw configuration command and the show ip inspect config command after
the inspection rule “mypolicy” is applied to all incoming HTTP traffic on the
FastEthernet0/0 interface.
!
Router# show appfw configuration

Application Firewall Rule configuration
Application Policy name mypolicy
  Application http
    strict-http action allow alarm
    content-length minimum 0 maximum 1 action allow alarm
    content-type-verification match-req-rsp action allow alarm
    max-header-length request length 1 response length 1 action allow alarm
    max-uri-length 1 action allow alarm
    port-misuse default action allow alarm
    request-method rfc put action allow alarm
    transfer-encoding default action allow alarm

Router# show ip inspect config

Session audit trail is disabled
Session alert is enabled
```

```
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
Inspection name firewall
http alert is on audit-trail is off timeout 3600
```

Additional References

The following sections provide references related to the HTTP Inspection Engine feature.

Related Documents

Related Topic	Document Title
Firewall commands: complete command syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS Security Command Reference , Release 12.3T

Standards

Standards	Title
No new or modified standards are supported by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2616	<i>Hypertext Transfer Protocol -- HTTP/1.1</i>

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at

<http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

New Commands

- **appfw policy-name**
- **application**
- **audit-trail**
- **content-length**
- **content-type-verification**
- **debug appfw**
- **max-header-length**
- **max-uri-length**
- **port-misuse**
- **request-method**
- **show appfw**
- **strict-http**
- **timeout**
- **transfer-encoding type**

Modified Command

- **ip inspect name**

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Inspection of Router-Generated Traffic

The Inspection of Router-Generated Traffic feature allows Context-Based Access Control (CBAC) to inspect traffic that is originated by or destined to the router on which CBAC is configured. Previously, inspection of Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and H.323 connections initiated by or destined to the router were allowed.

Feature History for Inspection of Router-Generated Traffic

Release	Modification
12.3(14)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Inspection of Router-Generated Traffic, page 2](#)
- [Restrictions for Inspection of Router-Generated Traffic, page 2](#)
- [Information About Inspection of Router-Generated Traffic, page 2](#)
- [How to Configure Inspection of Router-Generated Traffic, page 3](#)
- [Configuration Examples for Inspection of Router-Generated Traffic, page 9](#)
- [Additional References, page 9](#)
- [Command Reference, page 10](#)
- [Glossary, page 12](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for Inspection of Router-Generated Traffic

- Configure CBAC.
- Configure Cisco Call Manager Express (CCME) or H.323 Gateway to configure the inspection of H.323 connections to and from the router.

Restrictions for Inspection of Router-Generated Traffic

- Inspection of router-generated traffic is supported only on the following protocols: H.323, TCP, and UDP.
- The Cisco IOS Firewall supports only Version 2 of the H.323 protocol. If CCME or the H.323 Gateway has inspection of H.323 router traffic enabled, enter the following commands so that it is configured to support only Version 2 features:

```
voice service voip
h323
session transport tcp calls-per-connection 1
h245 tunnel disable
h245 caps mode restricted
h225 timeout tcp call-idle value 0
```

Information About Inspection of Router-Generated Traffic

To configure Inspection of Router-Generated Traffic, you need to understand the following concepts:

- [CBAC, page 2](#)
- [Inspection of Router-Generated Traffic Overview, page 3](#)

CBAC

CBAC is a Cisco IOS Firewall set feature that provides network protection by using the following functions:

- [Traffic Filtering](#)
- [Traffic Inspection](#)
- [Alerts and Audit Trails](#)
- [Intrusion Detection](#)

Traffic Filtering

CBAC filters TCP and UDP packets based on application-layer protocol session information. You can configure CBAC to permit specified TCP and UDP traffic through a firewall only when the connection is initiated from within the network you want to protect. CBAC can inspect traffic for sessions that originate from either side of the firewall, and CBAC can be used for intranet, extranet, and Internet perimeters of your network.

Traffic Inspection

CBAC inspects traffic that travels through the firewall to discover and manage state information for TCP and UDP sessions. This state information is used to create temporary openings in the firewall's access lists to allow return traffic and additional data connections for permissible sessions.

Alerts and Audit Trails

CBAC generates real-time alerts and audit trails. Enhanced audit trail features use SYSLOG to track all network transactions; it records time stamps, the source host, the destination host, the ports used, and the total number of transmitted bytes, for advanced, session-based reporting. Real-time alerts send SYSLOG error messages to central management consoles upon detecting suspicious activity.

Using CBAC inspection rules, you can configure alerts and audit trail information on a per-application protocol basis. For example, if you want to generate audit trail information for HTTP traffic, you can specify that in the CBAC rule covering HTTP inspection.

Intrusion Detection

CBAC provides a limited amount of intrusion detection to protect against specific Simple Mail Transfer Protocol (SMTP) attacks. With intrusion detection, SYSLOG messages are reviewed and monitored for specific “attack signatures.” Certain types of network attacks have specific characteristics, or signatures. When CBAC detects an attack, it resets the offending connections and sends SYSLOG information to the SYSLOG server.

Inspection of Router-Generated Traffic Overview

Inspection of Router-Generated Traffic enhances CBAC's functionality to inspect TCP, UDP, and H.323 connections that have a router or firewall as one of the connection endpoints. This enables CBAC to open pinholes for TCP, UDP, and H.323 control channel connections to and from the router, and to open pinholes for data and media channels negotiated over the H.323 control channels.

Inspection of TCP and UDP channels initiated from the router enables dynamic opening of pinholes on the interface access control list (ACL) to allow return traffic. You do not have to modify the ACL when a TCP connection such as Telnet is made from the router.

Inspection of local H.323 connections enables the deployment of CCME, H.323 gateway, and the Cisco IOS Firewall on the same router. This also simplifies ACL configuration on CCME's interface through which H.323 connections are made. Before this feature, in addition to configuring ACLs to allow H.323 connections on a standard port (for example, port 1720), you had to configure ACLs to allow all dynamically negotiated data and media channels. With this feature you just configure the ACLs to allow H.323 control channels on port 1720. The Cisco IOS Firewall inspects all the traffic on the control channel and opens pinholes to allow dynamically negotiated data and media channels.

To enable Inspection of Router-Generated Traffic, specify the **router-traffic** keyword in the **ip inspect name** command of the appropriate protocol.

How to Configure Inspection of Router-Generated Traffic

This section contains the following procedures:

- [Configuring H.323 Inspection, page 4](#) (required)
- [Configuring CBAC, page 5](#) (required)
- [Verifying the CBAC Configuration, page 7](#) (optional)

Configuring H.323 Inspection

To configure the H.323 protocol, perform the following steps.

SUMMARY STEPS

- 1. **enable**
- 2. **configure terminal**
- 3. **ip inspect name** *inspection-name* {TCP | UDP | H323} [alert {on | off}] [audit-trail {on | off}][router-traffic][timeout *seconds*]
- 4. **interface** *type slot/port*
- 5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip inspect name <i>inspection-name</i> {TCP UDP H323} [alert {on off}] [audit-trail {on off}][router-traffic][timeout <i>seconds</i>] Example: Router(config)# ip inspect name test H.323 router-traffic	Defines a set of inspection rules.
Step 4	interface <i>type slot/port</i> Example: Router(config)# interface FE 0/0	Configures an interface type.
Step 5	exit Example: Router(config)# exit	Exits global configuration mode.

Configuring CBAC

To configure CBAC, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]
4. **ip inspect name** *inspection-name* {**TCP** | **UDP** | **H323**} [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**router-traffic**] [**timeout** *seconds*]
5. **interface** *type slot/port*
6. **ip inspect** *inspection-name* {**in** | **out**}
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	access-list <i>access-list-number</i> { deny permit } <i>source</i> [<i>source-wildcard</i>] [log] Example: Router(config)# access-list 121 permit tcp host 100.168.11.1 any eq 1720	Defines a standard IP access list.
Step 4	ip inspect name <i>inspection-name</i> { TCP UDP H323 } [alert { on off }] [audit-trail { on off }] [router-traffic] [timeout <i>seconds</i>] Example: Router(config)# ip inspect name here H323 router-traffic timeout 180	Defines a set of inspection rules.
Step 5	interface <i>type slot/port</i> Example: Router(config)# Serial0/3/0	Configures an interface type.

	Command or Action	Purpose
Step 6	ip inspect <i>inspection-name</i> { in out }	Enables the Cisco IOS Firewall on an interface.
	Example: Router(config-if)# ip inspect test in	
Step 7	exit	Exits global configuration mode and returns to privileged EXEC mode.
	Example: Router(config)# exit	

Verifying the CBAC Configuration

To verify the CBAC configuration, perform the following steps.

SUMMARY STEPS

1. `show ip inspect name inspection-name`
2. `show ip inspect config`
3. `show ip inspect interfaces`
4. `show ip inspect session [detail]`
5. `show ip inspect all`

DETAILED STEPS

Step 1 `show ip inspect name inspection-name`

Use this command to show a particular configured inspection rule. The following example configures the inspection rule `myinspectionrule`. **The output** shows the protocols that should be inspected by CBAC and the corresponding idle timeouts for each protocol.

```
Router# show ip inspect name myinspectionrule
```

```
Inspection Rule Configuration
```

```
Inspection name myinspectionrule
tcp timeout 3600
udp timeout 30
ftp timeout 3600
```

Step 2 `show ip inspect config`

Use this command to show the CBAC configuration, including global timeouts, thresholds, and inspection rules.

```
Router# show ip inspect config
```

```
Session audit trail is disabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
inspection name myinspectionrule
tcp timeout 3600
udp timeout 30
ftp timeout 3600
```

Step 3 show ip inspect interfaces

Use this command to show the interface configuration with respect to applied inspection rules and access lists.

```
Router# show ip inspect interfaces

Interface Configuration
Interface Ethernet0
  Inbound inspection rule is myinspectionrule
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
  Outgoing inspection rule is not set
  Inbound access list is not set
  Outgoing access list is not set
```

Step 4 show ip inspect session detail

Use this command to display existing sessions that CBAC is currently tracking and inspecting. The following sample output shows that an outgoing ACL and an inbound ACL (dynamic ACLs) have been created to allow return traffic.

```
Router# show ip inspect session detail

Established Sessions
Session 80E87274 (192.168.1.116:32956)=>(192.168.101.115:23) tcp SIS_OPEN
  Created 00:00:08, Last heard 00:00:04
  Bytes sent (initiator:responder) [140:298] acl created 2
  Outgoing access-list 102 applied to interface FastEthernet0/0
  Inbound access-list 101 applied to interface FastEthernet0/1
```

Step 5 show ip inspect all

Use this command to show all CBAC configuration and all existing sessions that are currently being tracked and inspected by CBAC.

```
Router# show ip inspect all

Session audit trail is disabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
  Inspection name all
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
Interface Configuration
Interface Ethernet0
  Inbound inspection rule is all
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
  Outgoing inspection rule is not set
  Inbound access list is not set
  Outgoing access list is not set
Established Sessions
Session 25A6E1C (30.0.0.1:46065)=>(40.0.0.1:21) ftp SIS_OPEN
Session 25A34A0 (40.0.0.1:20)=>(30.0.0.1:46072) ftp-data SIS_OPEN
```


Configuration Examples for Inspection of Router-Generated Traffic

This section provides the following configuration examples:

- [Configuring CBAC with Inspection of H.323 Traffic: Example, page 9](#)

Configuring CBAC with Inspection of H.323 Traffic: Example

These commands create the ACL. In this example, TCP traffic from subnet 100.168.11.1, 192.168.11.50, and 192.168.100.1 is permitted.

```
access-list 120 permit tcp host 100.168.11.1 any eq 1720
access-list 121 permit tcp host 192.168.11.50 host 100.168.11.1 eq 1720
access-list 121 permit tcp host 192.168.100.1 host 100.168.11.1 eq 1720
```

These commands create the CBAC inspection rule LOCAL-H323, allowing inspection of the protocol traffic specified by the rule. This inspection rule sets the timeout value to 180 seconds for each protocol (except for RPC). The timeout value defines the maximum time that a connection for a given protocol can remain active without any traffic passing through the router. When these timeouts are reached, the dynamic ACLs that are inserted to permit the returning traffic are removed, and subsequent packets (possibly even valid ones) are not permitted.

```
ip inspect name LOCAL-H323 tftp timeout 180
ip inspect name LOCAL-H323 h323 router-traffic timeout 180
```

These commands apply the inspection rule and ACL. In this example, the inspection rule LOCAL-H323 is applied to traffic at interface Serial0/3/0.

```
interface Serial0/3/0
 ip address 11.168.11.2 255.255.255.0
 ip access-group 121 in
 ip access-group 120 out
 ip inspect LOCAL-H323 in
 ip inspect LOCAL-H323 out
 encapsulation frame-relay
 frame-relay map ip 11.168.11.1 168 broadcast
 no frame-relay inverse-arp
 frame-relay intf-type dce
```

Additional References

The following sections provide references related to Inspection of Router-Generated Traffic.

Related Documents

Related Topic	Document Title
CBAC	<i>Cisco IOS Security Configuration Guide</i> , Release 12.3 <i>Cisco IOS Security Command Reference</i> , Release 12.3T
H.323	<i>Cisco IOS H.323 Configuration Guide</i> , Release 12.3

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **ip inspect name**

Glossary

CBAC—Context-Based Access Control. Scrutinizes source and destination addresses to enhance security for TCP and UDP applications that use well-known ports, such as FTP and e-mail traffic.

firewall—One or more router or access servers designated as a buffer between any connected public networks and a private network. A firewall router uses access lists and other methods to ensure the security of the private network.

FTP—File Transfer Protocol. An application protocol, part of the TCP/IP protocol stack, for transferring files between network nodes.

H.323—A multimedia conferencing protocol that includes voice, video, and data conferencing for use over packet-switched networks. H.323 allows dissimilar communication devices to communicate with each other by using a standardized communication protocol.

IMAP—Internet Message Access Protocol. A method of accessing e-mail or bulletin board messages kept on a mail server that can be shared. IMAP permits client e-mail applications to access remote message stores as if they were local without actually transferring the message.

IP—Internet Protocol. Connectionless protocol at the network layer (Layer 3) of the OSI reference model. Provides features for addressing, type-of-service specification, fragmentation and reassemble, and security. IP works with TCP and is usually identified as TCP/IP.

POP—Post Office Protocol. A protocol that client e-mail applications use to retrieve mail from a mail server.

SMTP—Simple Mail Transfer Protocol. A simple ASCII protocol that describes the exchange of e-mail between two message-transfer agents using TCP/IP.

TCP—Transmission Control Protocol. A connection-oriented transport-layer protocol that provides reliable full-duplex data transmissions.

TCP/IP—Transmission Control Protocol/Internet Protocol. Common name for the suite of protocols developed by the U.S. Department of Defense in the 1970s to support the construction of worldwide internetworks. TCP and IP are the two best-known protocols in the suite.

UDP—User Datagram Protocol. A connectionless transport-layer protocol for exchanging datagrams without acknowledgments or guaranteed delivery.

VoIP—Voice over IP. Capability of carrying normal telephony-style voice over an IP network with circuit-based telephone-like functionality, reliability, and voice quality. VoIP generally refers to the Cisco standards-based (H.323 and so forth) approach to IP voice traffic.

**Note**

Refer to [Networking Terms and Acronyms](#) for terms not included in this glossary.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



TCP Out-of-Order Packet Support for Cisco IOS Firewall and Cisco IOS IPS

First Published: November 17, 2006

Last Updated: November 17, 2006

This feature allows out-of-order packets in TCP streams to be cached and reassembled before they are inspected by Cisco IOS Intrusion Prevention System (IPS) or Cisco IOS Firewall.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for TCP Out-of-Order Packet Support for Cisco IOS Firewall and IPS](#)” section on page 8.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for TCP Out-of-Order Packet Support for Cisco IOS Firewall and Cisco IOS IPS, page 2](#)
- [Restrictions for TCP Out-of-Order Packet Support for Cisco IOS Firewall and Cisco IOS IPS, page 2](#)
- [Information About TCP Out-of-Order Packet Support for Cisco IOS Firewall and Cisco IOS IPS, page 2](#)
- [How to Configure Cisco IOS Firewall or IPS to Handle TCP Out-of-Order Packets, page 3](#)
- [Configuration Examples for TCP Out-of-Order Packet Parameters, page 4](#)
- [Additional References, page 5](#)
- [Command Reference, page 6](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Feature Information for TCP Out-of-Order Packet Support for Cisco IOS Firewall and IPS, page 8](#)

Prerequisites for TCP Out-of-Order Packet Support for Cisco IOS Firewall and Cisco IOS IPS

Cisco IOS IPS or Cisco IOS Firewall must be configured on your router.

Restrictions for TCP Out-of-Order Packet Support for Cisco IOS Firewall and Cisco IOS IPS

- The feature is enabled by default. The user must explicitly disable it. To disable TCP out-of-order packet buffering and reassembly, issue the **ip inspect tcp reassembly queue length 0** command.
- Zone-based policy firewall is not supported. Only Cisco IOS IPS and Cisco IOS Firewall application inspection can support out-of-order TCP packets.

Information About TCP Out-of-Order Packet Support for Cisco IOS Firewall and Cisco IOS IPS

Before reassembling TCP out-of-order packets, you should understand the following concept:

- [How TCP Out-of-Order Packet Support Works, page 2](#)

How TCP Out-of-Order Packet Support Works

Cisco IOS Firewall and IPS track packets in TCP connections. If configured to look into the application data of the packets, Cisco IOS Firewall and IPS expect the TCP packets to arrive in the correct order because some data items are split across segments. When packets arrive out of order, they are dropped by the firewall or IPS. Dropping out-of-order packets can cause significant delays in end applications because packets are dropped only after the retransmission timer expires (on behalf of the sender).

Out-of-order TCP packet support enables Cisco IOS Firewall and IPS to hold a copy of the out-of-order packet in a buffer (whose size is configurable with a maximum of 1024 packets per session). The original packet passes through the router and reaches its destination, but the firewall or IPS do not execute on the packet. When the next packet arrives, the firewall or IPS look for that packet to “fill the hole,” providing a consecutive sequence of segments. If this packet does not fulfill that requirement, it is processed as an out-of-order packet; when another packet arrives and provides a consecutive sequence of segments, it is processed by the firewall or IPS.

How to Configure Cisco IOS Firewall or IPS to Handle TCP Out-of-Order Packets

This section contains the following procedure:

- [Changing Default TCP Out-of-Order Packet Parameters, page 3](#)

Changing Default TCP Out-of-Order Packet Parameters

Use this task to change any of the predefined parameters that instruct Cisco IOS Firewall application inspection or Cisco IOS IPS how to handle out-of-order TCP packets.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip inspect tcp reassembly** {[*queue length packet-number*] [*timeout seconds*] [*memory limit size-in-kb*] [*alarm {on | off}*]}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip inspect tcp reassembly {[queue length <i>packet-number</i>] [timeout <i>seconds</i>] [memory limit <i>size-in-kb</i>] [alarm { on off }]} Example: Router(config)# ip inspect tcp reassembly queue length 10 timeout 8	Sets parameters that define how a Cisco IOS IPS handles out-of-order TCP packets. <ul style="list-style-type: none"> queue length <i>packet-number</i>—Maximum number of out-of-order packets that can be held per queue (buffer). Note that there are 2 queues per session. Available value range: 0 to 1024. Default value: 16. If the queue length is set to 0, all out-of-order packets are dropped. timeout <i>seconds</i>—Number of seconds the TCP reassembly module will hold out-of-order segments waiting for the first segment missing in the sequence. After the timeout timer has expired, a retry timer is started. The value for the retry timer is four times the configured timeout value. memory limit <i>size-in-kb</i>—Maximum allowed memory use by the TCP reassembly module. alarm {on off}—If enabled, a syslog message is generated when an out-of-order packet is dropped. Default value: on

Configuration Examples for TCP Out-of-Order Packet Parameters

This sections contains the following configuration example:

- [Verifying TCP Out-of-Order Packets: Example, page 4](#)

Verifying TCP Out-of-Order Packets: Example

The following example shows how to instruct Cisco IOS IPS how to handle out of order packets for TCP connections:

```
Router(config)# ip inspect tcp reassembly queue length 18
Router(config)# ip inspect tcp reassembly memory limit 200
```

The following sample output displays the configured out-of-order packet parameters:

```
Router# show ip ips statistics
```

```
Signature Statistics [process switch:fast switch]
Signature 1000: 324 packets checked: [124:200]
Signature 1024: 100 packets checked: [0:100]
Interfaces configured for ips 0
Session creations since subsystem startup or last reset 0
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [0:0:0]
Last session created never
Last statistic reset never
TCP reassembly statistics
received 200 packets out-of-order; dropped 25
peak memory usage; 200 KB; current usage: 154 KB
peak queue length 18
```

Additional References

The following sections provide references related to the TCP Out-of-Order Packet Support for Cisco IOS Firewall and Cisco IOS IPS feature.

Related Documents

Related Topic	Document Title
IPS configuration	<i>IPS 5.x Signature Format Support and Usability Enhancements</i> , Cisco IOS Release 12.4(11)T feature module
Firewall configuration	<i>Cisco IOS Security Configuration Guide</i>
Firewall IPS commands	Cisco IOS Security Command Reference

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and technical documentation. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information

about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **ip inspect tcp reassembly**

Feature Information for TCP Out-of-Order Packet Support for Cisco IOS Firewall and IPS

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for TCP Out-of-Order Support

Feature Name	Releases	Feature Information
TCP Out-of-Order Packet Support for Cisco IOS Firewall and Cisco IOS IPS	12.4(11)T	This feature allows out-of-order packets in TCP streams to be cached and reassembled before they are inspected by Cisco IOS Intrusion Prevention System (IPS) or Cisco IOS Firewall.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Transparent Cisco IOS Firewall

The Transparent Cisco IOS Firewall feature allows users to “drop” a Cisco IOS Firewall in front of their existing network without changing the statically defined IP addresses of their network-connected devices. Thus, users can allow selected devices from a subnet to traverse the firewall while access to other devices on the same subnet is denied.

Feature History for Transparent Cisco IOS Firewall

Release	Modification
12.3(7)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions for Transparent Cisco IOS Firewall, page 2](#)
- [Information About Transparent Cisco IOS Firewall, page 2](#)
- [How to Configure a Transparent Cisco IOS Firewall, page 3](#)
- [Configuration Examples for Transparent Cisco IOS Firewall, page 9](#)
- [Additional References, page 17](#)
- [Command Reference, page 19](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Restrictions for Transparent Cisco IOS Firewall

Layer 3 IP Packet Support Only

Only IP packets (TCP, User Datagram Protocol [UDP], and Internet Control Message Protocol [ICMP]) are subjected to inspection by the transparent firewall. Non-IP traffic is bridged as usual without interference from the transparent firewall. However, if users wish to block non-IP traffic, the MAC access control lists (ACLs) can be applied on interfaces to filter out non-IP traffic and allow only IP traffic.

The following example shows how to configure an ACL that permits all IP packets (0x0800) into the Ethernet interface but denies all Internetwork Packet Exchange (IPX) packets (0x8137):

```
Router(config)# access-list 201 permit 0x0800
Router(config)# access-list 201 deny 0x8137
Router(config)# interface ethernet 0
Router(config-if)# bridge-group 1 input-type-list 201
```

VLAN Trunk Bridging

Bridging between VLAN trunks works only for dot1q encapsulation; Inter-Switch Link (ISL) encapsulation will not work. (However, ISL VLANs will work if subinterfaces are created and placed in a bridge group.)

Information About Transparent Cisco IOS Firewall

To use a transparent Cisco IOS Firewall in your network, you should understand the following concepts:

- [Benefit of the Transparent Firewall, page 2](#)
- [Transparent Firewall Overview, page 2](#)
- [Layer 2 and Layer 3 Firewalls Configured on the Same Router, page 3](#)

Benefit of the Transparent Firewall

Added Security with Minimum Configuration

Users can simply drop a transparent Cisco IOS Firewall into an existing network without having to reconfigure their statically defined devices. Thus, the tedious and costly overhead that is required to renumber devices on the trusted network is eliminated.

Transparent Firewall Overview

A typical Cisco IOS Firewall is a Layer 3 device with trusted and untrusted interfaces on different IP subnets. A Layer 3 firewall works well with Cisco IOS devices that function as routers with preexisting subnet separations. However, when a Layer 3 firewall is placed in an existing network, the network IP addresses must be reconfigured to accommodate the firewall.

A transparent Cisco IOS firewall acts as a Layer 2 transparent bridge with context-based access control (CBAC) and ACLs configured on the bridged interface. Because the Layer 2 firewall intercepts packets at Layer 2 and is “transparent” to the existing network, Layer 3 firewall limitations are not applicable.

Transparent Bridging Overview

If configured for bridging, a Cisco IOS device can bridge any number of interfaces. The device can complete basic bridging tasks such as learning MAC addresses on ports to restrict collision domains and running Spanning Tree Protocol (STP) to prevent looping in the topology.

Within bridging, a user can configure Integrated Routed Bridging (IRB), which allows a device to bridge on some interfaces while a Layer 3 Bridged Virtual Interface (BVI) is presented for routing. The bridge can determine whether the packet is to be bridged or routed on the basis of the destination of the Layer 2 or Layer 3 IP address in the packet. Configured with an IP address, the BVI can manage the device even if there is no interface configured for routing.

Layer 2 and Layer 3 Firewalls Configured on the Same Router

A transparent firewall supports a BVI for routing, so a packet that comes in on a bridged interface can be bridged or routed out of the BVI. This functionality allows a Layer 2 (transparent) firewall and a Layer 3 firewall to be configured on the same router: The transparent firewall operates on the bridged packets while the “normal” firewall operates on the routed packets. For example, if you have six interfaces on your router and two of them are in a bridge group, you can simultaneously configure and run normal inspection on the remaining four interfaces.

How to Configure a Transparent Cisco IOS Firewall

You configure a transparent firewall just as you would configure a Layer 3 firewall (via the **ip inspect** command, which can be configured on any of the bridged interfaces for the transparent firewall). Also, you configure transparent bridging for a firewall just as you would for any other Cisco IOS device.

This section contains the following procedures:

- [Configuring a Bridge Group, page 3](#) (required)
- [Configuring Inspection and ACLs, page 6](#) (required)
- [Forwarding DHCP Traffic, page 8](#) (optional)
- [Monitoring Transparent Firewall Events, page 8](#) (optional)

Configuring a Bridge Group

Use this task to configure a bridge group and to associate interfaces or subinterfaces in the configured bridge group.

BVI Configuration Requirements

- If a BVI is not configured, you must disable IP routing (via the **no ip routing** command) for the bridging operation to take effect.
- If configured, a BVI must be configured with an IP address in the same subnet.
- You *must* configure a BVI if more than two interfaces are placed in a bridge group.

Restrictions

- If more than two interfaces are assigned to a bridge group, any routers that are acting as first-hop gateways to hosts that are in the bridged network (the bridge group) must allow ICMP time-to-live (TTL) exceeded messages to pass.
- Spanning Tree Bridge Protocol Data Units (BPDU) and packets that are to be routed out of the bridge, if IRB is configured, are not inspected.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bridge *bridge-group* protocol {dec | ibm | ieee | vlan-bridge}**
4. **interface *type number***
5. **bridge-group *bridge-group***
6. **exit**
7. **bridge irb**
8. **bridge *bridge-group* route protocol**
9. **interface *type number***
10. **ip address *ip-address mask***
11. **no shutdown**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	bridge <i>bridge-group</i> protocol {dec ibm ieee vlan-bridge} Example: Router(config)# bridge 1 protocol ieee	Defines the type of Spanning Tree Protocol (STP).
Step 4	interface <i>type number</i> Example: Router(config)# interface Ethernet0	Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 5	bridge-group <i>bridge-group</i> Example: Router(config-if)# bridge-group 1	Assigns each network interface to a bridge group. Note Complete Step 4 and Step 5 for each interface you want to assign to a bridge group. Note You can also assign subinterfaces to a bridge group to control bridging between VLANs.
Step 6	exit	Exits interface configuration mode.
Step 7	bridge irb Example: Router(config)# bridge irb	Enables the Cisco IOS software to route a given protocol between routed interfaces and bridge groups or to route a given protocol between bridge groups. Note Step 7 through Step 11 are necessary only if you want to configure a BVI.
Step 8	bridge <i>bridge-group</i> route <i>protocol</i> Example: Router(config)# bridge 1 route ip	Enables the routing of a specified protocol in a specified bridge group.
Step 9	interface <i>type number</i> Example: Router(config)# interface BVI1	Configures a BVI and enters interface configuration mode.
Step 10	ip address <i>ip-address mask</i> Example: Router(config-if) ip address 10.1.1.1 255.255.255.0	Sets a primary IP address for an interface.
Step 11	no shutdown Example: Router(config-if)# no shutdown	Restarts a disabled interface.

Examples

The following example shows how to configure interfaces “ethernet0” and “ethernet1” in a bridge group. These interfaces are associated with the BVI interface “BVI1,” which can be reached from any host on either of the interfaces via the IP address 10.1.1.1.

```
Router(config)# bridge 1 protocol ieee
Router(config)# interface ethernet0
Router(config-if)# bridge-group 1
Router(config-if)# interface ethernet1
Router(config-if)# bridge-group 1
Router(config-if)# exit
! Configure the BVI.
Router(config)# bridge irb
Router(config)# bridge 1 route ip
Router(config)# interface BVI1
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# no shutdown
```

Troubleshooting Tips

To display the status of each bridge group, use the **show bridge-group** command or to display entries in the bridge table, use the **show bridge** command.

What to Do Next

After you have configured the bridge group, you must configure an inspection rule and at least one IP ACL. To complete this task, refer to the following section, “[Configuring Inspection and ACLs](#).”



Note

If inspection is not configured on any interface in the bridge group, IP ACLs on bridged interfaces will not be active.

Configuring Inspection and ACLs

Use this task to configure an inspection rule and apply it on the appropriate interface. Also, use this task to configure at least one ACL and apply it on one or more of the interfaces that you configured in the bridge group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip inspect name** *protocol* [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*]
4. **interface** *type number*
5. **ip inspect** *inspection-name* {**in** | **out**}
6. **exit**
7. **access-list** *access-list-number* {**permit** | **deny**} {*type-code wild-mask* | *address mask*}
8. **interface** *type number*
9. **ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	ip inspect name protocol [alert {on off}] [audit-trail {on off}] [timeout seconds] Example: Router(config)# ip inspect name test tcp	Defines a set of inspection rules.
Step 4	interface type number Example: Router(config)# interface Ethernet0	Configures an interface type and enters interface configuration mode.
Step 5	ip inspect inspection-name {in out} Example: Router(config-if)# ip inspect test in	Applies a set of inspection rules to an interface.
Step 6	exit	Exits interface configuration mode.
Step 7	access-list access-list-number {permit deny} {type-code wild-mask address mask} Example: Router(config)# access-list 156 permit 10.1.1.0 0.0.0.255 any	Configures the ACL. Note Repeat this step for each ACL that you want to configure.
Step 8	interface type number Example: Router(config)# interface Ethernet0	Configures an interface type and enters interface configuration mode. Note Repeat Steps 8 and 9 for each ACL that you want to apply to inbound packets from a specific interface.
Step 9	ip access-group {access-list-number access-list-name} {in out} Example: Router(config-if) ip access-group 156 in	Controls access to an interface.

Examples

The following example shows how to configure an inspection rule on interface “ethernet0,” which is the inside interface. Policies can be specified via ACL 156 or 101; for example, ACL 156 can be used to specify that rlogin and rsh are not allowed for the internal users, and ACL 101 can be used to specify that an external host requires connectivity to a particular host in the internal domain.

```
Router(config)# ip inspect name test tcp
Router(config)# interface ethernet0
Router(config-if)# ip inspect test in
Router(config-if)# exit
!
! Configure the ACLs.
Router(config)# access-list 101 deny ip any any
Router(config)# access-list 156 permit 10.1.1.0 0.0.0.255 any
Router(config)# access-list 156 deny ip any any

Router(config)# interface ethernet0
Router(config-if) ip access-group 156 in
```

```
Router(config)# interface ethernet1
Router(config-if) ip access-group 101 in
```

Forwarding DHCP Traffic

Use this task to enable a transparent firewall to forward DHCP packets across the bridge without inspection; that is, the **ip inspect L2-transparent dhcp-passthrough** command overrides the ACL for DHCP packets, so DHCP packets will be forwarded even if the ACL is configured to deny all IP packets. Thus, clients on one side of the bridge can get an IP address from a DHCP server on the opposite side of the bridge.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip inspect L2-transparent dhcp-passthrough**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip inspect L2-transparent dhcp-passthrough Example: Router#(config) ip inspect L2-transparent dhcp-passthrough	Allows a transparent firewall to forward DHCP passthrough traffic.

Monitoring Transparent Firewall Events

Use either of these optional steps to monitor the activity of the transparent firewall.



Note

Effective with Cisco IOS Release 12.4(20)T, the **debug ip inspect** command is replaced by the **debug policy-firewall** command. See the *Cisco IOS Debug Command Reference* for more information.

SUMMARY STEPS

1. **enable**
2. **debug ip inspect L2-transparent {packet | dhcp-passthrough}**

3. `show ip inspect {name inspection-name | config | interfaces | session [detail] | all}`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	debug ip inspect L2-transparent {packet dhcp-passthrough} Example: Router# debug ip inspect L2-transparent dhcp-passthrough	Enables debugging messages for transparent firewall events. <ul style="list-style-type: none"> packet—Displays messages for all debug packets that are inspected by the transparent firewall. dhcp-passthrough—Displays debug messages only for DHCP pass-through traffic that the transparent firewall forwards across the bridge.
Step 3	show ip inspect {name <i>inspection-name</i> config interfaces session [detail] all} Example: Router# show ip inspect all	Displays Cisco IOS Firewall configuration and session information. <ul style="list-style-type: none"> If the transparent firewall is configured, use the all keyword to display the bridging interface in the interface configuration section of the output.

Examples

The following sample output is a portion of the **show ip inspect all** command that shows the bridging interface:

```
Router# show ip inspect all
.
.
.
Interface Configuration
! Below is the bridging interface.
Interface Ethernet1
Inbound inspection rule is test
tcp alert is on audit-trail is off timeout 3600
ftp alert is on audit-trail is off timeout 3600
Outgoing inspection rule is not set
Inbound access list is not set
Outgoing access list is 156
.
.
.
```

Configuration Examples for Transparent Cisco IOS Firewall

This section contains the following configuration examples:

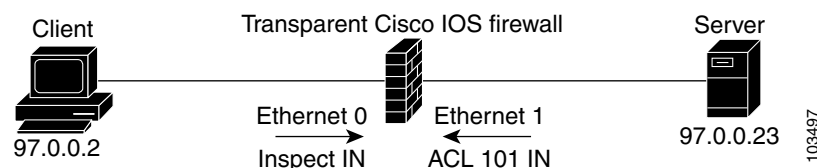
- [Comprehensive Transparent Firewall Configuration: Example, page 10](#)
- [Monitoring Telnet Connections via debug and show Output: Examples, page 12](#)

- [Configuring and Verifying DHCP Pass-Through Traffic: Examples, page 16](#)

Comprehensive Transparent Firewall Configuration: Example

The following example and sample topology (see [Figure 1](#)) illustrate how to configure and debug a transparent Cisco IOS Firewall configuration between a client, a firewall, and a server. This example also includes **show** command output for additional configuration verification. After you have configured a transparent firewall, you can Telnet from the client to the server through the firewall. (See the section “[Monitoring Telnet Connections via debug and show Output: Examples.](#)”

Figure 1 Sample Topology for Transparent Firewall Configuration



Note

Effective with Cisco IOS Release 12.4(20)T, the **debug ip inspect** command is replaced by the **debug policy-firewall** command. See the *Cisco IOS Debug Command Reference* for more information.

```

! Enable debug commands.
Router# debug ip inspect L2-transparent packet
INSPECT L2 firewall debugging is on
Router# debug ip inspect object-creation
INSPECT Object Creations debugging is on
Router# debug ip inspect object-deletion
INSPECT Object Deletions debugging is on
! Start the transparent firewall configuration process
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
! Configure bridging
Router(config)# bridge 1 protocol ieee
Router(config)# bridge irb
Router(config)# bridge 1 route ip
Router(config)# interface bvi1
*Mar 1 00:06:42.511:%LINK-3-UPDOWN:Interface BVI1, changed state to down.
Router(config-if)# ip address 209.165.200.225 255.255.255.254
! Configure inspection
Router(config)# ip inspect name test tcp
! Following debugs show the memory allocated for CBAC rules.
*Mar 1 00:07:21.127:CBAC OBJ_CREATE:create irc 817F04F0 (test)
*Mar 1 00:07:21.127:CBAC OBJ_CREATE:create irt 818AED20 Protocol:tcp Inactivity time:0
test
Router(config)# ip inspect name test icmp
Router(config)#
*Mar 1 00:07:39.211:CBAC OBJ_CREATE:create irt 818AEDCC Protocol:icmp Inactivity time:0
! Configure Bridging on ethernet0 interface
Router(config)# interface ethernet0
Router(config-if)# bridge-group 1
*Mar 1 00:07:49.071:%LINK-3-UPDOWN:Interface BVI1, changed state to up
*Mar 1 00:07:50.071:%LINEPROTO-5-UPDOWN:Line protocol on Interface BVI1, changed state to up
! Configure inspection on ethernet0 interface
Router(config-if)# ip inspect test in
Router(config-if)#
  
```



```
*Mar  1 00:07:57.543:CBAC OBJ_CREATE:create idbsb 8189CBFC (Ethernet0)

! Incremented the number of bridging interfaces configured for inspection
*Mar  1 00:07:57.543:L2FW:Incrementing L2FW i/f count
Router(config-if)# interface ethernet1
! Configure bridging and ACL on interface ethernet1
Router(config-if)# bridge-group 1
Router(config-if)# ip access-group 101 in
*Mar  1 00:08:26.711:%LINEPROTO-5-UPDOWN:Line protocol on Interface Ethernet1, changed
state to up
Router(config-if)# end
Router(config)# end
!
! Issue the show running-config command to verify the complete transparent firewall
! configuration.
Router# show running-config
Building configuration...

Current configuration :1126 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Firewall
!
logging buffered 12000 debugging
no logging console
!
no aaa new-model
ip subnet-zero
no ip domain lookup
!
!
ip inspect name test tcp
ip inspect name test icmp
ip audit notify log
ip audit po max-events 100
no ftp-server write-enable
!
!
no crypto isakmp enable
!
!
bridge irb
!
!
interface Ethernet0
  no ip address
  no ip proxy-arp
  ip inspect test in
  bridge-group 1
  hold-queue 100 out
!
interface Ethernet1
  no ip address
  ip access-group 101 in
  no ip unreachable
  no ip proxy-arp
  duplex auto
  bridge-group 1
```

```

!
interface BVI1
 ip address 209.165.200.225 255.255.255.254
!
ip classless
ip route 9.1.0.0 255.255.0.0 9.4.0.1
no ip http server
no ip http secure-server
!
!
ip access-list log-update threshold 1
access-list 101 permit icmp any any log
access-list 101 deny ip any any log
!
control-plane
!
bridge 1 protocol ieee
bridge 1 route ip
!
line con 0
 no modem enable
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
scheduler max-task-time 5000
!
end
!
! Issue show bridge commands to check the tables.
Router# show bridge

Total of 300 station blocks, 300 free
Codes:P - permanent, S - self

Bridge Group 1:

! The bridge table is empty because no traffic has been seen
!
Router# show bridge group

Bridge Group 1 is running the IEEE compatible Spanning Tree protocol

Port 2 (Ethernet0) of bridge group 1 is forwarding
Port 3 (Ethernet1) of bridge group 1 is forwarding
! Note that the interfaces are in a "forwarding" state. The interfaces move from
! a listening state to a learning state and finally to a forwarding state. It takes
! approximately 30 seconds to move to a forwarding after "bridge-group 1" is configured.

```

Monitoring Telnet Connections via debug and show Output: Examples

The following examples shows how to monitor established Telnet connections from the client to the server through the firewall (see [Figure 1](#)) and from the server to the client. In these example, the **debug ip inspect L2-transparent packet** command has been issued to generate the debug messages. Relevant **show** commands are also issued for additional verification.

**Note**

Effective with Cisco IOS Release 12.4(20)T, the **debug ip inspect** command is replaced by the **debug policy-firewall** command. See the *Cisco IOS Debug Command Reference* for more information.

- [Telnet Connection from the Client \(97.0.0.2\) to the Server \(97.0.0.23\), page 13](#)
- [Telnet Connection from the Server \(97.0.0.23\) to the Client \(97.0.0.2\), page 15](#)

Telnet Connection from the Client (97.0.0.2) to the Server (97.0.0.23)

The following example is output from the initial Telnet connection between the client and the server. A subsequent connection is established to highlight differences in the debug output. Explanations are given inline.

```
! A packet is received by the firewall in the flood path because the bridge-table is
! initially empty. However, the client seems to have the server's mac-address in its ARP
! cache, so the bridge floods the packet and it appears in the firewall's "flood" path.
*Mar 1 00:17:32.119:L2FW:insp_l2_flood:input is Ethernet0 output is Ethernet1
! Source and destination IP addresses and the L4 protocol of the packet
*Mar 1 00:17:32.123:L2FW*:Src 97.0.0.2 dst 97.0.0.23 protocol tcp
! ACL processing status. An ACL is not configured in this direction; that is, from the
! client to the server.
*Mar 1 00:17:32.123:L2FW:Input ACL not configured or the ACL is bypassed
*Mar 1 00:17:32.123:L2FW:Output ACL is not configured or ACL is bypassed
! If there are exactly two interfaces in the bridge-group and the packet is in flood path,
! the firewall invokes inspection directly, skipping the Unicast flood algorithm. If there
! are more than 2 interfaces, the firewall "drops" the packet and issues the algorithm.
*Mar 1 00:17:32.123:L2FW:FLOOD number of i/fs in bridge-group is exactly 2. Calling
Inspection
! The packet is being inspected.
*Mar 1 00:17:32.123:L2FW:insp_l2_inspection:input is Ethernet0 output is Ethernet1
*Mar 1 00:17:32.123:L2FW*:Src 97.0.0.2 dst 97.0.0.23 protocol tcp
*Mar 1 00:17:32.123:L2FW:Input ACL not configured or the ACL is bypassed
*Mar 1 00:17:32.123:L2FW:Output ACL is not configured or ACL is bypassed

! Memory is allocated for the transparent firewall attributes in the session structure
*Mar 1 00:17:32.123:L2FW:allocating L2 extension for sis
! CBAC-related debug messages: The packet has been passed to the existing CBAC code.
*Mar 1 00:17:32.123:CBAC Pak 814635DC sis 816C9C24 initiator_addr (97.0.0.2:11016)
responder_addr (97.0.0.23:23)
initiator_alt_addr (97.0.0.2:11016) responder_alt_addr (97.0.0.23:23)
! CBAC session structure has been allocated
*Mar 1 00:17:32.127:CBAC OBJ_CREATE:create sis 816C9C24
*Mar 1 00:17:32.127:CBAC OBJ_CREATE:sid 816D69D8 acl 101 Prot:tcp
*Mar 1 00:17:32.127: Src 97.0.0.23 Port [23:23]
*Mar 1 00:17:32.127: Dst 97.0.0.2 Port [11016:11016]
! The Layer 2 header length is being computed for caching the L2 header, which will be
! used if a TCP RST should be sent in the future to tear down the connection.
*Mar 1 00:17:32.127:L2FW:L2 header length(initiator->responder) is 14
! Checks to see if the header is 802.3, SNAP, SAP. (This header is 802.3.)
*Mar 1 00:17:32.127:L2FW:info_start is NULL for init->rsp
*Mar 1 00:17:32.127:CBAC OBJ_CREATE:create host entry 816D4018 addr 97.0.0.23 bucket 118
! CBAC has indicated that the packet should be passed
*Mar 1 00:17:32.127:L2FW:insp_inspection returned FALSE. PASS

! The next packet in the flow has arrived on the interrupt path. This packet is from the
! server (ethernet1) to the client (ethernet0).
*Mar 1 00:17:32.131:L2FW*:insp_l2_fast_inspection:pak 812C9084, input-interface
Ethernet1, output-interface Ethernet0
*Mar 1 00:17:32.131:L2FW*:Src 97.0.0.23 dst 97.0.0.2 protocol tcp
*Mar 1 00:17:32.131:L2FW:Input ACL not configured or the ACL is bypassed
```

```

*Mar 1 00:17:32.131:L2FW:Output ACL is not configured or ACL is bypassed
! The Layer 2 header length is computed and will be cached
*Mar 1 00:17:32.131:L2FW:L2 header length is 14 (rsp->init)
*Mar 1 00:17:32.131:L2FW:info_start is NULL rsp->init
! CBAC has indicated that the packet should be forwarded
*Mar 1 00:17:32.131:L2FW*:insp_l2_fast_inspection returning INSP_L2_OK
! A new packet has arrived from the client. The following trace repeats for each packet
received by the firewall
*Mar 1 00:17:32.135:L2FW*:insp_l2_fast_inspection:pak 81462FB4, input-interface
Ethernet0, output-interface Ethernet1
*Mar 1 00:17:32.135:L2FW*:Src 97.0.0.2 dst 97.0.0.23 protocol tcp
*Mar 1 00:17:32.135:L2FW:Input ACL not configured or the ACL is bypassed
*Mar 1 00:17:32.135:L2FW:Output ACL is not configured or ACL is bypassed
*Mar 1 00:17:32.135:L2FW*:insp_l2_fast_inspection returning INSP_L2_OK
...<more packets >...
! The host entry for the server is deleted.
*Mar 1 00:17:32.263:CBAC OBJ_DELETE:delete host entry 816D4018 addr 97.0.0.23

! Issue the show ip inspect command to verify that a CBAC session has been established
Router# show ip inspect session detailed

Established Sessions
  Session 816C9C24 (97.0.0.2:11016)=>(97.0.0.23:23) tcp SIS_OPEN
    Created 00:00:28, Last heard 00:00:09
    Bytes sent (initiator:responder) [38:75]
    In SID 97.0.0.23[23:23]=>97.0.0.2[11016:11016] on ACL 101 (12 matches)
Router#
!
! Issue the show bridge command to verify that entries for the client and server have been
! created in the bridge-table.
Router# show bridge

Total of 300 station blocks, 298 free
Codes:P - permanent, S - self

Bridge Group 1:

      Address      Action   Interface   Age    RX count  TX count
0008.a3b6.b603    forward Ethernet0     2         14      12
0007.0d97.308f    forward Ethernet1     2         12      13
Router#
!
! Close the TCP connection (by typing exit at the client).
*Mar 1 00:21:26.259:CBAC OBJ_DELETE:delete sis 816C9C24
*Mar 1 00:21:26.259:CBAC OBJ_DELETE:sid 816D69D8 on acl 101 Prot:tcp
*Mar 1 00:21:26.259: Src 97.0.0.23 Port [23:23]
*Mar 1 00:21:26.259: Dst 97.0.0.2 Port [11016:11016]
! The data structures pertaining to the Layer 2 firewall have been deleted from the
! session. The session has also been deleted.
*Mar 1 00:21:26.259:L2FW:Deleting L2FW data structures

```

A New Telnet Connection from the Client (97.0.0.2) to the Server (97.0.0.23)

```

! The initial SYN packet from the client has arrived in the interrupt path. Note that the
! corresponding packet from the previous telnet session came in on the flood path because
! the bridge-table was empty so the bridge was forced to flood the packet. Since the
! bridge-table is now populated, the packet does not not to be flooded. This is the only
! difference between the previous telnet session and this session. Subsequent packets will
! follow the same path (and generate the same debugs) as the previous session.
*Mar 1 00:23:31.883:L2FW*:insp_l2_fast_inspection:pak 81465190, input-interface
Ethernet0, output-interface Ethernet1
*Mar 1 00:23:31.883:L2FW*:Src 97.0.0.2 dst 97.0.0.23 protocol tcp
*Mar 1 00:23:31.883:L2FW:Input ACL not configured or the ACL is bypassed
*Mar 1 00:23:31.883:L2FW:Output ACL is not configured or ACL is bypassed

```

```

! CBAC has indicated that the packet should be punted to the process path since memory
! allocation and the control-plane is involved
*Mar 1 00:23:31.883:L2FW*:insp_l2_fast_inspection returning INSP_L2_PUNT

! After being punted from the interrupt path, the packet has arrived at the process level
! for inspection. Moving forward, the debug messages are similar to the flood case in the
! previous session.
*Mar 1 00:23:31.883:L2FW:insp_l2_inspection:input is Ethernet0 output is Ethernet1
*Mar 1 00:23:31.883:L2FW*:Src 97.0.0.2 dst 97.0.0.23 protocol tcp
*Mar 1 00:23:31.883:L2FW:Input ACL not configured or the ACL is bypassed
*Mar 1 00:23:31.883:L2FW:Output ACL is not configured or ACL is bypassed
*Mar 1 00:23:31.887:L2FW:allocating L2 extension for sis
*Mar 1 00:23:31.887:CBAC Pak 81465190 sis 816C9C24 initiator_addr (97.0.0.2:11017)
responder_addr (97.0.0.23:23)
initiator_alt_addr (97.0.0.2:11017) responder_alt_addr (97.0.0.23:23)
*Mar 1 00:23:31.887:CBAC OBJ_CREATE:create sis 816C9C24
*Mar 1 00:23:31.887:CBAC OBJ_CREATE:sid 816D69D8 acl 101 Prot:tcp
*Mar 1 00:23:31.887: Src 97.0.0.23 Port [23:23]
*Mar 1 00:23:31.887: Dst 97.0.0.23 Port [11017:11017]
*Mar 1 00:23:31.887:L2FW:L2 header length(initiator->responder) is 14
*Mar 1 00:23:31.887:L2FW:info_start is NULL for init->rsp
*Mar 1 00:23:31.887:CBAC OBJ_CREATE:create host entry 816D4018 addr 97.0.0.23 bucket 118
! CBAC has indicated that the packet should be Passed
*Mar 1 00:23:31.891:L2FW:insp_inspection returned FALSE. PASS
!
! Issue the show ip inspect command to verify the newly created inspect session
Router# show ip inspect session details
Established Sessions
  Session 816C9C24 (97.0.0.2:11017)=>(97.0.0.23:23) tcp SIS_OPEN
    Created 00:00:52, Last heard 00:00:37
    Bytes sent (initiator:responder) [38:75]
    In SID 97.0.0.23[23:23]=>97.0.0.2[11017:11017] on ACL 101 (10 matches)
Router#

```

Telnet Connection from the Server (97.0.0.23) to the Client (97.0.0.2)

The following sample output is from a Telnet connection that was initiated from the server to the client. This connection will not go through because “ACL 101” is configured to allow only ICMP packets and deny all other packets. Note that inspection is not configured from the server to the client. This example is shown to display the debug messages that are associated with dropped packets.

```

! The first packet from the server comes in on ethernet1 interface
*Mar 1 00:26:12.367:L2FW*:insp_l2_fast_inspection:pak 815C89FC, input-interface
Ethernet1, output-interface Ethernet0
*Mar 1 00:26:12.367:L2FW*:Src 97.0.0.23 dst 97.0.0.2 protocol tcp
! This packet is punted up since ACL 101 is configured for logging. Logging happens in the
process path. If logging was not configured, the packet would have been dropped instead of
being punted to process level
*Mar 1 00:26:12.367:L2FW:Packet punted up by Input ACL for logging
! The packet arrives at process level
*Mar 1 00:26:12.367:L2FW:insp_l2_inspection:input is Ethernet1 output is Ethernet0
*Mar 1 00:26:12.371:L2FW*:Src 97.0.0.23 dst 97.0.0.2 protocol tcp
! The ACL log is generated
*Mar 1 00:26:12.371:%SEC-6-IPACCESSLOGP:list 101 denied tcp 97.0.0.23(11045) ->
97.0.0.2(23), 1 packet
! The packet is dropped by the ACL
*Mar 1 00:26:12.371:L2FW:Packet processed and dropped by Input ACL
! The packet is dropped by the ACL and is therefore NOT sent to CBAC for inspection
*Mar 1 00:26:12.371:L2FW:Packet is dropped in insp_l2_inspection

```

Configuring and Verifying DHCP Pass-Through Traffic: Examples

The following examples show how to verify (via debug messages) DHCP pass-through that has been allowed and traffic that has not been allowed.

- [Allowing DHCP Pass-Through Traffic: Example, page 16](#)
- [Denying DHCP Pass-Through Traffic: Example, page 17](#)

Allowing DHCP Pass-Through Traffic: Example

In this example, the static IP address of the client is removed and the address is acquired via DHCP using the **ip address dhcp** command on the interface that is connected to the transparent firewall.

```
Router# show debug
ARP:
  ARP packet debugging is on
L2 Inspection:
  INSPECT L2 firewall debugging is on
  INSPECT L2 firewall DHCP debugging is on
Router#
Router#
! Configure DHCP passthrough
Router(config)# ip insp L2-transparent dhcp-passthrough
! The DHCP discover broadcast packet arrives from the client. Since this packet is a
! broadcast (255.255.255.255), it arrives in the flood path
*Mar 1 00:35:01.299:L2FW:insp_l2_flood:input is Ethernet0 output is Ethernet1
*Mar 1 00:35:01.299:L2FW*:Src 0.0.0.0 dst 255.255.255.255 protocol udp
*Mar 1 00:35:01.299:L2FW:udp ports src 68 dst 67
*Mar 1 00:35:01.299:L2FW:src 0.0.0.0 dst 255.255.255.255
! The DHCP pass through flag is checked and the packet is allowed
*Mar 1 00:35:01.299:L2FW:DHCP packet seen. Pass-through flag allows the packet
! The packet is a broadcast packet and therefore not sent to CBAC
*Mar 1 00:35:01.299:L2FW*:Packet is broadcast or multicast.PASS
! The DHCP server 97.0.0.23 responds to the client's request
*Mar 1 00:35:01.303:L2FW:insp_l2_flood:input is Ethernet1 output is Ethernet0
*Mar 1 00:35:01.303:L2FW*:Src 97.0.0.23 dst 255.255.255.255 protocol udp
*Mar 1 00:35:01.307:L2FW:udp ports src 67 dst 68
*Mar 1 00:35:01.307:L2FW:src 97.0.0.23 dst 255.255.255.255
*Mar 1 00:35:01.307:L2FW:DHCP packet seen. Pass-through flag allows the packet
*Mar 1 00:35:01.307:L2FW*:Packet is broadcast or multicast.PASS
*Mar 1 00:35:01.311:L2FW:insp_l2_flood:input is Ethernet0 output is Ethernet1
*Mar 1 00:35:01.311:L2FW*:Src 0.0.0.0 dst 255.255.255.255 protocol udp
*Mar 1 00:35:01.311:L2FW:udp ports src 68 dst 67
*Mar 1 00:35:01.311:L2FW:src 0.0.0.0 dst 255.255.255.255
*Mar 1 00:35:01.315:L2FW:DHCP packet seen. Pass-through flag allows the packet
*Mar 1 00:35:01.315:L2FW*:Packet is broadcast or multicast.PASS
*Mar 1 00:35:01.315:L2FW:insp_l2_flood:input is Ethernet1 output is Ethernet0
*Mar 1 00:35:01.323:L2FW*:Src 97.0.0.23 dst 255.255.255.255 protocol udp
*Mar 1 00:35:01.323:L2FW:udp ports src 67 dst 68
*Mar 1 00:35:01.323:L2FW:src 97.0.0.23 dst 255.255.255.255
*Mar 1 00:35:01.323:L2FW:DHCP packet seen. Pass-through flag allows the packet
*Mar 1 00:35:01.323:L2FW*:Packet is broadcast or multicast.PASS
! The client has an IP address (97.0.0.5) and has issued a G-ARP to let everyone know it's
address
*Mar 1 00:35:01.327:IP ARP:rcvd rep src 97.0.0.5 0008.a3b6.b603, dst 97.0.0.5 BVI1
Router#
```

Denying DHCP Pass-Through Traffic: Example

In this example, DHCP pass-through traffic is not allowed (via the **no ip inspect L2-transparent dhcp-passthrough** command). The client is denied when it attempts to acquire a DHCP address from the server.

```
! Deny DHCP pass-through traffic
Router(config)# no ip inspect L2-transparent dhcp-passthrough
! The DHCP discover broadcast packet arrives from the client
*Mar  1 00:36:40.003:L2FW:insp_l2_flood:input is Ethernet0 output is Ethernet1
*Mar  1 00:36:40.003:L2FW*:Src 0.0.0.0 dst 255.255.255.255 protocol udp
*Mar  1 00:36:40.003:L2FW:udp ports src 68 dst 67
*Mar  1 00:36:40.007:L2FW:src 0.0.0.0 dst 255.255.255.255
! The pass-through flag is checked
*Mar  1 00:36:40.007:L2FW:DHCP packet seen. Pass-through flag denies the packet
! The packet is dropped because the flag does not allow DHCP passthrough traffic. Thus,
! the client cannot acquire an address, and it times out
*Mar  1 00:36:40.007:L2FW:FLOOD Dropping the packet after ACL check.
Router#
```

Additional References

The following sections provide references related to Transparent Cisco IOS Firewall.

Related Documents

Related Topic	Document Title
Cisco IOS Firewall commands	<i>Cisco IOS Security Command Reference, Release 12.3 T</i>
Additional Cisco IOS Firewall configuration information	<i>The section “Traffic Filtering and Firewalls” of the Cisco IOS Security Configuration Guide</i>
Bridging commands	<i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2: Bridging, Release 12.3 T</i>
Additional bridging configuration information	<i>The section “Bridging” of the Cisco IOS Bridging and IBM Networking Configuration Guide</i>
DHCP configuration information	The chapter “Configuring DHCP” in the <i>Cisco IOS IP Configuration Guide</i>

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **ip inspect L2-transparent dhcp-passthrough**
- **debug ip inspect L2-transparent**

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



User-Based Firewall Support

First Published: July 11, 2008

Last Updated: July 11, 2008

Firewalls traditionally apply rules based on source and destination IP addresses. In the new, highly dynamic mobile world, IP addresses of end systems constantly change. Therefore it becomes increasingly difficult to have a particular user group function assigned to a particular block of IP addresses. It is also difficult to apply firewall policies for a user group that is the source of the traffic. This feature allows source IP addresses to be associated with user groups. Network administrators can apply firewall policies based on user-groups, and the infrastructure can seamlessly apply these security policies.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for User-Based Firewall Support”](#) section on page 28.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for User-Based Firewall Support, page 2](#)
- [Restrictions for User-Based Firewall Support, page 2](#)
- [Information About User-Based Firewall Support, page 2](#)
- [How to Configure User-Based Firewall Support, page 5](#)
- [Configuration Examples for User-Based Firewall Support, page 24](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008 Cisco Systems, Inc. All rights reserved.

- [Additional References, page 26](#)
- [Command Reference, page 27](#)
- [Feature Information for User-Based Firewall Support, page 28](#)

Prerequisites for User-Based Firewall Support

The following prerequisites apply to the configuration of User-Based Firewall Support.

Hardware Requirements

- Access Control Server
- Cisco Network Access Device, which can be any of the following:
 - Cisco 7200 router
 - Cisco 1800 router
 - Cisco 2800 router
 - Cisco 3800 router

Software Requirements

- Cisco IOS Release 12.4(20)T or a later release
- An Ingress Security feature that uses the Identity Policy infrastructure for policy application

Restrictions for User-Based Firewall Support

User-group mapping is based on the end-host's source IPv4 address. The “user-group” match criterion is supported for inspect class-maps.

Authentication Proxy and IP Admission

Authentication Proxy and IP Admission is an input only feature that should be configured on all the interfaces of the source zone. The Authentication Proxy and IP Admission feature is not virtual routing and forwarding (VRF) aware; therefore, user-group Zone Policy Firewall policies cannot be applied on a per VRF basis.

Information About User-Based Firewall Support

To configure the User-Based Firewall Support feature, you should understand the following concepts:

- [Feature Design of User-Based Firewall Support, page 3](#)
- [Firewall Support, page 3](#)
- [Authentication Proxy, page 4](#)
- [Zone-Based Policy Firewall, page 4](#)

- [Tag and Template, page 4](#)
- [Access Control List Overview, page 5](#)

Feature Design of User-Based Firewall Support

The User-Based Firewall Support feature was designed to provide identity or user-group based security that provides differentiated access for different classes of users. Classification can be provided on the basis of user identity, device type (for example, IP phones), location (for example, building) and role (for example, engineer). Because of the dynamic nature of end-host access, where every user is different and the resource he or she accesses is different, it is important to associate end-user's identity, role, or location with security policies. This association prevents the need for administrators to constantly update policy filters, a cumbersome task. The end-user identity can be derived through a variety of different mechanisms. Once a user's identity is established, security policies will be aware of the user's identity, not just the source address. Individual policies can be enforced allowing for greater control.

Cisco IOS supports several features that offer dynamic, per-user authentication and authorization of network access connections. These features include 802.1X, IKE, Authentication Proxy, Network Admission Control (NAC), and so on. These features allow network administrators to enforce security policies on per-user basis. By integrating authentication features with Cisco Policy Language based features such as Zone Based Firewall, Quality of Service (QoS), and so on, the combination can provide a transparent, reliable, ease to manage and deploy security solution to dynamically authenticate and enforce policies on a per user basis.

Cisco IOS User-Based Firewall Support leverages existing authentication and validation methods to associate each source IP address to a user-group. User-group association can be achieved using two methods. The first method (Tag and Template) uses locally defined policies to achieve the association, while the second method obtains the user-group information from the access control server (ACS) and requires no further configuration on the network access device (NAD).

The User-Based Firewall Support feature leverages the Tag and Template concept where the authenticating server returns a tag-name on validating the user credentials. This tag received on the authentication device is mapped to a template. The template is a control plane policy map that refers to an identity policy configured on the device. The identity policy contains the access policies that are to be applied for the corresponding tag-name. The identity policy defines one or more user-groups to which the source IP would be associated. This mapping provides administrators with flexibility to associate the end-host with multiple user-group memberships. The scope of the user-group defined in the identity policy is local to the device. Once the end-host's user-group membership has been established, other Cisco IOS policy language based features can enforce security policies on a per user-group basis.

Match Criterion

The match user-group criterion in the inspect type class map configuration can be used to enforce security policies on a per user-group basis. The match criterion filters the traffic stream based on the client's source IP address in the specified user-group, making it independent of the authentication method that established the group membership. The match criterion in the inspect type class map enables inspection for any ingress traffic and for any protocol, thereby enabling inspection for all traffic.

Firewall Support

Cisco IOS Firewall includes multiple security features. Cisco IOS Firewall stateful packet inspection provides true firewall capabilities to protect networks against unauthorized traffic and control legitimate business-critical data. Authentication proxy controls access to hosts or networks based on user

credentials stored in an authentication, authorization, and accounting (AAA) server. Multi-VRF firewall offers firewall services on virtual routers with VRF, accommodating overlapping address space to provide multiple isolated private route spaces with a full range of security services. Transparent firewall adds stateful inspection without time-consuming, disruptive IP addressing modifications. Application inspection controls application activity to provide granular policy enforcement of application usage, protecting legitimate application protocols from rogue applications and malicious activity. For more information on firewall support see the [Cisco IOS Firewall Design Guide](#).

Authentication Proxy

The Cisco IOS Firewall Authentication Proxy feature provides dynamic, per-user authentication and authorization, authenticating users against industry standard TACACS+ and RADIUS authentication protocols. Authenticating and authorizing connections by users provides more robust protection against network attacks. See the [Authentication Proxy](#) chapter in the *Cisco IOS Security Configuration Guide* for more information about this feature.

Zone-Based Policy Firewall

Cisco IOS Zone-Based Policy Firewall can be used to deploy security policies by assigning interfaces to different zones and configuring a policy to inspect the traffic moving between these zones. The policy specifies a set of actions to be applied on the defined traffic class. For more information see the chapter “Configuring Cisco IOS Firewall” in the *Cisco IOS Security Configuration Guide*. See the [Zone-Based Firewall](#) chapter in the *Cisco IOS Security Configuration Guide* for more information about this feature.

Tag and Template

The Tag and Template feature allows network administrators to define enforcement policies on a local device and have a RADIUS server specify the policy selector to be enforced. This feature can be applied to a NAC architecture. See the [Tag and Template feature guide](#) for more information about this feature.

Network Admission Control

In a typical Network Admission Control deployment, an ACS or a RADIUS server is used for validating the user posture information and for applying the policies on the NAD. A centralized ACS can be used to support multiple NADs. This solution has inherent problems associated with it, namely:

- Version control of policies. Typically, a specific NAD that is running a Cisco IOS image may support some access control lists (ACLs), and another NAD may support a different version. Managing different versions can be a problem.
- Users connect on different interfaces to the NAD, and on the basis of the interface type, the policies that can be applied to the user can change, and the NAD can determine the policies to be applied. In the current architecture, the ACS sends the same set of policies to all the NADs when a profile is matched, which does not give enough control to the administrator to configure the policies on the basis of the NAD configuration.

Configuring the Tag and Template feature allows the ACS to map users to specific groups and associate a tag with them. For example, the Usergroup1 user group may have a tag with the name "usergroup1." When the NAD queries the ACS for the policies, the ACS can return the tag that is associated with the user group. When this tag is received at the NAD, the NAD can map the tag to a specific template that

can have a set of policies that are associated with the user group. This mapping provides administrators with the flexibility to configure the template on a NAD basis, and the policies can change from NAD to NAD even though the tag is the same.

In summary, a template must be configured on the NAD, and the template must be associated with a tag. When the ACS sends the policies back to the NAD, the template that matches the tag that was received from the ACS is used.

Access Control List Overview

Cisco provides basic traffic filtering capabilities with access control lists (also referred to as access lists). Access lists can be configured for all routed network protocols (IP, AppleTalk, and so on) to filter the packets of those protocols as the packets pass through a router. You can configure access lists at your router to control access to a network. Access lists can prevent certain traffic from entering or exiting a network. See the [Access Control List](#) guidelines in the *Cisco IOS Security Configuration Guide* for more information about this feature.

How to Configure User-Based Firewall Support

Perform the following tasks to configure User-Based Firewall Support:

- [Configuring Access Control Lists, page 5](#)
- [Configuring the Identity Policy for Tag and Template, page 6](#)
- [Configuring Control Type Tag Class-Maps or Policy-Maps for Tag and Template, page 7](#)
- [Configuring Supplicant-Group Attribute on the ACS, page 9](#)
- [Configuring Firewall Class-Maps and Policy-Maps, page 9](#)
- [Configuring Firewall Zone Security and Zone-Pair, page 11](#)
- [Configuring ACLs for Authentication Proxy, page 12](#)
- [Configuring Authentication Proxy, page 14](#)
- [Configuring AAA and RADIUS, page 17](#)

Configuring Access Control Lists

To configure ACLs, perform the steps in this section. Policy specific ACLs are defined under the identity policy.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list extended** *access-list-name*
4. **permit** *protocol* **any host** *ip-address*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip access-list extended <i>access-list-name</i> Example: Router(config)# ip access-list extended auth_proxy_acl	Defines an IP access list and enters extended named access list configuration mode.
Step 4	permit <i>protocol</i> any host <i>ip-address</i> Example: Router(config-ext-nacl)# permit tcp any host 192.168.104.136	Sets the permission for an access list using TCP.
Step 5	end Example: Router(config-ext-nacl)# end	Exits extended named access list configuration mode.

Configuring the Identity Policy for Tag and Template

To configure the identity policy for Tag and Template, perform the steps in this section. Usergroup support is achieved by configuring the usergroup that is to be associated with the IP address on the NAD itself using a locally defined identity policy. A tag is received from the ACS that matches a template (identity policy) on the NAD. The user-group associated with the IP address is obtained from the NAD.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **identity policy** *policy-name*
4. **user-group** *group-name*
5. **access-group** *group-name*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	identity policy <i>policy-name</i> Example: Router(config)# identity policy auth_proxy_ip	Creates an identity policy and enters identity policy configuration mode.
Step 4	user-group <i>group-name</i> Example: Router(config-identity-policy)# user-group auth_proxy_ug	Establishes a user-group.
Step 5	access-group <i>group-name</i> Example: Router(config-identity-policy)# access-group auth_proxy_acl	Specifies the access-group to be applied to the identity policy.
Step 6	end Example: Router(config-identity-policy)# end	Exits identity policy configuration mode.

Configuring Control Type Tag Class-Maps or Policy-Maps for Tag and Template

To configure control type tag class-maps or policy-maps for Tag and Template, perform the steps in this section. Tag names are received from the AAA server as authorization data and are matched with their respective class-maps. The security policies that are associated with the identity policies are applied to the host. In this way host IP addresses gain membership of user-groups.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control tag** *policy-map-name*
4. **class type control tag** *control-class-name*
5. **identity policy** *policy-name*
6. **exit**

7. **configure terminal**
8. **class-map type control tag match-all** *class-map-name*
9. **match tag** *tag-name*
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy-map type control tag <i>policy-map-name</i> Example: Router(config)# policy-map type control tag all_tag_cm_pm	Creates a control policy map and enters policy-map configuration mode.
Step 4	class type control tag <i>control-class-name</i> Example: Router(config-pmap)# class type control tag auth_proxy_tag_cm	Creates a control class and enters policy-map-class configuration mode.
Step 5	identity policy <i>policy-name</i> Example: Router(config-pmap-c)# identity policy auth_proxy_ip	Creates an identity policy.
Step 6	exit Example: Router(config-pmap-c)# exit	Exits policy-map-class configuration mode.
Step 7	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 8	class-map type control tag match-all <i>class-map-name</i> Example: Router(config)# class-map type control tag match-all auth_proxy_tag_cm	Creates a control class map and enters class-map configuration mode.

	Command or Action	Purpose
Step 9	match tag <i>tag-name</i> Example: Router(config-cmap)# match tag <i>auth_proxy_tag</i>	Specifies the tag to be matched for a tag type of class map.
Step 10	end Example: Router(config-cmap)# end	Exits class-map configuration mode.

Configuring Supplicant-Group Attribute on the ACS

The supplicant group attribute needs to be configured as a Cisco attribute value (AV) Pair on the ACS for user based firewall support. To configure the supplicant-group attribute on the ACS, perform the steps in this section. The supplicant-group attribute is defined in the RADIUS authorization group attributes from where all authorization data pertaining to the client resides. The user-group information is obtained from the ACS and no further user-group specific configuration is required on the NAD.

SUMMARY STEPS

1. Cisco:Avpair=supplicant-group=*group-name*

DETAILED STEPS

- Step 1** Cisco:Avpair=supplicant-group=eng
Defines the supplicant-group attribute.

Configuring Firewall Class-Maps and Policy-Maps

To configure firewall class-maps and policy-maps, perform the steps in this section. User-groups are configured and attached to policy-maps by using the **inspect** command with each class-map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-all** *class-map-name*
4. **match protocol** *protocol-name*
5. **match user-group** *group-name*
6. **exit**
7. **configure terminal**
8. **policy-map type inspect** *policy-map-name*
9. **class type inspect** *class-map-name*

10. **inspect**

11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	class-map type inspect match-all <i>class-map-name</i> Example: Router(config)# class-map type inspect match-all auth_proxy_ins_cm	Creates an inspect type class map and enters class-map configuration mode.
Step 4	match protocol <i>protocol-name</i> Example: Router(config-cmap)# match protocol telnet	Configures the match criterion for the class map on the basis of the specified protocol.
Step 5	match user-group <i>group-name</i> Example: Router(config-cmap)# match user-group auth_proxy_ug	Configures the match criterion for the class map on the basis of the specified user-group.
Step 6	exit Example: Router(config-cmap)# exit	Exits class-map configuration mode.
Step 7	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 8	policy-map type inspect <i>policy-map-name</i> Example: Router(config)# policy-map type inspect all_ins_cm_pm	Creates an inspect type policy map and enters policy-map configuration mode.
Step 9	class type inspect <i>class-map-name</i> Example: Router(config-pmap)# class type inspect auth_proxy_ins_cm	Specifies the traffic (class) on which an action is to be performed.

	Command or Action	Purpose
Step 10	inspect Example: Router(config-pmap)# inspect	Enables Cisco IOS stateful packet inspection.
Step 11	end Example: Router(config-pmap)# end	Exits policy-map configuration mode.

Configuring Firewall Zone Security and Zone-Pair

To configure firewall zone security and zone -pair, perform the steps in this section. Security zones are configured for untrustworthy (outside) and trustworthy (inside) networks or interfaces. Zone-pairs are configured where the source zone is untrustworthy and the destination zone is trustworthy.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **zone security** *zone-name*
4. **end**
5. **configure terminal**
6. **zone-pair security** *zone-pair-name* **source** *source-zone-name* **destination** *destination-zone-name*
7. **service-policy type inspect** *policy-map-name*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	zone security <i>zone-name</i> Example: Router(config)# zone security out_sec_zone	Creates a security zone, and enters security zone configuration mode.

	Command or Action	Purpose
Step 4	end Example: Router(config-sec-zone)# end	Exits security zone configuration mode.
Step 5	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 6	zone-pair security zone-pair-name source source-zone-name destination destination-zone-name Example: Router(config)# zone-pair security out_in source out_sec_zone destination in_sec_zone	Creates a zone-pair and enters security zone-pair configuration mode.
Step 7	service-policy type inspect policy-map-name Example: Router(config-sec-zone-pair)# service-policy type inspect all_ins_cm_pm	Attaches a firewall policy map to the zone-pair.
Step 8	end Example: Router(config-sec-zone-pair)# end	Exits security zone-pair configuration mode.

Configuring ACLs for Authentication Proxy

To configure ACLs for authentication proxy, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list extended access-list-name**
4. **permit protocol any source-ip-address destination-ip-address**
5. **permit protocol any host destination-ip-address**
6. **permit protocol any any eq bootps**
7. **permit protocol any any eq domain**
8. **end**
9. **configure terminal**
10. **ip access-list extended access-list-name**
11. **permit protocol any host destination-ip-address**
12. **permit protocol any host destination-ip-address eq domain**

13. **permit** *protocol any host destination-ip-address eq www*
14. **permit** *protocol any host destination-ip-address eq port*
15. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip access-list extended <i>access-list-name</i> Example: Router(config)# ip access-list extended 102	Defines an IP access list and enters extended named access list configuration mode.
Step 4	permit <i>protocol any source-ip-address destination-ip-address</i> Example: Router(config-ext-nacl)# permit ip any 192.168.100.0 10.0.0.255	Sets the permission for an access list using IP.
Step 5	permit <i>protocol any host destination-ip-address</i> Example: Router(config-ext-nacl)# permit ip any host 192.168.104.136	Sets the permission for an access list using IP.
Step 6	permit <i>protocol any any eq bootps</i> Example: Router(config-ext-nacl)# permit ip any any eq bootps	Sets the permission for an access list using IP.
Step 7	permit <i>protocol any any eq domain</i> Example: Router(config-ext-nacl)# permit ip any any eq domain	Sets the permission for an access list using IP.
Step 8	end Example: Router(config-ext-nacl)# end	Exits extended named access list configuration mode.

	Command or Action	Purpose
Step 9	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 10	ip access-list extended access-list-name Example: Router(config)# ip access-list extended 103	Defines an IP access list and enters extended named access list configuration mode.
Step 11	permit protocol any host destination-ip-address Example: Router(config-ext-nacl)# permit ip any host 192.168.104.136	Sets the permission for an access list using IP.
Step 12	permit protocol any host destination-ip-address eq domain Example: Router(config-ext-nacl)# permit udp any host 192.168.104.136 eq domain	Sets the permission for an access list using user datagram protocol (UDP).
Step 13	permit protocol any host destination-ip-address eq www Example: Router(config-ext-nacl)# permit tcp any host 192.168.104.136 eq www	Sets the permission for an access list using TCP.
Step 14	permit protocol any host destination-ip-address eq port Example: Router(config-ext-nacl)# permit udp any host 192.168.104.136 eq 443	Sets the permission for an access list using UDP.
Step 15	end Example: Router(config-ext-nacl)# end	Exits extended named access list configuration mode.

Configuring Authentication Proxy

To configure authentication proxy default IP admissions, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission auth-proxy-banner http c Auth-Proxy-Banner-Text c**
4. **ip admission watch-list expiry-time expiry-minutes**

5. **ip admission max-login-attempts** *attempt-number*
6. **ip admission inactivity-timer** *timeout-minutes*
7. **ip admission absolute-timer** *timeout-minutes*
8. **ip admission init-state-timer** *timeout-minutes*
9. **ip admission auth-proxy-audit**
10. **ip admission watch-list enable**
11. **ip admission ratelimit** *limit*
12. **ip admission name** *admission-name* **proxy http list** *acl*
13. **ip admission name** *admission-name* **proxy telnet list** *acl*
14. **ip admission name** *admission-name* **proxy http list** *acl* **service-policy type tag** *service-policy-name*
15. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip admission auth-proxy-banner http c <i>Auth-Proxy-Banner-Text c</i> Example: Router(config)# ip admission auth-proxy-banner http c Auth-Proxy-Banner-Text c	Creates a network admission control rule with an authentication proxy banner to be applied to the interface.
Step 4	ip admission watch-list expiry-time <i>expiry-minutes</i> Example: Router(config)# ip admission watch-list expiry-time 50	Creates a network admission control rule with a watch-list to be applied to the interface.
Step 5	ip admission max-login-attempts <i>attempt-number</i> Example: Router(config)# ip admission max-login-attempts 10	Creates a network admission control rule with a specified maximum login attempts per user number to be applied to the interface.

	Command or Action	Purpose
Step 6	ip admission inactivity-timer <i>timeout-minutes</i> Example: Router(config)# ip admission inactivity-timer 205	Creates a network admission control rule with a specified inactivity timeout to be applied to the interface.
Step 7	ip admission absolute-timer <i>timeout-minutes</i> Example: Router(config)# ip admission absolute-timer 305	Creates a network admission control rule with a specified absolute timeout to be applied to the interface.
Step 8	ip admission init-state-timer <i>timeout-minutes</i> Example: Router(config)# ip admission init-state-timer 15	Creates a network admission control rule with a specified init-state timeout to be applied to the interface.
Step 9	ip admission auth-proxy-audit Example: Router(config)# ip admission auth-proxy-audit	Creates a network admission control rule with authentication proxy auditing to be applied to the interface.
Step 10	ip admission watch-list enable Example: Router(config)# ip admission watch-list enable	Creates a network admission control rule with a watch-list to be applied to the interface.
Step 11	ip admission ratelimit <i>limit</i> Example: Router(config)# ip admission ratelimit 100	Creates a network admission control rule with a specified session rate limit to be applied to the interface.
Step 12	ip admission name <i>admission-name</i> proxy http list <i>acl</i> Example: Router(config)# ip admission name auth_rule proxy http list 103	Creates an IP network admission control rule. <ul style="list-style-type: none"> Telnet, HTTP, or both can be configured.
Step 13	ip admission name <i>admission-name</i> proxy telnet list <i>acl</i> Example: Router(config)# ip admission name auth_rule proxy telnet list 103	Creates an IP network admission control rule. <ul style="list-style-type: none"> Telnet, HTTP, or both can be configured.

	Command or Action	Purpose
Step 14	<p>ip admission name <i>admission-name</i> proxy http list acl service-policy type tag <i>service-policy-name</i></p> <p>Example: Router(config)# ip admission name auth_rule proxy http list 103 service-policy type tag all_tag_cm_pm</p>	<p>(Optional) Creates an IP network admission control rule.</p> <ul style="list-style-type: none"> Configures a control plane service policy when the Tag & Template method of user-group association is used. Control plane tag service policy that is configured using the policy-map type control tag <i>{policy name}</i> command, keyword, and argument. This policy map is used to apply the actions on the host when a tag is received.
Step 15	<p>exit</p> <p>Example: Router(config)# exit</p>	Exits global configuration mode.

Configuring AAA and RADIUS

To configure AAA and RADIUS servers, perform the steps in this section.

SUMMARY STEPSs

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login default group radius**
5. **aaa authentication login** *list-name* **none**
6. **aaa authentication eou default enable group radius**
7. **aaa authorization network default group radius local**
8. **aaa authorization** *list-name* **default group radius**
9. **aaa accounting auth-proxy default start-stop group** *group-name*
10. **aaa accounting system default start-stop group** *group-name*
11. **aaa session-id common**
12. **radius-server attribute 6 on-for-login-auth**
13. **radius-server attribute 8 include-in-access-req**
14. **radius-server attribute 25 access-request include**
15. **radius-server configure-nas**
16. **radius-server host** *ip-address* **auth-port** *port-number* **acct-port** *port-number* **key** *string*
17. **radius-server host** *ip-address* **auth-port** *port-number* **acct-port** *port-number* **key** *string*
18. **radius-server source-ports extended**
19. **radius-server vsa send authentication**
20. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Router(config)# aaa new-model	Enables the AAA access control model.
Step 4	aaa authentication login default group radius Example: Router(config)# aaa authentication login default group radius	Sets AAA authentication at login using the group radius method.
Step 5	aaa authentication login list-name none Example: Router(config)# aaa authentication login noAAA none	Sets AAA authentication at login and ensures that the authentication succeeds even if all methods of authentication return an error.
Step 6	aaa authentication eou default enable group radius Example: Router(config)# aaa authentication eou default enable group radius	Sets authentication lists for Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP).
Step 7	aaa authorization network default group radius local Example: Router(config)# aaa authorization network default group radius local	Sets parameters that restrict user access to a network using the group radius and local methods. <ul style="list-style-type: none"> The group radius method uses the list of all RADIUS servers for authentication. The local method uses the local database for authorization.
Step 8	aaa authorization list-name default group radius Example: Router(config)# aaa authorization auth-proxy default group radius	Sets parameters that restrict user access to a network using the group radius method.

	Command or Action	Purpose
Step 9	aaa accounting auth-proxy default start-stop group group-name Example: Router(config)# aaa accounting auth-proxy default start-stop group radius	Creates a method list to provide information about all authenticated-proxy user events. <ul style="list-style-type: none"> Sends a “start” accounting notice at the beginning of a process and a “stop” accounting notice at the end of a process.
Step 10	aaa accounting system default start-stop group group-name Example: Router(config)# aaa accounting system default start-stop group radius	Creates a method list to provide accounting for all system-level events not associated with users. <ul style="list-style-type: none"> Sends a “start” accounting notice at the beginning of a process and a “stop” accounting notice at the end of a process.
Step 11	aaa session-id common Example: Router(config)# aaa session-id common	Specifies that the same ID will be assigned for each AAA accounting service type within a call.
Step 12	radius-server attribute 6 on-for-login-auth Example: Router(config)# radius-server attribute 6 on-for-login-auth	Sends the Service-Type attribute in the authentication packets.
Step 13	radius-server attribute 8 include-in-access-req Example: Router(config)# radius-server attribute 8 include-in-access-req	Sends the IP address of a user to the RADIUS server in the access request.
Step 14	radius-server attribute 25 access-request include Example: Router(config)# radius-server attribute 25 access-request include	Sends an arbitrary value that the network access server includes in all accounting packets for the user if supplied by the RADIUS server.
Step 15	radius-server configure-nas Example: Router(config)# radius-server configure-nas	Configures the Cisco router or access server to query the vendor-proprietary RADIUS server for the static routes and IP pool definitions used throughout its domain when the device starts up.
Step 16	radius-server host ip-address auth-port port-number acct-port port-number key string Example: Router(config)# radius-server host 192.168.104.131 auth-port 1645 acct-port 1646 key string1	Specifies a RADIUS server host. <ul style="list-style-type: none"> Specifies the UDP destination port for authentication requests. Specifies the UDP destination port for accounting requests.

	Command or Action	Purpose
Step 17	radius-server host <i>ip-address</i> auth-port <i>port-number</i> acct-port <i>port-number</i> key <i>string</i> Example: Router(config)# radius-server host 192.168.104.132 auth-port 1645 acct-port 1646 key string2	Specifies a RADIUS server host. <ul style="list-style-type: none"> Specifies the UDP destination port for authentication requests. Specifies the UDP destination port for accounting requests.
Step 18	radius-server source-ports extended Example: Router(config)# radius-server source-ports extended	Enables 200 ports in the range from 21645 to 21844 to be used as the source ports for sending out RADIUS requests. <ul style="list-style-type: none"> Ports 1645 and 1646 are used as the source ports for RADIUS requests.
Step 19	radius-server vsa send authentication Example: Router(config)# radius-server vsa send authentication	Configures the network access server (NAS) to recognize and use vendor-specific attributes (VSAs).
Step 20	exit Example: Router(config)# exit	Exits global configuration mode.

Troubleshooting Tips

The following commands can be used to troubleshoot User-Based Firewall Support:

- **clear ip admission cache**
- **debug user-group**
- **show debugging**
- **show epm session ip**
- **show ip access-lists**
- **show ip admission**
- **show logging**
- **show policy-map type inspect zone-pair**
- **show user-group**

Examples

show epm session ip

The following example shows sample output of the **show epm session** command when the **summary** keyword is used.

```
Router# show epm session ip summary
EPM Session Information
-----
Total sessions seen so far: 8
Total Active sessions: 1
```

```

Session IP Address:
-----
192.168.101.131

```

The following example shows sample output of the **show epm session** command when the *ip-address* argument is specified. The output below is displayed if a locally defined user-group association (Tag and Template method) is used.

```

Router# show epm session ip 192.168.101.131
Admission feature: Authproxy
Tag Received: eng_group_tag
Policy map used: all_tag_cm_pm
Class map matched: eng_tag_cm

```

The following example shows sample output of the **show epm session** command when the *ip-address* argument is specified. The output below is displayed if ACS defined (supplicant-group attribute configured on the ACS) user-group association is used.

```

Router# show epm session ip 192.168.101.131
Admission feature: Authproxy
AAA policies:
ACS ACL: xACSAClX-IP-TEST_ACL-47dfc392
Supplicant-Group: eng
Supplicant-Group: mgr
Proxy ACL: permit udp any any
Router#

```

show ip access-lists

The following example shows sample output of the **show ip access-lists** command.

```

Router# show ip access-lists
Extended IP access list 102
    permit icmp host 192.168.101.131 host 192.168.104.136Auth-Proxy ACE downloaded from
AAA
    permit udp host 192.168.101.131 host 192.168.104.136Auth-Proxy ACE downloaded from AAA
    permit tcp host 192.168.101.131 host 192.168.104.136Auth-Proxy ACE downloaded from AAA
10 permit ip any 192.168.100.0 10.0.0.255 (956 matches)
    20 permit ip any 192.168.101.0 10.0.0.255 (9 matches)
    30 permit ip any host 192.168.104.136 (20 matches)
    40 permit udp any any eq bootps
    50 permit udp any any eq domain
Extended IP access list 103
    10 permit ip any host 192.168.104.136 (3 matches)
    20 permit udp any host 192.168.104.136 eq domain
    30 permit tcp any host 192.168.104.136 eq www
    40 permit udp any host 192.168.104.136 eq 443
    50 permit tcp any host 192.168.104.136 eq 443
Extended IP access list vendor_group_acl
    10 permit ip any host 192.168.104.136
Extended IP access list auth_proxy_acl
    10 permit tcp any host 192.168.104.136
    20 permit udp any host 192.168.104.136
    30 permit icmp any host 192.168.104.136
Extended IP access list sales_group_acl
    10 permit ip any host 192.168.104.131
Extended IP access list eng_group_acl
    10 permit ip any host 192.168.100.132
Extended IP access list manager_group_acl
    10 permit ip any host 192.168.104.128
Router#

```

show ip admission

The following example shows sample output of the **show ip admission** command when the **configuration** keyword is used.

```
Router# show ip admission configuration

Authentication Proxy Banner
  HTTP Protocol Banner: Auth-Proxy-Banner-Text
Authentication global cache time is 205 minutes
Authentication global absolute time is 305 minutes
Authentication global init state time is 15 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Session Watch-list is enabled
Watch-list expiry timeout is 50 minutes
Authentication Proxy Auditing is enabled
Max Login attempts per user is 10

Authentication Proxy Rule Configuration
Auth-proxy name auth_rule
  http list 103 inactivity-timer 205 minutes
Router#
```

The following example shows sample output of the **show ip admission** command when the **cache** keyword is used. After a successful Telnet/HTTP-proxy session, from a Cisco Trust Agent (CTA) client to an Audit Server, is established, logs are displayed.

```
Router# show ip admission cache
Authentication Proxy Cache
Client Name aaatestuser, Client IP 192.168.101.131, Port 1870, timeout 205, Time Remaining
205, state ESTAB
```

show logging

The following example shows sample output of the **show logging** command.

```
Router# show logging
Log Buffer (65000 bytes):
*Jul 3 05:33:13.935: %SYS-5-CONFIG_I: Configured from console by console
*Jul 3 05:33:18.471: USRGRP-API: [Type=IPv4 Val=192.168.101.131 Group=h_ug]: Usergroup
opcode entry deletion.
*Jul 3 05:33:18.471: %UG-6-MEMBERSHIP: IP=192.168.101.131| INTERFACE=Vlan|
USERGROUP=eng_group_ug| STATUS=REMOVED
*Jul 3 05:33:18.471: USRGRP-ENTRY: [Type=IPv4 Val=192.168.101.131 :: Group=eng_group_ug
Count=0]:Usergroup entry deleted
*Jul 3 05:33:18.471: USRGRP-ENTRY: [Type=IPv4 Val=192.168.101.131 :: Group=eng_group_ug
Count=0]:Usergroup entry clean up and free
*Jul 3 05:33:18.471: USRGRP-DB: Group=h_ug Count=0: Usergroup is empty. Destroy Group.
*Jul 3 05:33:18.471: USRGRP-DB: Group=h_ug Count=0: Clean up and free usergroup db.
*Jul 3 05:33:22.383: USRGRP-API: [Type=IPv4 Val=192.168.101.131 Group=eng_group_ug]:
Usergroup opcode entry addition.
*Jul 3 05:33:22.383: USRGRP-DB: Group=h_ug Count=0 New usergroup db created.
*Jul 3 05:33:22.383: %UG-6-MEMBERSHIP: IP=192.168.101.131| INTERFACE=Vlan333|
USERGROUP=eng_group_ug| STATUS=ESTABLISHED
*Jul 3 05:33:22.383: USRGRP-ENTRY: [Type=IPv4 Val=192.168.101.131 :: Group=eng_group_ug
Count=1]: Usergroup entry added
*Jul 3 05:33:41.239: USRGRP-API: [Type=IPv4 Val=192.168.101.131 Group=eng_group_ug]:
Usergroup opcode entry deletion.
*Jul 3 05:33:41.239: %UG-6-MEMBERSHIP: IP=192.168.101.131| INTERFACE=Vlan333|
USERGROUP=eng_group_ug| STATUS=REMOVED
*Jul 3 05:33:41.239: USRGRP-ENTRY: [Type=IPv4 Val=192.168.101.131 :: Group=eng_group_ug
Count=0]: Usergroup entry deleted
*Jul 3 05:33:41.239: USRGRP-ENTRY: [Type=IPv4 Val=192.168.101.131 :: Group=eng_group_ug
Count=0]: Usergroup entry clean up and free
```



```
*Jul 3 05:33:41.239: USRGRP-DB: Group=eng_group_ug Count=0: Usergroup is empty. Destroy
group.
*Jul 3 05:33:41.239: USRGRP-DB: Group=eng_group_ug Count=0: Clean up and free usergroup
db.
*Jul 3 05:33:50.687: USRGRP-API: {Type=IPv4 Val=192.168.101.131 Group=eng_group_ug}:
Usergroup opcode entry addition.
*Jul 3 05:33:50.687: USRGRP-DB: Group=eng_group_ug Count=0: New usergroup db created.
*Jul 3 05:33:50.687: %UG-6-MEMBERSHIP: IP=192.168.101.131| INTERFACE=Vlan333|
USERGROUP=eng_group_ug| STATUS=ESTABLISHED
*Jul 3 05:33:50.687: USRGRP-ENTRY: [Type=IPv4 Val=192.168.101.131 :: Group=eng_group_ug
Count=1]: Usergroup entry added
```

show policy-map type inspect zone-pair

The following example shows sample output of the **show policy-map type inspect zone-pair** command when the **sessions** keyword is used.

```
Router# show policy-map type inspect zone-pair sessions
policy exists on zp out_in
Zone-pair: out_in
Service-policy inspect: all_ins_cm_pm
Class-map: vendor_group_ins_cm (match-all)
Match: user-group vendor_group_ug

Class-map: manager_group_ins_cm (match-all)
Match: protocol telnet
Match: user-group manager_group_ug

Class-map: auth_proxy_ins_cm (match-all)
Match: user-group auth_proxy_ug
Match: protocol telnet

Number of Established Sessions = 1
Established Sessions
Session 49D12BE0 (192.168.101.131:1872)=>(192.168.104.136:23) telnet:tcp SIS_OPEN
Created 00:00:15, Last heard 00:00:09
Bytes sent (initiator:responder) [171:249]

Class-map: eng_group_ins_cm (match-all)
Match: user-group eng_group_ug
Match: protocol ftp

Number of Established Sessions = 1
Established Sessions
Session 49D12E20 (192.168.101.131:1874)=>(192.168.104.136:21) ftp:tcp SIS_OPEN
Created 00:00:12, Last heard 00:00:06
Bytes sent (initiator:responder) [45:137]

Class-map: sales_group_ins_cm (match-all)
Match: protocol ftp
Match: user-group sales_group_ug

Class-map: class-default (match-any)
Match: any
```

show user-group

The following example shows sample output of the **show user-group** command when the **configuration** keyword is used.

```
Router# show user-group
Usergroup: auth_proxy_ug
```

```

-----
User Name      Type      Interface  Learn  Age (min)
-----
192.168.101.131IPv4  Vlan333    Dynamic 0

```

```
Usergroup: eng_group_ug
```

```

-----
User Name      Type      Interface  Learn  Age (min)
-----
192.168.101.131IPv4  Vlan333    Dynamic 0

```

The following example shows sample output of the **show user-group** command when the *group-name* argument is used.

```
Router# show user-group auth_proxy_ug
Usergroup: auth_proxy_ug
```

```

-----
User Name      Type      Interface  Learn  Age (min)
-----
192.168.101.131IPv4  Vlan333    Dynamic 0

```

The following example shows sample output of the **show user-group** command when the **count** keyword is used.

```
Router# show user-group count
Total Usergroup: 2
```

```

-----
User Group      Members
-----
auth_proxy_ug   1
eng_proxy_ug    1

```

Configuration Examples for User-Based Firewall Support

This section contains the following example:

- [Cisco IOS Authentication Proxy Mapping: Example, page 24](#)

Cisco IOS Authentication Proxy Mapping: Example

The following example shows how to configure User-Based Firewall Support. The Cisco IOS Authentication Proxy maps two users to different user-groups. Zone Policy Firewall policies are configured on a per user-group basis.

```

!IP Admission configuration
Configure the rule for HTTP based proxy authentication and associate the control plane tag
service policy.
!
configure terminal

ip admission name auth-http proxy http service-policy type tag global-policy
ip http server
ip http secure-server

!AAA configuration
!
aaa new-model
!

```

```
aaa authentication login default group radius
aaa authentication login noAAA none
aaa authentication eou default group radius
aaa authorization network default group radius local
aaa authorization auth-proxy default group radius
aaa accounting auth-proxy default start-stop group radius
aaa accounting system default start-stop group radius
aaa session-id common
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server configure-nas
radius-server host 192.168.104.131 auth-port 1645 acct-port 1646 key cisco
radius-server host 192.168.104.132 auth-port 1645 acct-port 1646 key cisco
radius-server source-ports extended
radius-server vsa send authentication
!
!Tag and Template configuration.
Configuration policy attributes for the engineer.
!
identity policy engineer-policy
    access-group engineer-acl
    user-group group-engineer

identity policy manager-policy
    access-group manager-acl
    user-group group-manager

!Define type control tag class-maps
!
class-map type control tag match-all auth_proxy_tag_cm
match tag auth_proxy_tag
class-map type control tag match-all eng_tag_cm
match tag eng_group_tag
class-map type control tag match-all manager_tag_cm
match tag manager_group_tag
!

!Define the control plane tag policy map.
!
policy-map type tag control tag global-policy
    class engineer-class
        identity policy engineer-policy

    class manager-class
        identity policy manager-policy

!Define per-user group traffic classification based on membership of the source IP address
in the specified user-group.
!
class-map type inspect match-all engineer-insp-cmap
    match user-group group-engineer
    match protocol tcp
    match protocol udp

class-map type inspect match-all manager-insp-cmap
    match user-group group-manager
    match protocol http

!Zone Policy Firewall configuration.
Configure zones z1 and z2.
!
zone security z1
```

```

zone security z2

!Configure the policy map to inspect traffic between z1 and z2.
!
policy-map type inspect z1-z2-policy
  class type inspect engineer-insp-cmap
    inspect
  class type inspect manager-insp-cmap
    inspect

!Configure interfaces to their respective zones and apply the ip admission rule on the
source zone member(s).
!
interface e0
  ip admission auth-http
  zone-member security z1

interface e1
  zone-member security z2

!Configure the zone-pair and apply the appropriate policy-map.
!
zone-pair security z1-z2 source z1 destination z2
  service-policy type inspect z1-z2-policy

```

Additional References

The following sections provide references related to the User-Based Firewall Support feature.

Related Documents

Related Topic	Document Title
Cisco IOS Firewall Design	The Cisco IOS Firewall Design Guide
Cisco IOS firewall commands	<i>Cisco IOS Security Command Reference.</i>
Cisco IOS Tag and Template Feature	The chapter “Tag and Template” in the <i>Cisco IOS Security Configuration Guide.</i>
Cisco IOS Zone-Based Policy Firewall Feature	The chapter “Zone-Based Policy Firewall” in the <i>Cisco IOS Security Configuration Guide.</i>
Cisco IOS Authentication Proxy Feature	The chapter “Authentication Proxy” in the <i>Cisco IOS Security Configuration Guide.</i>
Cisco IOS Access Control Lists Overview	The “Access Control Lists: Overview and Guidelines” chapter in the <i>Cisco IOS Security Configuration Guide.</i>

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html.

- **debug user-group**
- **match user-group**
- **show debugging**
- **show user-group**
- **user-group**
- **user-group logging**

Feature Information for User-Based Firewall Support

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for User-Based Firewall Support

Feature Name	Releases	Feature Information
User-Based Firewall Support	12.4(20)T	<p>This feature provides the option for configuring a security solution to dynamically authenticate and enforce policies on a per user basis in Cisco IOS software for Release 12.4(20)T and later releases.</p> <p>In Release 12.4(20)T, this feature was introduced on the Cisco 7200, Cisco 1800, Cisco 2800, and Cisco 3800 routers.</p> <p>The following commands were introduced or modified: debug user-group, match user-group, show debugging, show user-group, user-group, user-group logging.</p>

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.



Virtual Fragmentation Reassembly

Currently, the Cisco IOS Firewall—specifically context-based access control (CBAC) and the intrusion detection system (IDS)—cannot identify the contents of the IP fragments nor can it gather port information from the fragment. These inabilities allow the fragments to pass through the network without being examined or without dynamic access control list (ACL) creation.

Virtual fragmentation reassembly (VFR) enables the Cisco IOS Firewall to create the appropriate dynamic ACLs, thereby, protecting the network from various fragmentation attacks.

Feature History for Virtual Fragmentation Reassembly

Release	Modification
12.3(8)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions for Virtual Fragmentation Reassembly, page 2](#)
- [Information About Virtual Fragmentation Reassembly, page 2](#)
- [How to Use Virtual Fragmentation Reassembly, page 3](#)
- [Configuration Examples for Fragmentation Reassembly, page 4](#)
- [Additional References, page 6](#)
- [Command Reference, page 7](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Restrictions for Virtual Fragmentation Reassembly

Performance Impact

VFR will cause a performance impact on the basis of functions such as packet copying, fragment validation, and fragment reorder. This performance impact will vary depending on the number of concurrent IP datagram that are being reassembled.

VFR Configuration Restriction

VFR should not be enabled on a router that is placed on an asymmetric path. The reassembly process requires all of the fragments within an IP datagram. Routers placed in the asymmetric path may not receive all of the fragments, so the fragment reassembly will fail.

SIP and RTSP Limitation

The Session Initiation Protocol (SIP) and the Real-Time Streaming Protocol (RTSP) do not have the ability to parse port information across noncontiguous buffers. Thus, virtual fragmentation reassembly may fail. (If the application fails, the session will be blocked.)

Information About Virtual Fragmentation Reassembly

To use fragmentation support for Cisco IOS Firewall, you should understand the following concept:

- [Detected Fragment Attacks, page 2](#)
- [Automatically Enabling or Disabling VFR, page 3](#)

Detected Fragment Attacks

VFR is responsible for detecting and preventing the following types of fragment attacks:

- **Tiny Fragment Attack**—In this type of attack, the attacker makes the fragment size small enough to force Layer 4 (TCP and User Datagram Protocol (UDP)) header fields into the second fragment. Thus, the ACL rules that have been configured for those fields will not match.

VFR drops all tiny fragments, and an alert message such as follows is logged to the syslog server: “VFR-3-TINY_FRAGMENTS.”

- **Overlapping Fragment Attack**—In this type of attack, the attacker can overwrite the fragment offset in the noninitial IP fragment packets. When the firewall reassembles the IP fragments, it might create wrong IP packets, causing the memory to overflow or your system to crash.

VFR drops all fragments within a fragment chain if an overlap fragment is detected, and an alert message such as follows is logged to the syslog server: “VFR-3-OVERLAP_FRAGMENT.”

- **Buffer Overflow Attack**—In this type of denial-of-service (DoS) attack, the attacker can continuously send a large number of incomplete IP fragments, causing the firewall to lose time and memory while trying to reassemble the fake packets.

To avoid buffer overflow and control memory usage, configure a maximum threshold for the number of IP datagrams that are being reassembled and the number of fragments per datagram. (Both of these parameters can be specified via the **ip virtual-reassembly** command.)

When the maximum number of datagrams that can be reassembled at any given time is reached, all subsequent fragments are dropped, and an alert message such as the following is logged to the syslog server: “VFR-4_FRAG_TABLE_OVERFLOW.”

When the maximum number of fragments per datagram is reached, subsequent fragments will be dropped, and an alert message such as the following is logged to the syslog server: “VFR-4_TOO_MANY_FRAGMENTS.”

In addition to configuring the maximum threshold values, each IP datagram is associated with a managed timer. If the IP datagram does not receive all of the fragments within the specified time, the timer will expire and the IP datagram (and all of its fragments) will be dropped.

Automatically Enabling or Disabling VFR

VFR is designed to work with any feature that requires fragment reassembly (such as Cisco IOS Firewall and NAT). Currently, NAT enables and disables VFR internally; that is, when NAT is enabled on an interface, VFR is automatically enabled on that interface.

If more than one feature attempts to automatically enable VFR on an interface, VFR will maintain a reference count to keep track of the number of features that have enabled VFR. When the reference count is reduced to zero, VFR is automatically disabled.

How to Use Virtual Fragmentation Reassembly

This section contains the following procedures:

- [Configuring VFR, page 3](#)

Configuring VFR

Use this task to enable VFR on an interface, specify maximum threshold values to combat buffer overflow and control memory usage, and verify any VFR configurations.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface type** *type number*
4. **ip virtual-reassembly** [**max-reassemblies** *number*] [**max-fragments** *number*] [**timeout** *seconds*] [**drop-fragments**]
5. **exit**
6. **exit**
7. **show ip virtual-reassembly** [**interface type**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Router(config)# interface ethernet1/1	Configures an interface type and enters interface configuration mode.
Step 4	ip virtual-reassembly [max-reassemblies <i>number</i>] [max-fragments <i>number</i>] [timeout <i>seconds</i>] [drop-fragments] Example: Router(config-if)# ip virtual-reassembly max-reassemblies 64 max-fragments 16 timeout 5	Enables VFR on an interface.
Step 5	exit Example: Router(config-if)# exit	Exits interface configuration mode.
Step 6	exit Example: Router(config)# exit	Exits global configuration mode.
Step 7	show ip virtual-reassembly [interface <i>type</i>] Example: Router# show ip virtual-reassembly ethernet1/1	Displays the configuration and statistical information of the VFR. If an interface is not specified, VFR information is shown for all configured interfaces.

Troubleshooting Tips

To view debugging messages related to the VFR subsystem, use the **debug ip virtual-reassembly** command.

Configuration Examples for Fragmentation Reassembly

This section contains the following configuration example:

- [Configuring VFR and a Cisco IOS Firewall: Example, page 5](#)

Configuring VFR and a Cisco IOS Firewall: Example

The following example shows a typical scenario where the Virtual Fragment Reassembly module is enabled on interfaces ethernet2/1, ethernet2/2, and serial3/0 to facilitate the firewall that is enabled in the outbound direction on interface serial3/0. In this example, the firewall rules that specify the list of LAN1 and LAN2 originating protocols (FTP, HTTP and SMTP) are to be inspected.

Figure 1 *VFR and Cisco IOS Firewall Sample Topology*



```
!  
ip inspect name INTERNET-FW ftp  
ip inspect name INTERNET-FW http  
ip inspect name INTERNET-FW smtp  
!  
!  
interface Loopback0  
  ip address 1.1.1.1 255.255.255.255  
!  
interface Ethernet2/0  
  ip address 9.4.21.9 255.255.0.0  
  no ip proxy-arp  
  no ip mroute-cache  
  duplex half  
  no cdp enable  
!  
interface Ethernet2/1  
  description LAN1  
  ip address 14.0.0.2 255.255.255.0  
  ip virtual-reassembly  
  duplex half  
!  
interface Ethernet2/2  
  description LAN2  
  ip address 15.0.0.2 255.255.255.0  
  ip virtual-reassembly  
  duplex half  
!  
interface Ethernet2/3  
  no ip address  
  no ip mroute-cache  
  shutdown  
  duplex half  
!  
interface Serial3/0  
  description Internet  
  ip unnumbered Loopback0  
  encapsulation ppp  
  ip access-group 102 in  
  ip inspect INTERNET-FW out  
  ip virtual-reassembly
```

```
    serial restart-delay 0
    !
ip classless
ip route 0.0.0.0 0.0.0.0 s3/0
    !
    !
    ! Access Control Rule that drops all internet originated traffic.
    !
access-list 102 deny    ip any any
    !
    !
    !
control-plane
    !
no call rsvp-sync
    !
    !
    !
dial-peer cor custom
    !
    !
    !
    !
gatekeeper
shutdown
    !
    !
line con 0
    exec-timeout 0 0
    stopbits 1
line aux 0
    stopbits 1
line vty 0 4
    password lab
    login
    !
    !
end
```

Additional References

The following sections provide references related to virtual fragmentation reassembly.

Related Documents

Related Topic	Document Title
Dynamic IDS	<i>Cisco IOS Intrusion Prevention System</i> , Cisco IOS Release 12.3(8)T feature module
CBAC	<i>The chapter “Configuring Context-Based Access Control” in the Cisco IOS Security Configuration Guide</i>

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 791	Internet Protocol
RFC 1858	Security Considerations for IP Fragment Filtering

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug ip virtual-reassembly**
- **ip virtual-reassembly**
- **show ip virtual-reassembly**

Glossary

fragment—Part of an IP datagram that is fragmented into multiple pieces. Each piece is called a fragment or an IP fragment.

fragmentation—Process of breaking down an IP datagram into smaller packets (fragments) that are transmitted over different types of network media.

initial fragment— First fragment within a fragment set. This fragment should have a Layer 4 header and should have an offset of zero.

noninitial fragment—All fragments within a fragment set, except the initial fragment.



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



VRF Aware Cisco IOS Firewall

VRF Aware Cisco IOS Firewall applies Cisco IOS Firewall functionality to VRF (Virtual Routing and Forwarding) interfaces when the firewall is configured on a service provider (SP) or large enterprise edge router. SPs can provide managed services to small and medium business markets.

The VRF Aware Cisco IOS Firewall supports VRF-aware URL filtering and VRF-lite (also known as Multi-VRF CE).

Feature History for VRF Aware Cisco IOS Firewall

Release	Modification
12.3(14)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for VRF Aware Cisco IOS Firewall, page 2](#)
- [Restrictions for VRF Aware Cisco IOS Firewall, page 2](#)
- [Information About VRF Aware Cisco IOS Firewall, page 2](#)
- [How to Configure VRF Aware Cisco IOS Firewall, page 11](#)
- [Configuration Examples for VRF Aware Cisco IOS Firewall, page 15](#)
- [Additional References, page 24](#)
- [Command Reference, page 26](#)
- [Glossary, page 28](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for VRF Aware Cisco IOS Firewall

- Understand Cisco IOS firewalls.
- Configure VRFs.
- Verify that the VRFs are operational.

Restrictions for VRF Aware Cisco IOS Firewall

- VRF Aware Cisco IOS Firewall is not supported on Multiprotocol Label Switching (MPLS) interfaces.
- If two VPN networks have overlapping addresses, VRF-aware network address translation (NAT) is required for them to support VRF-aware Firewalls.
- When crypto tunnels belonging to multiple VPNs terminate on a single interface, you cannot apply per-VRF firewall policies.

Information About VRF Aware Cisco IOS Firewall

To configure VRF Aware Cisco IOS Firewall, you need to understand the following concepts:

- [Cisco IOS Firewall, page 2](#)
- [VRF, page 3](#)
- [VRF-lite, page 4](#)
- [Per-VRF URL Filtering, page 5](#)
- [Alerts and Audit Trails, page 5](#)
- [MPLS VPN, page 5](#)
- [VRF-aware NAT, page 5](#)
- [VRF-aware IPSec, page 6](#)
- [VRF Aware Cisco IOS Firewall Deployment, page 7](#)

Cisco IOS Firewall

The Cisco IOS Firewall provides robust, integrated firewall and intrusion detection functionality for every perimeter of the network. Available for a wide range of Cisco IOS software-based routers, the Cisco IOS Firewall offers sophisticated security and policy enforcement for connections within an organization (intranet) and between partner networks (extranets), as well as for securing Internet connectivity for remote and branch offices.

The Cisco IOS Firewall enhances existing Cisco IOS security capabilities such as authentication, encryption, and failover, with state-of-the-art security features such as stateful, application-based filtering (context-based access control), defense against network attacks, per-user authentication and authorization, and real-time alerts.

The Cisco IOS Firewall is configurable via Cisco ConfigMaker software, an easy-to-use Microsoft Windows 95, Windows 98, NT 4.0 based software tool.

The Cisco IOS Firewall provides great value in addition to these benefits:

- Flexibility—Provides multiprotocol routing, perimeter security, intrusion detection, VPN functionality, and dynamic per-user authentication and authorization.
- Scalable deployment—Scales to meet any network's bandwidth and performance requirements.
- Investment protection—Leverages existing multiprotocol router investment.
- VPN support—Provides a complete VPN solution based on Cisco IOS IPSec and other CISCOS IOS software-based technologies, including L2TP tunneling and quality of service (QoS).

The VRF Aware Cisco IOS Firewall is different from the non-VRF Aware Firewall because it does the following:

- Allows users to configure a per-VRF Firewall. The firewall inspects IP packets that are sent and received within a VRF.
- Allows SPs to deploy the firewall on the provider edge (PE) router.
- Supports overlapping IP address space, thereby allowing traffic from nonintersecting VRFs to have the same IP address.
- Supports per-VRF (not global) firewall command parameters and Denial-of-Service (DoS) parameters so that the VRF-aware Firewall can run as multiple instances (with VRF instances) allocated to various Virtual Private Network (VPN) customers.
- Performs per-VRF URL filtering.
- Generates VRF-specific syslog messages that can be seen only by a particular VPN. These alert and audit-trail messages allow network administrators to manage the firewall; that is, they can adjust firewall parameters, detect malicious sources and attacks, add security policies, and so forth. The vrf name is tagged to syslog messages being logged to the syslog server.

Both VFR Aware and non-VFR Aware Firewalls now allow you to limit the number of firewall sessions. Otherwise, it would be difficult for VRFs to share router resources because one VRF may consume a maximum amount of resources, leaving few resources for other VRFs. That would cause the denial of service to other VRFs. To limit the number of sessions, enter the **ip inspect name** command.

VRF

VPN Routing and Forwarding (VRF) is an IOS route table instance for connecting a set of sites to a VPN service. A VRF contains a template of a VPN Routing/Forwarding table in a PE router.

The overlapping addresses, usually resulting from the use of private IP addresses in customer networks, are one of the major obstacles to successful deployment of peer-to-peer VPN implementation. The MPLS VPN technology provides a solution to this dilemma.

Each VPN has its own routing and forwarding table in the router, so any customer or site that belongs to a VPN is provided access only to the set of routes contained within that table. Any PE router in the MPLS VPN network therefore contains a number of per-VPN routing tables and a global routing table that is used to reach other routers in the service provider network. Effectively, a number of virtual routers are created in a single physical router.

VRF-lite

VRF-lite is a feature that enables a service provider to support two or more VPNs, where IP addresses can be overlapped among the VPNs. VRF-lite uses input interfaces to distinguish routes for different VPNs and forms virtual packet-forwarding tables by associating one or more Layer 3 interfaces with each VRF. Interfaces in a VRF can be physical, such as Ethernet ports, or logical, such as VLAN switched virtual interfaces (SVIs). However, a Layer 3 interface cannot belong to more than one VRF at a time.


Note

VRF-lite interfaces must be Layer 3 interfaces.

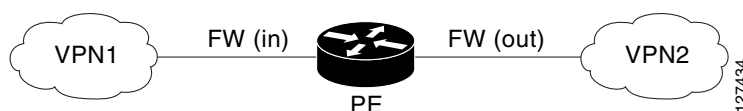
VRF-lite includes these devices:

- Customer edge (CE) devices provide customer access to the service provider network over a data link to one or more provider edge (PE) routers. The CE device advertises the site's local routes to the PE router and learns the remote VPN routes from it. A Catalyst 4500 switch can be a CE.
- Provider edge (PE) routers exchange routing information with CE devices by using static routing or a routing protocol such as BGP, RIPv1, or RIPv2.
- Provider routers (or core routers) are any routers in the service provider network that do not attach to CE devices.
- The PE is only required to maintain VPN routes for those VPNs to which it is directly attached, eliminating the need for the PE to maintain all of the service provider VPN routes. Each PE router maintains a VRF for each of its directly connected sites. Multiple interfaces on a PE router can be associated with a single VRF if all of these sites participate in the same VPN. Each VPN is mapped to a specified VRF. After learning local VPN routes from CEs, a PE router exchanges VPN routing information with other PE routers by using internal BGP (IBPG).

With VRF-lite, multiple customers can share one CE, and only one physical link is used between the CE and the PE. The shared CE maintains separate VRF tables for each customer, and switches or routes packets for each customer based on its own routing table. VRF-lite extends limited PE functionality to a CE device, giving it the ability to maintain separate VRF tables to extend the privacy and security of a VPN to the branch office.

In a VRF-to-VRF situation, if firewall policies are applied on both inbound and outbound interfaces as shown in [Figure 35](#), the firewall on the inbound interface takes precedence over the firewall on the outbound interface. If the incoming packets do not match against the firewall rules (that is, the inspection protocols) configured on the inbound interface, the firewall rule on the outbound interface is applied to the packet.

Figure 35 Firewall in a VRF-to-VRF Scenario



Per-VRF URL Filtering

The VRF Aware firewall supports per-VRF URL filtering. Each VPN can have its own URL filter server. The URL filter server typically is placed in the Shared Service segment of the corresponding VPN. (Each VPN has a VLAN segment in the Shared Service network.) It can also be placed at the customer's site.

Alerts and Audit Trails

CBAC generates real-time alerts and audit trails based on events tracked by the firewall. Enhanced audit trail features use SYSLOG to track all network transactions; recording time stamps, the source host, the destination host, ports used, and the total number of transmitted bytes, for advanced, session-based reporting. Real-time alerts send SYSLOG error messages to central management consoles upon detecting suspicious activity. Using CBAC inspection rules, you can configure alerts and audit trail information on a per-application protocol basis. For example, if you want to generate audit trail information for HTTP traffic, you can specify that in the CBAC rule covering HTTP inspection.

MPLS VPN

When used with MPLS, the VPN feature allows several sites to interconnect transparently through a service provider's network. One service provider network can support several IP VPNs. Each VPN appears to its users as a private network, separate from all other networks. Within a VPN, each site can send IP packets to any other site in the same VPN.

Each VPN is associated with one or more VPN VRF instances. A VRF consists of an IP routing table, a derived Cisco express forwarding (CEF) table, and a set of interfaces that use the forwarding table.

The router maintains a separate routing and CEF table for each VRF. This prevents information from being sent outside the VPN and allows the same subnet to be used in several VPNs without causing duplicate IP address problems.

The router using Multiprotocol BGP (MP-BGP) distributes the VPN routing information using the MP-BGP extended communities.

VRF-aware NAT

Network Address Translation (NAT) allows a single device, such as a router, to act as an agent between the Internet (or public network) and a local (or private) network. Although NAT systems can provide broad levels of security advantages, their main objective is to economize on address space.

NAT allows organizations to resolve the problem of IP address depletion when they have existing networks and need to access the Internet. Sites that do not yet possess NIC-registered IP addresses must acquire them. Cisco IOS NAT eliminates concern and bureaucratic delay by dynamically mapping thousands of hidden internal addresses to a range of easy-to-get addresses.

In general, a NAT system makes it more difficult for an attacker to determine the following:

- Number of systems running on a network
- Type of machines and operating systems they are running
- Network topology and arrangement

NAT integration with MPLS VPNs allows multiple MPLS VPNs to be configured on a single device to work together. NAT can differentiate which MPLS VPN it receives IP traffic from even if the MPLS VPNs are all using the same IP addressing scheme. This enables multiple MPLS VPN customers to share services while ensuring that each MPLS VPN is completely separate from the other.

MPLS service providers would like to provide value-added services such as Internet connectivity, domain name servers (DNS), and VoIP service to their customers. This requires that their customers IP addresses be different when reaching the services. Because MPLS VPN allows customers to use overlapped IP addresses in their networks, NAT must be implemented to make the services possible.

There are two approaches to implementing NAT in the MPLS VPN network. NAT can be implemented on the CE router, which is already supported by NAT, or it can be implemented on a PE router. The NAT Integration with MPLS VPNs feature enables the implementation of NAT on a PE router in an MPLS cloud.

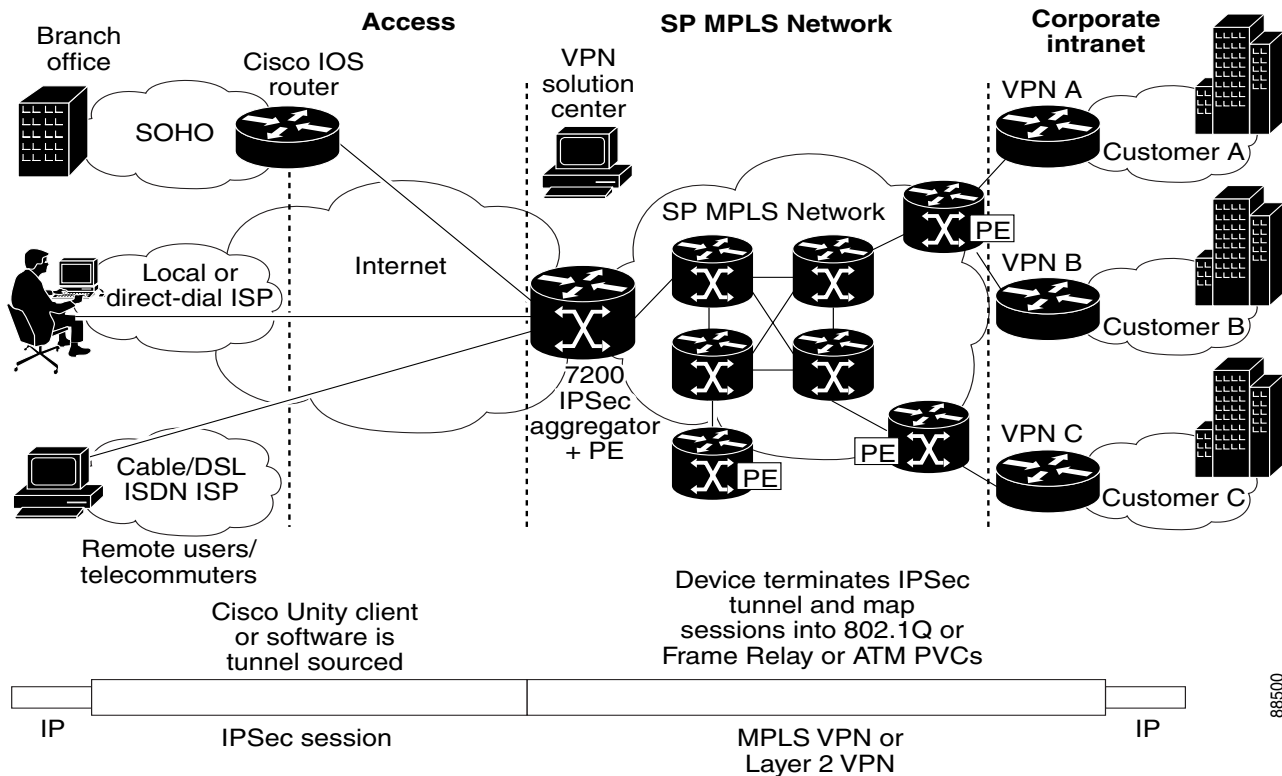
VRF-aware IPSec

The VRF-aware IPSec feature maps an IP Security (IPSec) tunnel to an MPLS VPN. Using the VRF-aware IPSec feature, you can map IPSec tunnels to VRF instances using a single public-facing address.

Each IPSec tunnel is associated with two VRF domains. The outer encapsulated packet belongs to a VRF domain called the Front Door VRF (FVRF). The inner, protected IP packet belongs to a domain called the Inside VRF (IVRF). In other words, the local endpoint of the IPSec tunnel belongs to the FVRF, whereas the source and destination addresses of the inside packet belong to the IVRF.

One or more IPSec tunnels can terminate on a single interface. The FVRF of all these tunnels is the same and is set to the VRF that is configured on that interface. The IVRF of these tunnels can be different and depends on the VRF that is defined in the Internet Security Association and Key Management Protocol (ISAKMP) profile that is attached to a crypto map entry.

[Figure 36](#) illustrates a scenario showing IPSec to MPLS and Layer 2 VPNs.

Figure 36 *IPSec-to-MPLS and Layer 2 VPNs*

88500

VRF Aware Cisco IOS Firewall Deployment

A firewall can be deployed at many points within the network to protect VPN sites from Shared Service (or the Internet) and vice versa. The following firewall deployments are described:

- [Distributed Network Inclusion of VRF Aware Cisco IOS Firewall, page 7](#)
- [Hub-and-Spoke Network Inclusion of VRF Aware Cisco IOS Firewall, page 9](#)

Distributed Network Inclusion of VRF Aware Cisco IOS Firewall

A VRF Aware Cisco IOS Firewall in a distributed network has the following advantages:

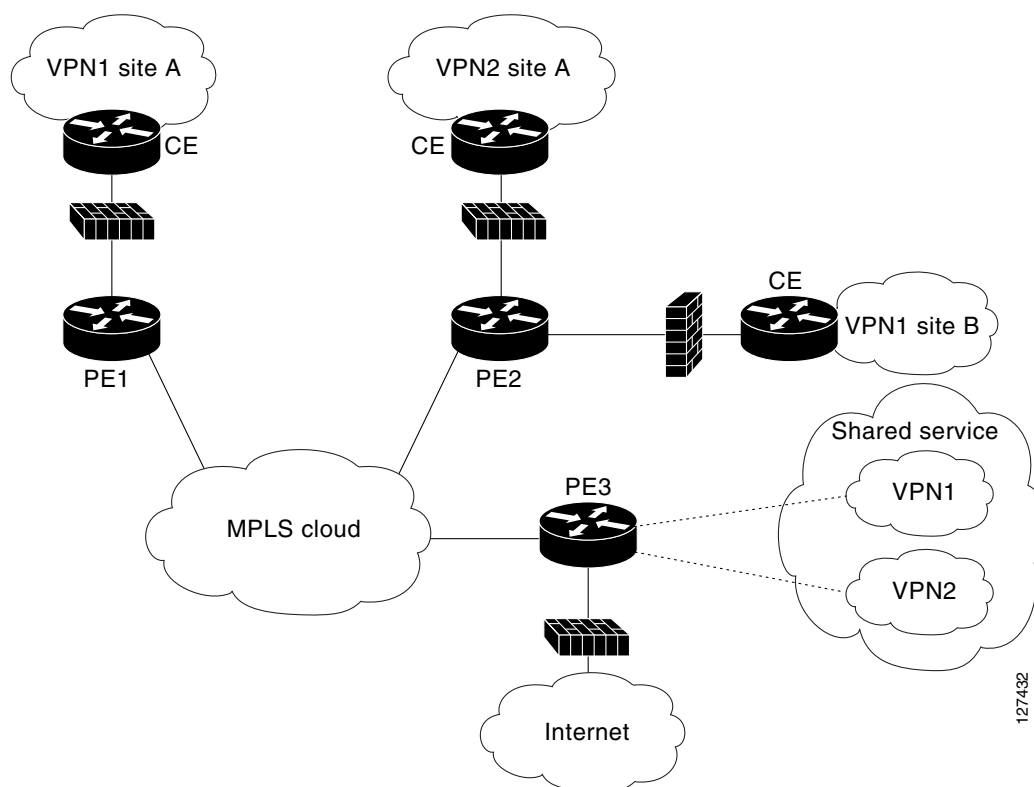
- The firewall is distributed across the MPLS core, so the firewall processing load is distributed to all ingress PE routers.
- VPN Firewall features can be deployed in the inbound direction.
- Shared Service is protected from the VPN site at the ingress PE router; therefore, malicious packets from VPN sites are filtered at the ingress PE router before they enter the MPLS core.

However, the following disadvantages exist:

- There is no centralized firewall deployment, which complicates the deployment and management of the firewall.
- Shared Service firewall features cannot be deployed in the inbound direction.
- The MPLS core is open to the Shared Service. Therefore, malicious packets from Shared Service are filtered only at the ingress PE router after traveling through all core routers.

Figure 37 illustrates a typical situation in which an SP offers firewall services to VPN customers VPN1 and VPN2, thereby protecting VPN sites from the external network (for example, Shared Services and the Internet) and vice versa.

Figure 37 *Distributed Network*



In this example, VPN1 has two sites, Site A and Site B, that span across the MPLS core. Site A is connected to PE1, and Site B is connected to PE2. VPN2 has only one site that is connected to PE2.

Each VPN (VPN1 and VPN2) has the following:

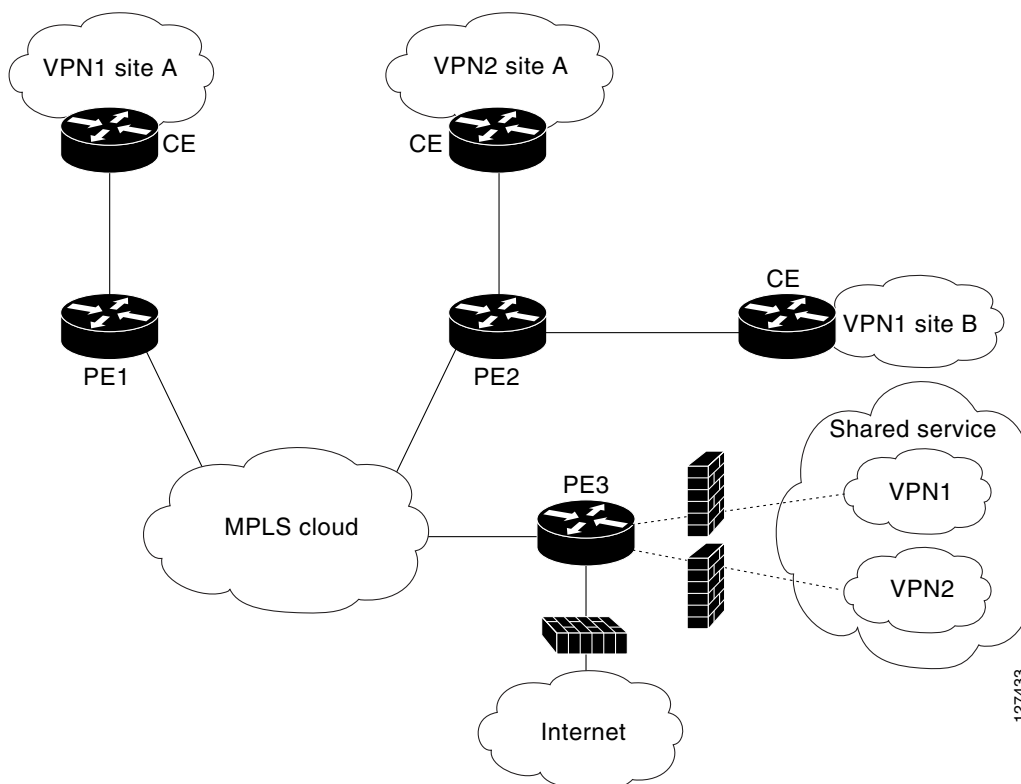
- A VLAN segment in the Shared Service that is connected to the corresponding VLAN subinterface on PE3.
- Internet access through the PE3 router that is connected to the Internet

A distributed network requires the following firewall policies:

- **VPN Firewall (VPN1-FW and VPN2-FW)**—Inspects VPN-generated traffic that is destined to Shared Service or the Internet and blocks all non-firewall traffic that is coming from outside (Shared Service or the Internet), thereby protecting the VPN sites from outside traffic. This firewall typically is deployed on the VRF interface of the ingress PE router that is connected to the VPN site being protected. It is deployed in the inbound direction because the VRF interface is inbound to the VPN site being protected.
- **Shared Service Firewall (SS-FW)**—Inspects Shared Service-originated traffic that is destined to VPN sites and blocks all non-firewall traffic that is coming from outside (the VPN site), thereby protecting the Shared Service network from VPN sites. This firewall typically is deployed on the VRF interface of the ingress PE router that is connected to the VPN site from where the Shared Service is being protected. It is deployed in the outbound direction because the VRF interface is outbound to the Shared Service that is being protected.
- **Generic-VPN Firewall (GEN-VPN-FW)**—Inspects VPN-generated traffic that is destined to the Internet and blocks all non-firewall traffic that is coming from the Internet, thereby protecting all VPNs from the Internet. This firewall typically is deployed on the Internet-facing interface of the PE router that is connected to the Internet. It is deployed in the outbound direction because the Internet-facing interface is outbound to VPNs being protected.
- **Internet Firewall (INET-FW)**—Inspects Internet-generated traffic that is destined to Shared Service and blocks all non-firewall traffic that is coming from VPNs or Shared Service, thereby protecting the Internet from VPNs. This firewall typically is deployed on the Internet-facing interface of the PE router that is connected to the Internet. It is deployed in the inbound direction because the Internet-facing interface is inbound to the Internet being protected.

Hub-and-Spoke Network Inclusion of VRF Aware Cisco IOS Firewall

[Figure 38](#) illustrates a hub-and-spoke network where the firewalls for all VPN sites are applied on the ingress PE router PE3 that is connected to the Shared Service.

Figure 38 *Hub-and-Spoke Network*

Typically each VPN has a VLAN and/or VRF subinterface connected to the Shared Service. When a packet arrives from an MPLS interface, the inner tag represents the VPN-ID. MPLS routes the packet to the corresponding subinterface that is connected to Shared Service.

A Hub-and-Spoke network requires the following firewall policies:

- **VPN Firewall (VPN1-FW and VPN2-FW)**—Inspects VPN-generated traffic that is destined to Shared Service and blocks all non-firewall traffic that is coming from Shared Service, thereby protecting the VPN sites from Shared Service traffic. This firewall typically is deployed on the VLAN subinterface of the egress PE router that is connected to the Shared Service network. It is deployed in the outbound direction because the VLAN interface is outbound to the VPN site being protected.
- **Shared Service Firewall (SS-FW)**—Inspects Shared Service originated traffic that is destined to the VPN/Internet and blocks all non-firewall traffics that is coming from outside, thereby protecting the Shared Service network from VPN/Internet traffic. This firewall typically is deployed on the VLAN interface of the egress PE router that is connected to the Shared Service being protected. It is deployed in the inbound direction because the VLAN interface is inbound to the Shared Service being protected.

- Generic-VPN firewall (GEN-VPN-FW)—Inspects VPN-generated traffic that is destined to the Internet and blocks all non-firewall traffic that is coming from the Internet, thereby protecting all VPNs from the Internet. This firewall typically is deployed on the Internet-facing interface of the PE router that is connected to the Internet. It is deployed in the outbound direction because the Internet-facing interface is outbound to the VPNs being protected.
- Internet firewall (INET-FW)—Inspects Internet-generated traffic that is destined to Shared Service and blocks all non-firewall traffic that is coming from VPNs or Shared Service, thereby protecting the Internet from VPNs. This firewall typically is deployed on the Internet-facing interface of the PE router that is connected to the Internet. It is deployed in the inbound direction because the Internet-facing interface is inbound to the Internet being protected.

How to Configure VRF Aware Cisco IOS Firewall

This section contains the following procedures:

- [Configuring and Checking ACLs to Ensure that Only Inspected Traffic Can Pass Through the Firewall and that Non-Firewall Traffic is Blocked, page 11](#) (required)
- [Creating and Naming Firewall Rules and Applying the Rules to the Interface, page 12](#) (required)
- [Identifying and Setting Firewall Attributes, page 13](#) (optional)

Configuring and Checking ACLs to Ensure that Only Inspected Traffic Can Pass Through the Firewall and that Non-Firewall Traffic is Blocked

To configure ACLs and verify that only inspected traffic can pass through the firewall, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list extended** *access-list-name*
4. **interface** *interface-type*
5. **ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**}
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip access-list extended <i>access-list-name</i> Example: Router(config)# ip access-list extended vpn-acl	Defines an extended IP ACL to block non-firewall traffic in both inbound and outbound directions.
Step 4	interface <i>interface-type</i> Example: Router(config)# interface ethernet0/1.10	Enters interface configuration mode and specifies an interface that is associated with a VRF.
Step 5	ip access-group { <i>access-list-number</i> <i>access-list-name</i> } { in out } Example: Router(config-if)# ip access-group vpn-acl in	Controls access to an interface. Applies the previously defined IP access list to a VRF interface whose non-firewall traffic is blocked.
Step 6	exit Example: Router(config-if)# exit	Exits interface configuration mode. Returns to global configuration mode.

Creating and Naming Firewall Rules and Applying the Rules to the Interface

To create and name firewall rules and apply the rules to the interface, perform the following steps.

SUMMARY STEPS

- enable**
- configure terminal**
- ip inspect name** *inspection-name* [**parameter** *max-sessions* *number*] *protocol* [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*]
- interface** *interface-id*
- ip inspect** *rule-name* {**in** | **out**}
- exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip inspect name inspection-name [parameter max-sessions number] protocol [alert {on off}] [audit-trail {on off}] [timeout seconds] Example: Router(config)# ip inspect name vpn_fw ftp	Defines a set of inspection rules.
Step 4	interface interface-id Example: Router(config)# interface ethernet0/1.10	Enters interface configuration mode and specifies an interface that is associated with a VRF.
Step 5	ip inspect rule-name {in out} Example: Router(config-if)# ip inspect vpn_fw in	Applies the previously defined inspection role to a VRF interface whose traffic needs to be inspected.
Step 6	exit Example: Router(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.

Identifying and Setting Firewall Attributes

To identify and set firewall attributes, perform the following steps.

SUMMARY STEPS

1. enable
2. configure terminal
3. ip inspect tcp max-incomplete host number block-time minutes [vrf vrf-name]
4. exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip inspect tcp max-incomplete host <i>number</i> block-time <i>minutes</i> [vrf <i>vrf-name</i>] Example: Router(config)# ip inspect tcp max-incomplete host 256 vrf bank-vrf	Specifies threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.
Step 4	exit Example: Router(config)# exit	Exits global configuration mode.

Verifying the VRF Aware Cisco IOS Firewall Configuration and Functioning

Verify the configuration and functioning of the firewall by entering the commands shown below. For detailed descriptions of these commands and other verification commands, see the [“Command Reference” section on page 26](#).

SUMMARY STEPS

1. **show ip inspect** {name *inspection-name* | config | interfaces | session [detail] | statistics | all}[vrf *vrf-name*]
2. **show ip urlfilter** {config | cache | statistics} [vrf *vrf-name*]

DETAILED STEPS

Step 1 **show ip inspect** {name *inspection-name* | config | interfaces | session [detail] | statistics | all}[vrf *vrf-name*]

Use this command to view the firewall configurations, sessions, statistics, and so forth, pertaining to a specified VRF. For example, to view the firewall sessions pertaining to the VRF bank, enter the following command:

```
Router# show ip inspect interfaces vrf bank
```

Step 2 **show ip urlfilter** {config | cache | statistics} [vrf *vrf-name*]

Use this command to view the configurations, cache entries, statistics, and so forth, pertaining to a specified VRF. For example, to view the URL filtering statistics pertaining to the VRF bank, enter the following command:

```
Router# show ip urlfilter statistics vrf bank
```

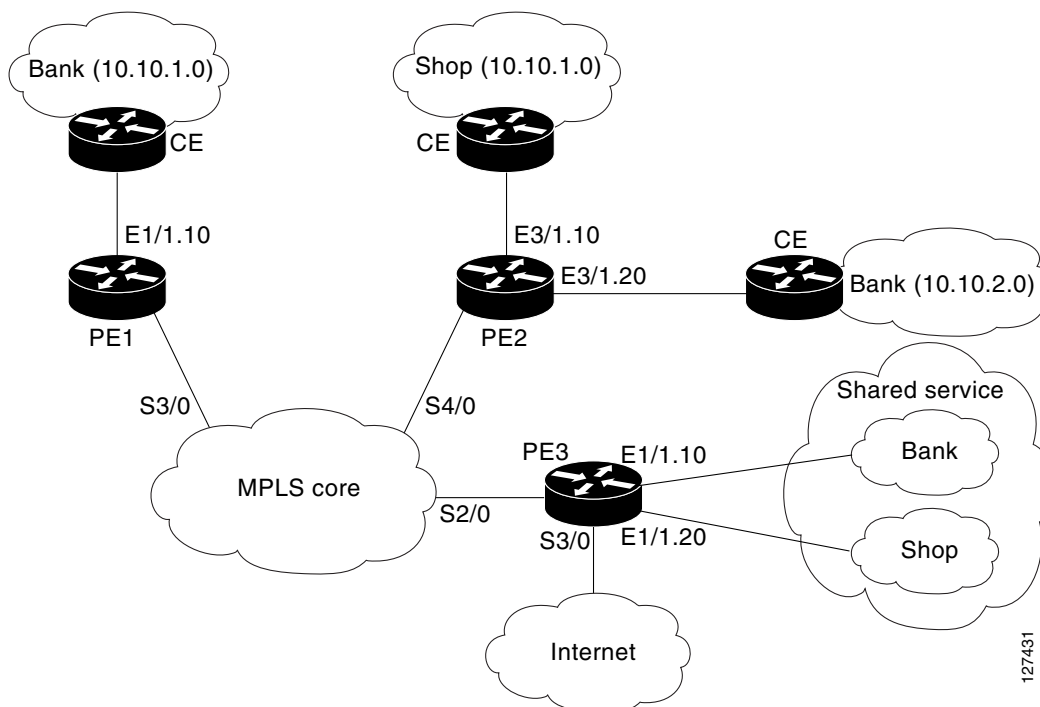
Configuration Examples for VRF Aware Cisco IOS Firewall

In the example illustrated in [Figure 39](#), a service provider offers firewall service to VPN customers **Bank** and **Shop**. The Bank VPN has the following two sites in an MPLS network:

- Site connected to PE1, whose network address is 10.10.1.0/24
- Site connected to PE2, whose network address is 10.10.2.0/24

The Bank VPN also has a VLAN network segment in Shared Service that is connected to PE3.

The Shop VPN has only one site, which is connected to PE4. The network address 10.10.1.0/24 is the same network address to which the Bank VPN site is connected.

Figure 39 *VPN with Two Sites Across MPLS Network*

Each VPN needs the following two firewalls:

- VPN firewall to protect the VPN site from Shared Services
- Shared Service (SS) firewall to protect SS from the VPN site

In addition, the following two firewalls are required:

- Internet firewall to protect VPNs from the Internet
- Generic VPN firewall to protect the Internet from VPNs

In this example, the security policies for Bank and Shop VPNs are as follows:

- Bank VPN Firewall—bank_vpn_fw (Inspects FTP, HTTP, and ESMTP protocols)
- Bank SS Firewall—bank_ss_fw (Inspects ESMTP protocol)
- Shop VPN Firewall—shop_vpn_fw (Inspects HTTP and RTSP protocols)
- Shop SS Firewall—shop_ss_fw (Inspects H323 protocol)

The security policies for the Internet firewall and generic VPN firewall are as follows:

- Internet firewall—innet_fw (Inspects HTTP and ESMTP protocols)
- Generic VPN firewall—gen_vpn_fw (Inspects FTP, HTTP, ESMTP, and RTSP protocols)

DISTRIBUTED NETWORK**PE1:**

```

! VRF instance for the Bank VPN
ip vrf bank
rd 100:10
route-target export 100:10
route-target import 100:10
!
! VPN Firewall for Bank VPN protects Bank VPN from Shared Service
ip inspect name bank_vpn_fw ftp
ip inspect name bank_vpn_fw http
ip inspect name bank_vpn_fw esmtp
!
! Shared Service firewall for Bank VPN protects Shared Service from Bank VPN
ip inspect name bank_ss_fw esmtp
!
! VRF interface for the Bank VPN
interface ethernet0/1.10
!
! description of VPN site Bank to PE1
encapsulation dot1Q 10
ip vrf forwarding bank
ip address 10.10.1.2 255.255.255.0
ip access-group bank_ss_acl in
ip access-group bank_vpn_acl out
ip inspect bank_vpn_fw in
ip inspect bank_ss_fw out
!
! MPLS interface
interface Serial13/0
ip unnumbered Loopback0
tag-switching ip
serial restart-delay 0
!
! ACL that protects the VPN site Bank from Shared Service
ip access-list extended bank_vpn_acl
permit ip 10.10.2.0 0.0.0.255 10.10.1.0 0.0.0.255
permit tcp any any eq smtp
deny ip any any log
!
! ACL that protects Shared Service from VPN site Bank
ip access-list extended bank_ss_acl
permit ip 10.10.1.0 0.0.0.255 10.10.2.0 0.0.0.255
permit tcp any any eq ftp
permit tcp any any eq http
permit tcp any any eq smtp
deny ip any any log

```

PE2:

```

! VRF instance for the Bank VPN
ip vrf bank
rd 100:10
route-target export 100:10
route-target import 100:10
!
! VRF instance for the Shop VPN
ip vrf shop
rd 200:20
route-target export 200:20
route-target import 200:20
!

```

```

! VPN firewall for Bank BPN protects Bank VPN from Shared Service
ip inspect name bank_vpn_fw ftp
ip inspect name bank_vpn_fw http
ip inspect name bank_vpn_fw esmtp
!
! Shared Service firewall for Bank VPN protects Shared Service from Bank VPN
ip inspect name bank_ss_fw esmtp
!
! VPN firewall for Shop VPN protects Shop VPN from Shared Service
ip inspect name shop_vpn_fw http
ip inspect name shop_vpn_fw rtsp
!
! Shared Service firewall for Shop VPN protects Shared Service from Shop VPN
ip inspect name shop_ss_fw h323
!
! VRF interface for the Bank VPN
interface Ethernet3/1.10
!
! description of VPN site Bank to PE2
encapsulation dot1Q 10
ip vrf forwarding bank
ip address 10.10.2.2 255.255.255.0
ip access-group bank_ss_acl in
ip access-group bank_vpn_acl out
ip inspect bank_vpn_fw in
ip inspect bank_ss_fw out
!
interface Ethernet3/1.20
!
! description of VPN site Shop to PE2
encapsulation dot1Q 20
ip vrf forwarding shop
ip address 10.10.1.2 255.255.255.0
ip access-group shop_ss_acl in
ip access-group shop_vpn_acl out
ip inspect shop_vpn_fw in
ip inspect shop_ss_fw out
!
interface Serial4/0
ip unnumbered Loopback0
tag-switching ip
serial restart-delay 0
!
! ACL that protects the VPN site Bank from Shared Service
ip access-list extended bank_vpn_acl
permit ip 10.10.1.0 0.0.0.255 10.10.2.0 0.0.0.255
permit tcp any any eq smtp
deny ip any any log
!
! ACL that protects Shared Service from VPN site Bank
ip access-list extended bank_ss_acl
permit ip 10.10.2.0 0.0.0.255 10.10.1.0 0.0.0.255
permit tcp any any eq ftp
permit tcp any any eq http
permit tcp any any eq smtp
deny ip any any log
!

```

```

! ACL that protects VPN site Shop from Shared Service
ip access-list extended shop_vpn_acl
  permit tcp any any eq h323
  deny ip any any log
!
ip access-list extended shop_ss_acl
  permit tcp any any eq http
  permit tcp any any eq rtsp
  deny ip any any log

```

PE3:

```

! VRF instance for the Bank VPN
ip vrf bank
rd 100:10
route-target export 100:10
route-target import 100:10
!
! VRF instance for the Shop VPN
ip vrf shop
rd 200:20
route-target export 200:20
route-target import 200:20
!
! Generic VPN firewall to protect Shop and Bank VPNs from internet
ip inspect name gen_vpn_fw esmtp
ip inspect name gen_vpn_fw ftp
ip inspect name gen_vpn_fw http
ip inspect name gen_vpn_fw rtsp
!
! Internet firewall to prevent malicious traffic from being passed
! to internet from Bank and Shop VPNs
ip inspect name inet_fw esmtp
ip inspect name inet_fw http
!
! VRF interface for the Bank VPN
interface Ethernet1/1.10
!
! Description of Shared Service to PE3
encapsulation dot1Q 10
ip vrf forwarding bank
ip address 10.10.1.50 255.255.255.0
!
! VRF interface for the Shop VPN
interface Ethernet1/1.20
!
! Description of Shared Service to PE3
encapsulation dot1Q 20
ip vrf forwarding shop
ip address 10.10.1.50 255.255.255.0
!
interface Serial2/0
  ip unnumbered Loopback0
  tag-switching ip
  serial restart-delay 0
!
! VRF interface for the Bank VPN
interface Serial3/0
!
! Description of Internet-facing interface
ip address 192.168.10.2 255.255.255.0
ip access-group inet_acl out
ip access-group gen_vpn_acl in
ip inspect gen_vpn_fw out

```

```

ip inspect inet_fw in
!
! ACL that protects the Bank and Shop VPNs from internet
ip access-list extended gen_vpn_acl
  permit tcp any any eq smtp
  permit tcp any any eq www
  deny ip any any log
!
! ACL that protects internet from Bank and Shop VPNs
ip access-list extended inet_acl
  permit tcp any any eq ftp
  permit tcp any any eq http
  permit tcp any any eq smtp
  permit tcp any any eq rtsp
  deny ip any any log

```

HUB-AND-SPOKE NETWORK

PE3:

```

! VRF instance for the VPN Bank
ip vrf bank
rd 100:10
route-target export 100:10
route-target import 100:10
!
! VRF instance for the VPN Shop
ip vrf shop
rd 200:20
route-target export 200:20
route-target import 200:20
!
! VPN firewall for Bank BPN protects Bank VPN from Shared Service
ip inspect name bank_vpn_fw ftp
ip inspect name bank_vpn_fw http
ip inspect name bank_vpn_fw esmtp
!
! Shared Service firewall for Bank VPN protects Shared Service from Bank VPN
ip inspect name bank_ss_fw esmtp
!
! VPN firewall for Shop VPN protects Shop VPN from Shared Service
ip inspect name shop_vpn_fw http
ip inspect name shop_vpn_fw rtsp
!
! Shared Service firewall for Shop VPN protects Shared Service from Shop VPN
ip inspect name shop_ss_fw h323
!
! Generic VPN firewall protects Shop and Bank VPNs from internet
ip inspect name gen_vpn_fw esmtp
ip inspect name gen_vpn_fw ftp
ip inspect name gen_vpn_fw http
ip inspect name gen_vpn_fw rtsp
!
! Internet firewall prevents malicious traffic from being passed
! to internet from Bank and Shop VPNs
ip inspect name inet_fw esmtp
ip inspect name inet_fw http
!
! VRF interface for the Bank VPN
interface Ethernet1/1.10
!
! description of Shared Service to PE3
encapsulation dot1Q 10

```

```

ip vrf forwarding bank
ip address 10.10.1.50 255.255.255.0
ip access-group bank_ss_acl out
ip access-group bank_vpn_acl in
ip inspect bank_vpn_fw out
ip inspect bank_ss_fw in
!
! VRF interface for the Shop VPN
interface Ethernet1/1.20
!
! description of Shared Service to PE3
encapsulation dot1Q 20
ip vrf forwarding shop
ip address 10.10.1.50 255.255.255.0
ip access-group shop_ss_acl out
ip access-group shop_vpn_acl in
ip inspect shop_vpn_fw out
ip inspect shop_ss_fw in
!
interface Serial2/0
  ip unnumbered Loopback0
  tag-switching ip
  serial restart-delay 0
!
! VRF interface for the Bank VPN
interface Serial3/0
!
! description of Internet-facing interface
ip address 192.168.10.2 255.255.255.0
ip access-group inet_acl out
ip access-group gen_vpn_acl in
ip inspect gen_vpn_fw out
ip inspect inet_fw in
!
! ACL that protects the VPN site Bank from Shared Service
ip access-list extended bank_vpn_acl
  permit tcp any any eq smtp
  deny ip any any log
!
! ACL that protects Shared Service from VPN site Bank
ip access-list extended bank_ss_acl
  permit tcp any any eq ftp
  permit tcp any any eq http
  permit tcp any any eq smtp
  deny ip any any log
!
! ACL that protects VPN site Shop from Shared Service
ip access-list extended shop_vpn_acl
  permit tcp any any eq h323
  deny ip any any log
!
ip access-list extended shop_ss_acl
  permit tcp any any eq http
  permit tcp any any eq rtsp
  deny ip any any log
!
! ACL that protects the Bank and Shop VPNs from internet
ip access-list extended gen_vpn_acl
  permit tcp any any eq smtp
  permit tcp any any eq www
  deny ip any any log
!
! ACL that protects internet from Bank and Shop VPNs
ip access-list extended inet_acl

```

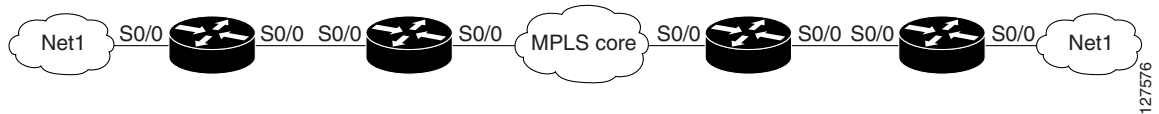
```

permit tcp any any eq ftp
permit tcp any any eq http
permit tcp any any eq smtp
permit tcp any any eq rtsp
deny ip any any log

```

In the example illustrated in [Figure 40](#), the Cisco IOS Firewall is configured on PE1 on the VRF interface E3/1. The host on NET1 wants to reach the server on NET2.

Figure 40 Sample VRF Aware Cisco IOS Firewall Network



The configuration steps are followed by a sample configuration and log messages.

1. Configure VRF on PE routers.
2. Ensure that your network supports MPLS traffic engineering.
3. Confirm that the VRF interface can reach NET1 and NET2.
4. Configure the VRF Aware Cisco IOS Firewall.
 - a. Configure and apply ACLs.
 - b. Create Firewall rules and apply them to the VRF interface.
5. Check for VRF firewall sessions.

VRF Configuration on PE1

```

! configure VRF for host1
ip cef
ip vrf vrf1
rd 100:1
route-target export 100:1
route-target import 100:1
exit
end
!
! apply VRF to the interface facing CE
interface ethernet3/1
ip vrf forwarding vrf1
ip address 190.1.1.2 255.255.0.0
!
! make the interface facing the MPLS network an MPLS interface
interface serial2/0
mpls ip
ip address 191.171.151.1 255.255.0.0
!
! configure BGP protocol for MPLS network
router bgp 100
no synchronization
bgp log-neighbor-changes
neighbor 191.171.151.2 remote-as 100
neighbor 191.171.151.2 update-source serial2/0
no auto-summary
address-family vpnv4
neighbor 191.171.151.2 activate
neighbor 191.171.151.2 send-community both
exit-address-family

```

```
address-family ipv4 vrf vrf1
redistribute connected
redistribute static
no auto-summary
no synchronization
exit-address-family
!
! configure VRF static route to reach CE network
ip route vrf vrf1 192.168.4.0 255.255.255.0 190.1.1.1
```

VRF Configuration on PE2

```
! configure VRF for host2
ip cef
ip vrf vrf1
rd 100:1
route-target export 100:1
route-target import 100:1
!
! apply VRF on CE-facing interface
interface fastethernet0/0
ip vrf forwarding vrf1
ip address 193.1.1.2 255.255.255.0
!
! make MPLS network-facing interface an MPLS interface
interface serial1/0
mpls ip
ip address 191.171.151.2 255.255.0.0
!
! configure BGP protocol for MPLS network
router bgp 100
no synchronization
bgp log-neighbor-changes
neighbor 191.171.151.1 remote-as 100
neighbor 191.171.151.1 update-source serial1/0
no auto-summary
address-family vpnv4
neighbor 191.171.151.1 activate
neighbor 191.171.151.1 send-community both
exit-address-family
address-family ipv4 vrf vrf1
redistribute connected
redistribute static
no auto-summary
no synchronization
exit-address-family

!configure VRF static route to reach CE network
ip route vrf vrf1 192.168.4.0 255.255.255.0 193.1.1.1
```

Configuration on CE1

```
interface e0/1
ip address 190.1.1.1 255.255.255.0

interface e0/0
ip address 192.168.4.2 255.255.255.0

ip route 192.168.104.0 255.255.255.0 190.1.1.2
```

Configuration on CE2

```

interface e0/1
ip address 190.1.1.1 255.255.255.0

interface e0/0
ip address 192.168.4.2 255.255.255.0

ip route 192.168.4.0 255.255.255.0 193.1.1.2

```

Configure Firewall on PE1 and Apply on the VRF Interface

```

! configure ACL so that NET2 cannot access NET1
ip access-list extended 105
permit tcp any any fragment
permit udp any any fragment
deny tcp any any
deny udp any any
permit ip any any
!
! apply ACL to VRF interface on PE1
interface ethernet3/1
ip access-group 105 out
!
! configure firewall rule
ip inspect name test tcp
!
! apply firewall rule on VRF interface
interface ethernet3/1
ip inspect test in

```

Check for VRF Firewall Sessions When Host on NET1 Tries to Telnet to Server on NET2

```

show ip inspect session vrf vrf1
Established Sessions
  Session 659CE534 (192.168.4.1:38772)=>(192.168.104.1:23) tcp SIS_OPEN
!
! checking for ACLs
show ip inspect session detail vrf vrf1 | include ACL 105
  Out SID 192.168.104.1[23:23]=>192.168.4.1[38772:38772] on ACL 105
(34 matches)

```

Additional References

The following sections provide references related to VRF Aware Cisco IOS Firewall.

Related Documents

Related Topic	Document Title
VRF-lite	<ul style="list-style-type: none"> <i>Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, Release 12.2</i>
MPLS VPN	<ul style="list-style-type: none"> <i>Configuring a Basic MPLS VPN, Document ID 13733</i>
VRF Aware IPSec	<ul style="list-style-type: none"> <i>VRF-Aware IPSec</i> feature module, Release 12.2(15)T <i>Cisco IOS Security Configuration Guide, Release 12.3</i> <i>Cisco IOS Security Command Reference, Release 12.3T</i>
VRF management	<ul style="list-style-type: none"> <i>Cisco 12000/10720 Router Manager User's Guide, Release 3.2</i>
NAT	<ul style="list-style-type: none"> <i>NAT and Stateful Inspection of Cisco IOS Firewall, White Paper</i> <i>Configuring Network Address Translation: Getting Started</i>—Document ID 13772

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **clear ip urlfilter cache**
- **ip inspect alert-off**
- **ip inspect audit trail**
- **ip inspect dns-timeout**
- **ip inspect max-incomplete high**
- **ip inspect max-incomplete low**
- **ip inspect name**
- **ip inspect one-minute high**
- **ip inspect one-minute low**
- **ip inspect tcp finwait-time**
- **ip inspect tcp idle-time**
- **ip inspect tcp max-incomplete host**
- **ip inspect tcp synwait-time**
- **ip inspect udp idle-time**
- **ip urlfilter alert**
- **ip urlfilter allowmode**
- **ip urlfilter audit-trail**
- **ip urlfilter cache**
- **ip urlfilter exclusive-domain**
- **ip urlfilter exclusive-domain**
- **ip urlfilter max-request**
- **ip urlfilter max-resp-pak**
- **ip urlfilter server vendor**

- **ip urlfilter urlf-server-log**
- **show ip inspect**
- **show ip urlfilter cache**
- **show ip urlfilter config**
- **show ip urlfilter statistics**

Glossary

CE router—customer edge router. A router that is part of a customer network and that interfaces to a provider edge (PE) router.

CBAC—Context-Based Access Control. A protocol that provides internal users with secure access control for each application and for all traffic across network perimeters. CBAC enhances security by scrutinizing both source and destination addresses and by tracking each application's connection status.

data authentication—Refers to one or both of the following: data integrity, which verifies that data has not been altered, or data origin authentication, which verifies that the data was actually sent by the claimed sender.

data confidentiality—A security service where the protected data cannot be observed.

edge router—A router that turns unlabeled packets into labeled packets, and vice versa.

firewall—A router or access server, or several routers or access servers, designated as a buffer between any connected public networks and a private network. A firewall router uses access lists and other methods to ensure the security of the private network.

inspection rule—A rule that specifies what IP traffic (which application-layer protocols) will be inspected by CBAC at an interface.

intrusion detection—The Cisco IOS Firewall's Intrusion Detection System (Cisco IOS IDS) identifies the most common attacks, using signatures to detect patterns of misuse in network traffic.

IPSec—IP Security Protocol. A framework of open standards developed by the Internet Engineering Task Force (IETF). IPSec provides security for transmission of sensitive data over unprotected networks such as the Internet.

managed security services—A comprehensive set of programs that enhance service providers' abilities to meet the growing demands of their enterprise customers. Services based on Cisco solutions include managed firewall, managed VPN (network based and premises based), and managed intrusion detection.

NAT—Network Address Translation. Translates a private IP address used inside the corporation to a public, routable address for use outside of the corporation, such as the Internet. NAT is considered a one-to-one mapping of addresses from private to public.

PE router—provider edge router. A router that is part of a service provider's network and is connected to a customer edge (CE) router.

skinny—Skinny Client Control Protocol (SCCP). A protocol that enables CBAC to inspect Skinny control packets that are exchanged between a Skinny client and the Call Manager (CM); CBAC then configures the router (also known as the Cisco IOS Firewall) to enable the Skinny data channels to traverse through the router.

traffic filtering—A capability that allows you to configure CBAC to permit specified TCP and UDP traffic through a firewall only when the connection is initiated from within the network you want to protect. CBAC can inspect traffic for sessions that originate from either side of the firewall.

traffic inspection—CBAC inspection of traffic that travels through the firewall to discover and manage state information for TCP and UDP sessions. This state information is used to create temporary openings in the firewall's access lists to allow return traffic and additional data connections for permissible sessions (sessions that originated from within the protected internal network).

UDP—User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols.

VPN—Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses “tunneling” to encrypt all information at the IP level.

vrf—A VPN routing/forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a provider edge (PE) router.

VRF table—A table that stores routing data for each VPN. The VRF table defines the VPN membership of a customer site attached to the network access server (NAS). Each VRF table comprises an IP routing table, a derived Cisco Express Forwarding (CEF) table, and guidelines and routing protocol parameters that control the information that is included in the routing table.

**Note**

Refer to *Internetworking Terms and Acronyms* for terms not included in this glossary.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Zone-Based Policy Firewall

First Published: February 22, 2006

Last Updated: July 11, 2008

This module describes the Cisco IOS unidirectional firewall policy between groups of interfaces known as zones. Previously, Cisco IOS firewalls were configured as an inspect rule only on interfaces. Traffic entering or leaving the configured interface was inspected based on the direction that the “inspect” rule was applied.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Zone-Based Policy Firewall”](#) section on page 46.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Zone-Based Policy Firewall, page 2](#)
- [Restrictions for Zone-Based Policy Firewall, page 2](#)
- [Information About Zone-Based Policy Firewall, page 2](#)
- [How to Configure Zone-Based Policy Firewall, page 11](#)
- [Configuration Examples for Zone-Based Policy Firewall, page 41](#)
- [Additional References, page 43](#)
- [Feature Information for Zone-Based Policy Firewall, page 46](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Zone-Based Policy Firewall

Before you create zones, think about what should constitute the zones. The general guideline is that you should group together interfaces that are similar when they are viewed from a security perspective.

Restrictions for Zone-Based Policy Firewall

If a configuration includes both security zones and inspect rules on interfaces (the old methodology), the configuration may work, but that type of configuration is not recommend.

Information About Zone-Based Policy Firewall

To configure a zone-based policy firewall, you should understand the following concepts:

- [Top-level Class Maps and Policy Maps, page 2](#)
- [Application-specific Class Maps and Policy Maps, page 3](#)
- [Zones, page 3](#)
- [Security Zones, page 3](#)
- [Zone-Pairs, page 4](#)
- [Zones and Inspection, page 6](#)
- [Zones and ACLs, page 6](#)
- [Zones and VRF Aware Firewall, page 6](#)
- [Zones and Transparent Firewall, page 7](#)
- [Overview of Security Zone Firewall Policies, page 7](#)
- [Class Maps and Policy Maps for Zone-Based Policy Firewalls, page 8](#)
- [Parameter Maps, page 11](#)

Top-level Class Maps and Policy Maps

Top-level class maps allow you to identify the traffic stream at a high level. This is accomplished by using **match access-group** and **match protocol** commands. These class maps cannot be used to classify traffic at the application level (the Layer 7 level). Top-level class maps are also referred to as Layer 3 and Layer 4 class-maps.

Top-level policy maps allow you to define high-level actions such as **inspect**, **drop**, **pass**, and **urlfilter**. You can attach the maps to a target (zone-pair). The maps can contain “child” policies that are also known as application-specific Layer 7 policies.

**Note**

Only inspect class maps can be used in inspect policy maps.

Application-specific Class Maps and Policy Maps

Application-specific class maps allow you to identify traffic based on the attributes of a given protocol. All the match conditions in these class maps are specific to an application (for example, HTTP or SMTP). Application-specific class maps are identified by an additional subtype that generally is the protocol name (HTTP or SMTP) in addition to the type **inspect**.

Application-specific policy maps are used to specify a policy for an application protocol. For example, if you want to drop HTTP traffic with URI lengths exceeding 256 bytes, you must configure an HTTP policy map to do that. Application-specific policy maps cannot be attached directly to a target (zone-pair). They must be configured as “child” policies in a top-level Layer 3 or Layer 4 policy map.

Zones

A zone is a group of interfaces that have similar functions or features. They provide a way for you to specify *where* a Cisco IOS firewall is applied.

For example, on a router, interfaces Ethernet 0/0 and Ethernet 0/1 may be connected to the local LAN. These two interfaces are similar because they represent the internal network, so they can be grouped into a zone for firewall configurations.

Traffic between interfaces in the same zone is not be subjected to any policy. The traffic passes freely.

Firewall zones are used for security features.

Security Zones

A security zone is a group of interfaces to which a policy can be applied.

Grouping interfaces into zones involves two procedures:

- Creating a zone so that interfaces can be attached to it
- Configuring an interface to be a member of a given zone

By default, traffic flows among interfaces that are members of the same zone.

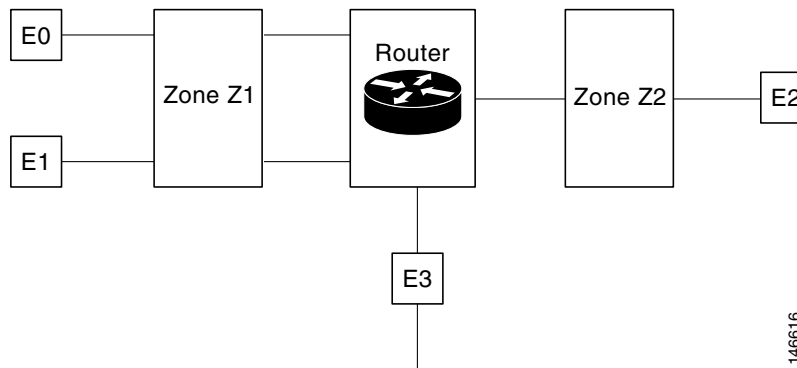
When an interface is a member of a security zone, all traffic to and from that interface (except traffic going to the router or initiated by the router) is dropped. To permit traffic to and from a zone-member interface, you must make that zone part of a zone-pair and then apply a policy to that zone-pair. If the policy permits traffic (via **inspect** or **pass** actions), traffic can flow through the interface.

For traffic to flow among all the interfaces in a router, all the interfaces must be a member of one security zone or another.

It is not necessary for all router interfaces to be members of security zones.

Figure 1 illustrates the following:

- Interfaces E0 and E1 are members of security zone Z1.
- Interface E2 is a member of security zone Z2.
- Interface E3 is not a member of any security zone.

Figure 1 **Security Zone Restrictions**

The following situations exist:

- Traffic flows freely between interfaces E0 and E1 because they are members of the same security zone (Z1).
- If no policies are configured, traffic will not flow between any other interfaces (for example, E0 and E2, E1 and E2, E3 and E1, and E3 and E2).
- Traffic can flow between E0 or E1 and E2 only when an explicit policy permitting traffic is configured between zone Z1 and zone Z2.
- Traffic can never flow between E3 and E0/E1/E2 because E3 is not part of any security zone.

Virtual Interfaces As Members of Security Zones

A virtual template interface is a logical interface configured with generic configuration information for a specific purpose or for configuration common to specific users, plus router-dependent information. The template contains Cisco IOS interface commands that are applied to virtual access interfaces, as needed. To configure a virtual template interface, use the **interface virtual-template** command.

Virtual interfaces can be members of a security zone. The virtual template interface is a member of a zone and all virtual access interfaces created from the template are members of that zone.

Zone member information is acquired from a RADIUS server and then the dynamically created interface is made a member of that zone.

The **zone-member security** command puts the dynamic interface into the corresponding zone.

Zone-Pairs

A zone-pair allows you to specify a unidirectional firewall policy between two security zones.

To define a zone-pair, use the **zone-pair security** command. The direction of the traffic is specified by specifying a source and destination zone. The source and destination zones of a zone-pair must be security zones. The same zone cannot be defined as both the source and the destination.

If desired, you can select the default self zone as either the source or the destination zone. The self zone is a system-defined zone. It does not have any interfaces as members. A zone-pair that includes the self zone, along with the associated policy, applies to traffic directed to the router or traffic generated by the router. It does not apply to traffic through the router.

The most common usage of firewalls is to apply them to traffic through a router, so you usually need at least two zones (that is, you cannot use the self zone).

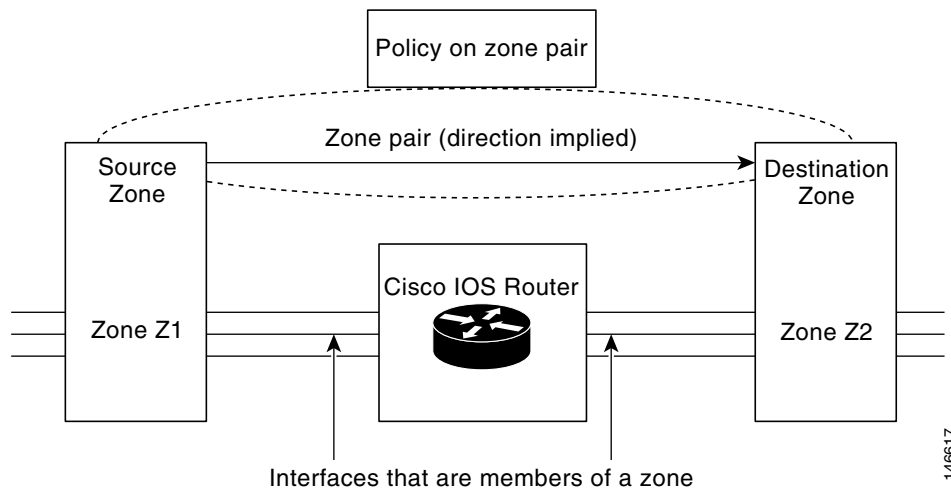
**Note**

Inspect policing is not allowed in policies that are attached to zone-pairs involving a self-zone.

To permit traffic between zone-member interfaces, you must configure a policy permitting (or inspecting) traffic between that zone and another zone. To attach a firewall policy map to the target zone-pair, use the **service-policy type inspect** command.

Figure 2 shows the application of a firewall policy to traffic flowing from zone z1 to zone z2, which means that the ingress interface for the traffic is a member of zone z1 and the egress interface is a member of zone z2.

Figure 2 **Zone Pairs**



If there are two zones and you require policies for traffic going in both directions (from z1 to z2 and z2 to z1), you must configure two zone-pairs (one for each direction).

If a policy is not configured between a pair of zones, traffic is dropped. However, it is not necessary to configure a zone-pair and a service policy solely for return traffic. Return traffic is allowed, by default, if a service policy permits the traffic in the forward direction. In the above example, it is not mandatory that you configure a zone-pair source Z2 destination Z1 solely for allowing return traffic from Z2 to Z1. The service policy on the Z1-Z2 zone-pair takes care of it.

Zones and Inspection

Zone-based policy firewalls examine the source and destination zones from the ingress and egress interfaces for a firewall policy. It is not necessary that all traffic flowing to or from an interface be inspected; you can designate that individual flows in a zone-pair be inspected through your policy map that you apply across the zone-pair. The policy map will contain class-maps that specify the individual flows.

For example, you can specify a policy map that performs HTTP URL filtering for hosts on 192.168.1.0/24 (engineers), but only does plain HTTP inspection for 192.168.2.0/24 (managers) for my inside_to_outside traffic.

This results in two flows (192.168.1.0/24 to any, 192.168.2.0/24 to any), and you can apply different inspect parameters to the flows to configure the desired different behaviors. Zone-based policy firewalls allow inside-to-internet traffic (source zone inside and destination zone outside).

You can also configure **inspect** parameters like TCP thresholds and timeouts on a per-flow basis.

Zones and ACLs

- Pinholes are not punched for return traffic in interface ACLs.
- ACLs applied to interfaces that are members of zones are processed before the policy is applied on the zone-pair. So, you must relax interface ACLs when there are policies between zones so that they cannot interfere with the policy firewall traffic.

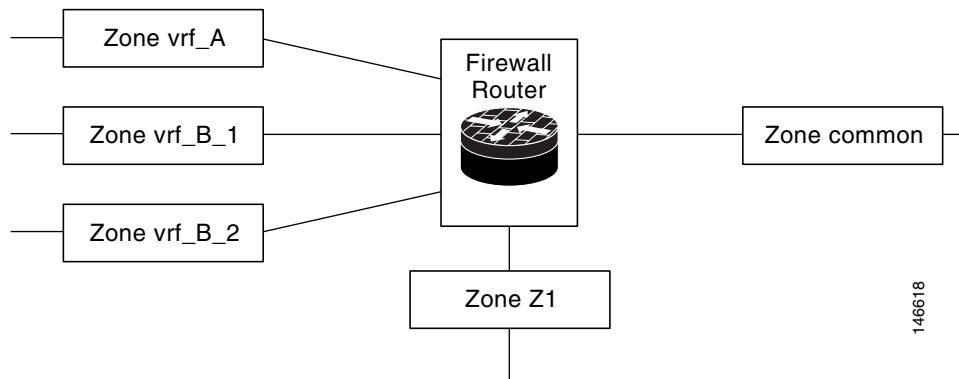
Zones and VRF Aware Firewall

Cisco IOS firewall is VRF aware. It handles IP address overlap across different VRFs, separate thresholds and timeouts for VRFs, and so forth. All interfaces in a zone must belong to the same VRF.

However, you should not group interfaces from different VRFs in the same zone because VRFs belong to different entities that typically have their own policies.

You can configure a zone-pair between two zones that contain different VRFs, as shown in [Figure 3](#).

When multiple VRFs are configured on a router and an interface provides common services to all the VRFs (for example, internet service), you should place that interface in a separate zone. You can then define policies between the common zone and other zones. (There can be one or more zones per VRF.)

Figure 3 **Zones and VRF**

In [Figure 3](#), the interface providing common services is a member of the zone “common.” All of VRF A is in a single zone, vrf_A. VRF B, which has multiple interfaces, is partitioned into multiple zones vrf_B_1 and vrf_B_2. Zone Z1 does not have VRF interfaces. You can specify policies between each of these zones and the common zone. Additionally, you can specify policies between each of the zones vrf_A, vrf_B_n and Z1 if VRF route export is configured and the traffic patterns make sense. You can configure a policy between zones vrf_A and vrf_B_1, but be sure that traffic can flow between them.

There is no need to specify the global thresholds and timers on a per-VRF basis. Instead, parameters are supplied to the **inspect** action through a parameter map.

146618

Zones and Transparent Firewall

The Cisco IOS firewall supports transparent firewalls where the interfaces are placed in bridging mode and IP firewalling is performed on the bridged traffic.

To configure a transparent firewall, use the **bridge** command to enable the bridging of a specified protocol in a specified bridge and the **zone-member security** command to attach an interface to a zone. The **bridge** command on the interface indicates that the interface is in bridging mode.

A bridged interface can be a member of a zone. In a typical case, the Layer 2 domain is partitioned into zones and a policy is applied the same way as for Layer 3 interfaces.

Transparent Firewall Restriction for P2P Inspection

A Cisco IOS Firewall uses Network Based Application Recognition (NBAR) for peer-to-peer (P2P) protocol classification and policy enforcement. NBAR is not available for bridged packets; thus, all P2P packet inspection is not supported for firewalls with transparent bridging.

Overview of Security Zone Firewall Policies

A class is a way of identifying a set of packets based on its contents. Normally you define a class so that you can apply an action on the identified traffic that reflects a policy. A class is designated via class maps.

An action is a specific functionality. It typically is associated with a traffic class. For example, **inspect**, **drop**, **pass**, and **police** are actions.

To create firewall policies, you should complete the following tasks:

- Define a match criteria (**class map**)
- Associate actions to the match criteria (**policy map**)
- Attach the policy map to a zone pair (**service policy**)

The **class-map** command creates a class map to be used for matching packets to a specified class. Packets arriving at the targets (such as the input interface, output interface, or zone-pair), determined by how the **service-policy** command is configured, are checked against the match criteria configured for a class map to determine if the packet belongs to that class.

The **policy-map** command creates or modifies a policy map that can be attached to one or more targets to specify a service policy. Use the **policy-map** command to specify the name of the policy map to be created, added to, or modified before you can configure policies for classes whose match criteria are defined in a class map.

Class Maps and Policy Maps for Zone-Based Policy Firewalls

Quality of Service (QoS) class maps have numerous match criteria; firewalls have fewer match criteria. Firewall class maps have type **inspect**; this information controls what shows up under firewall class maps.

A policy is an association of traffic classes and actions. It specifies what actions should be performed on the defined traffic classes. An action is a specific function, and it is typically associated with a traffic class. For example, **inspect**, **police**, and **drop** are actions.

Layer 3 and Layer 4 Class Maps and Policy Maps

Layer 3 and Layer 4 class maps are used to identify traffic streams on which different actions should be performed.

A Layer 3 or Layer 4 policy map is sufficient for the basic inspection of traffic.

The following example shows how to configure class map c1 with match criterias of ACL 101 and the HTTP protocol, and create an inspect policy map named p1 to specify that packets will be dropped on the traffic at c1:

```
Router(config)# class-map type inspect match-all c1
Router(config-cmap)# match access-group 101
Router(config-cmap)# match protocol http

Router(config)# policy-map type inspect p1
Router(config-pmap)# class type inspect c1
Router(config-pmap-c)# drop
```

To create a Layer 3 or Layer 4 policy, see the section “[Configuring Layer 7 Firewall Policies](#).”

Class-Map Configuration Restriction

If traffic meets multiple match criteria, the match criteria must be applied in the order of specific to less specific. For example, consider the following class map example:

```
class-map type inspect match-any my-test-cmap
  match protocol http
  match protocol tcp
```

In this example, HTTP traffic must first encounter the **match protocol http** command to ensure that the traffic will be handled by the service-specific capabilities of HTTP inspection. If the “match” lines were reversed so traffic encountered the **match protocol tcp** command before it was compared to the **match**

protocol http command, the traffic would simply be classified as TCP traffic and inspected according to the capabilities of the Firewall's TCP Inspection component. This configuration would be a problem for services such as FTP, TFTP, and for several multimedia and voice signaling services such as H.323, SIP, Skinny, and RTSP. These services require additional inspection capabilities to recognize their more complex activities.

Rate Limiting (Policing) Traffic Within a Layer 3 and Layer 4 Policy Map

Starting with Cisco IOS Release 12.4(9)T, you can issue the **police** command within an inspect policy to limit the number of concurrent connections allowed for applications such as Instant Messenger and P2P.

To effectively use the **police** command, you must also enable Cisco IOS stateful packet inspection within the inspect policy map. If you configure the **police** command without configuring the inspect action (via the **inspect** command), you will receive an error message and the **police** command will be rejected.

Compatibility with Existing Police Actions

Police actions provisioned in a Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC) policy map are applied as input and output policies on an interface. An inspect policy map can only be applied to a zone-pair, not an interface. The police action will be enforced on traffic that traverses the zone-pair. (The direction is inherent to the specification of the zone-pair.) Thus, a QoS policy containing a police action can be present on interfaces that make up a zone-pair and a police action can also be present in an inspect policy map applied across the zone-pair. If both police actions are configured, the zone-pair policer is executed after the input, interface policer, but before the output, interface policer. There is no interaction between the QoS and the inspect policers.

Police Restrictions

- The police action is not allowed in policies that are attached to zone pairs involving a “self” zone. If you want to perform this task, you should use control plane policing.
- Policing can only be specified in Layer 3 and Layer 4 policy maps; it cannot be specified in Layer 7 policy maps.

Layer 7 Class Maps and Policy Maps

Layer 7 class maps can be used in inspect policy maps only for deep packet inspection (DPI).

To create a Layer 7 class map, use the **class-map type inspect** command for the desired protocol. For example, for the HTTP protocol you would enter the **class-map type inspect http** command.

The type of class map (for example, HTTP) determines the match criteria that you can use. For example, if you want to specify HTTP traffic that contains Java applets, you must specify a “match response body java” statement in the context of an “inspect HTTP” class map.

A Layer 7 policy map provides application-level inspection of traffic. The policy map can include class maps only of the same type.

The DPI functionality is delivered through Layer 7 class maps and policy maps.

To create a Layer 7 policy map, specify the protocol in the applicable **policy-map type inspect** command. For example, to create a Layer 7 HTTP policy map, use the **policy-map type inspect http** command. In that command there is an argument where you enter the HTTP policy-map name.

If you do not specify a protocol name (for example, you use the **policy-map type inspect** command), you will be creating a Layer 3 or Layer 4 policy map, which can only be an inspect type policy map.

A Layer 7 policy map must be contained in a Layer 3 or Layer 4 policy map; it cannot be attached directly to a target. To attach a Layer 7 policy map to a top-level policy map, use the **service-policy (policy-map)** command and specify the application name (that is, HTTP, IMAP, POP3, SMTP, or SUNRPC). The parent class for a Layer 7 policy should have an explicit match criterion that matched only one Layer 7 protocol before the policy is attached.

If the Layer 7 policy map is in a lower level, you must specify the **inspect** action at the parent level for a Layer 7 policy map.

Layer 7 Supported Protocols

You can create Layer 7 class maps and policy maps for the following protocols:

- America Online (AOL) Instant Messenger (IM) protocol
- eDonkey P2P protocol
- FastTrack traffic P2P protocol
- Gnutella Version 2 traffic P2P protocol
- H.323 VoIP Protocol Version 4
- HTTP—The protocol used by web browsers and web servers to transfer files, such as text and graphic files.
- Internet Message Access Protocol (IMAP)—Method of accessing e-mail or bulletin board messages kept on a mail server that can be shared.
- I Seek You (ICQ) IM Protocol
- Kazaa Version 2 P2P protocol
- MSN Messenger IM protocol
- Post Office Protocol, Version 3 (POP3)—Protocol that client e-mail applications use to retrieve mail from a mail server.
- SIP—Session Initiation Protocol (SIP)
- SMTP—Simple Network Management Protocol
- SUNRPC—Sun RPC (Remote Procedure Call)
- Windows Messenger IM Protocol
- Yahoo IM protocol

For information on configuring a Layer 7 class map and policy map (policies), see the section [“Configuring Layer 7 Firewall Policies.”](#)

Class-Default Class Map

In addition to user-defined classes, there is a system-defined class map named class-default that represents all packets that do not match any of the user-defined classes in a policy. It always is the last class in a policy map.

You can define explicit actions for this group of packets. If you do not configure any actions for class-default in an inspect policy, the default action is **drop**.

The following example shows how to use class-default in a policy map. In this example, HTTP traffic is dropped and the remaining traffic is inspected. Class map c1 is defined for HTTP traffic, and class-default is used for a policy map p1.

```
Router(config)# class-map type inspect match-all c1
```



```
Router(config-cmap)# match protocol http

Router(config)# policy-map type inspect p1
Router(config-pmap)# class type inspect c1
Router(config-pmap-c)# drop
Router(config-pmap)# class class-default
Router(config-pmap-c)# inspect
```

Hierarchical Policy Maps

A policy can be nested within a policy. A policy that contains a nested policy is called a hierarchical policy.

To create a hierarchical policy, attach a policy directly to a class of traffic. A hierarchical policy contains a child and a parent policy. The child policy is the previously-defined policy that is associated with the new policy through the use of the **service-policy** command. The new policy using the pre-existing policy is the parent policy.



Note

There can be a maximum of two levels in a hierarchical inspect service-policy.

Parameter Maps

A parameter map allows you to specify parameters that control the behavior of actions and match criteria specified under a policy map and a class map, respectively.

There are currently three types of parameter maps:

- Inspect parameter map

An inspect parameter map is optional. If you do not configure a parameter map, the software uses default parameters. Parameters associated with the inspect action apply to all nested actions (if any). If parameters are specified in both the top and lower levels, those in the lower levels override those in the top levels.

- URL Filter parameter map

A parameter map is required for URL filtering (via the urlfilter action in a Layer 3 or Layer 4 policy map and the urlfilter parameter map).

- Protocol-specific parameter map

A parameter map is required for an Instant Messenger application (Layer 7) policy map.

How to Configure Zone-Based Policy Firewall

This section contains the following configuration tasks:

- [Configuring Layer 3 and Layer 4 Firewall Policies, page 12](#) (required)
- [Configuring a Parameter Map, page 15](#) (required)
- [Configuring Layer 7 Firewall Policies, page 21](#) (optional)
- [Creating Security Zones, Zone-Pairs, and Attaching a Policy Map to a Zone-Pair, page 38](#) (required)

Configuring Layer 3 and Layer 4 Firewall Policies

Layer 3 and Layer 4 policies are “top level” policies that are attached to the target (zone-pair). Use the following tasks to configure Layer 3 and Layer 4 firewall policies:

- [Configuring a Class Map for a Layer 3 and Layer 4 Firewall Policy](#), page 12
- [Creating a Policy Map for a Layer 3 and Layer 4 Firewall Policy](#), page 13

Configuring a Class Map for a Layer 3 and Layer 4 Firewall Policy

Use this task to configure a class map for classifying network traffic.



Note

You must perform at least one step from Step 4, 5, or 6.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type inspect** [**match any** | **match all**] *class-map-name*
4. **match access-group** {*access-group* | **name** *access-group-name*}
5. **match protocol** *protocol_name* [**signature**]
6. **match class-map** *class-map-name*
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	class-map type inspect [match-any match-all] <i>class-map-name</i> Example: Router(config)# class-map type inspect match-all c1	Creates a Layer 3 or Layer 4 inspect type class map. Enters class-map configuration mode.
Step 4	match access-group { <i>access-group</i> name <i>access-group-name</i> } Example: Router(config-cmap)# match access-group 101	Configures the match criteria for a class map based on the ACL name or number.

	Command or Action	Purpose
Step 5	match protocol <i>protocol-name</i> [signature] Example: Router(config-cmap)# match protocol http	Configures the match criteria for a class map on the basis of a specified protocol. Only Cisco IOS stateful packet inspection supported protocols can be used as match criteria in inspect type class maps. <ul style="list-style-type: none"> signature—Signature-based classification for peer-to-peer (P2P) packets is enabled.
Step 6	match class-map <i>class-map-name</i> Example: Router(config-cmap)# match class-map c1	Specifies a previously defined class as the match criteria for a class map.
Step 7	exit Example: Router(config-cmap)# exit	Returns to global configuration mode.

Creating a Policy Map for a Layer 3 and Layer 4 Firewall Policy

Use this task to create a policy map for a Layer 3 and Layer 4 firewall policy that will be attached to zone-pairs.



Note

If you are creating an inspect type policy map, note that only the following actions are allowed: drop, inspect, police, pass, service-policy, and urlfilter.



Note

You must perform at least one step from Step 5, 8, 9, or 10.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *policy-map-name*
4. **class type inspect** *class-name*
5. **inspect** [*parameter-map-name*]
6. **police rate** *bps* **burst** *size*
7. **drop** [log]
8. **pass**
9. **service-policy type inspect** *policy-map-name*
10. **urlfilter** *parameter-map-name*
11. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy-map type inspect <i>policy-map-name</i> Example: Router(config)# policy-map type inspect p1	Creates a Layer 3 and Layer 4 inspect type policy map. Enters policy-map configuration mode.
Step 4	class type inspect <i>class-name</i> Example: Router(config-pmap)# class type inspect c1	Specifies the traffic (class) on which an action is to be performed.
Step 5	inspect [<i>parameter-map-name</i>] Example: Router(config-pmap-c)# inspect inspect-params	Enables Cisco IOS stateful packet inspection.
Step 6	police rate <i>bps</i> <i>burst</i> <i>size</i> Example: Router(config-pmap-c)# police rate 2000 burst 3000	(Optional) Limits traffic matching within a firewall (inspect) policy.
Step 7	drop [log] Example: Router(config-pmap-c)# drop	(Optional) Drops packets that are matched with the defined class. Note The actions drop and pass are exclusive, and the actions inspect and drop are exclusive; that is, you cannot specify both of them.
Step 8	pass Example: Router(config-pmap-c)# pass	(Optional) Allows packets that are matched with the defined class.
Step 9	service-policy type inspect <i>policy-map-name</i> Example: Router(config-pmap-c)# service-policy type inspect p1	Attaches a firewall policy map to a zone-pair.

	Command or Action	Purpose
Step 10	urlfilter <i>parameter-map-name</i> Example: Router(config-pmap-c)# urlfilter param1	(Optional) Enables Cisco IOS firewall URL filtering.
Step 11	exit Example: Router(config-pmap-c)# exit	Returns to policy-map configuration mode.

Configuring a Parameter Map

Depending on your policy, you can configure either an inspect, URL filter, or protocol-specific type parameter map. If you are configuring a URL filter type or protocol-specific type policy, you must configure a parameter map, as appropriate. However, a parameter map is optional if you are using an inspect type policy.

Use one of the following tasks to configure a parameter map:

- [Creating an Inspect Parameter Map, page 15](#)
- [Creating a URLFILTER Parameter Map, page 17](#)
- [Configuring a Protocol-Specific Parameter Map, page 19](#)

Creating an Inspect Parameter Map

Use this task to create an inspect type parameter map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** *parameter-map-name*
4. **alert** {on | off}
5. **audit-trail** {on | off}
6. **dns-timeout** *seconds*
7. **icmp idle-timeout** *seconds*
8. **max-incomplete** {**low** *number-of-connections* | **high** *number-of-connections*}
9. **one-minute** {**low** *number-of-connections* | **high** *number-of-connections*}
10. **sessions maximum** *sessions*
11. **tcp finwait-time** *seconds*
12. **tcp idle-time** *seconds*
13. **tcp max-incomplete host** *threshold* [**block-time** *minutes*]
14. **tcp synwait-time** *seconds*
15. **udp idle-time** *seconds*

16. exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	parameter-map type inspect <i>parameter-map-name</i> Example: Router(config)# parameter-map type inspect eng-network-profile	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the inspect action. Enters parameter-map type inspect configuration mode.
Step 4	alert {on off} Example: Router(config-profile)# alert on	(Optional) Turns on and off Cisco IOS stateful packet inspection alert messages that are displayed on the console.
Step 5	audit-trail {on off} Example: Router(config-profile)# audit-trail on	(Optional) Turns audit trail messages on or off.
Step 6	dns-timeout <i>seconds</i> Example: Router(config-profile)# dns-timeout 60	(Optional) Specifies the domain name system (DNS) idle timeout (the length of time for which a DNS lookup session will continue to be managed while there is no activity).
Step 7	icmp idle-timeout <i>seconds</i> Example: Router(config-profile)# icmp idle-timeout 90	(Optional) Configures the timeout for Internet Control Message Protocol (ICMP) sessions.
Step 8	max-incomplete {low number-of-connections high number-of-connections} Example: Router(config-profile)# max-incomplete low 800 Router(config-profile)# max-incomplete high 10000	(Optional) Defines the number of existing half-open sessions that will cause the Cisco IOS firewall to start and stop deleting half-open sessions.
Step 9	one-minute {low number-of-connections high number-of-connections} Example: Router(config-profile)# one-minute low 300 Router(config-profile)# one-minute high 400	(Optional) Defines the number of new unestablished sessions that will cause the system to start deleting half-open sessions and stop deleting half-open sessions.

	Command or Action	Purpose
Step 10	sessions maximum <i>sessions</i> Example: Router(config-profile)# sessions maximum 200	(Optional) Sets the maximum number of allowed sessions that can exist on a zone-pair. You may want to use this command to limit the bandwidth used by the sessions. <ul style="list-style-type: none"> <i>sessions</i>—Maximum number of allowed sessions. Range: 1 to 2147483647.
Step 11	tcp finwait-time <i>seconds</i> Example: Router(config-profile)# tcp finwait-time 5	(Optional) Specifies how long a TCP session will be managed after the Cisco IOS firewall detects a FIN-exchange.
Step 12	tcp idle-time <i>seconds</i> Example: Router(config-profile)# tcp idle-time 90	(Optional) Configures the timeout for TCP sessions.
Step 13	tcp max-incomplete host <i>threshold</i> [<i>block-time minutes</i>] Example: Router(config-profile)# tcp max-incomplete host 500 block-time 10	(Optional) Specifies threshold and blocking time values for TCP host-specific DoS detection and prevention.
Step 14	tcp synwait-time <i>seconds</i> Example: Router(config-profile)# tcp synwait-time 3	(Optional) Specifies how long the software will wait for a TCP session to reach the established state before dropping the session.
Step 15	udp idle-time <i>seconds</i> Example: Router(config-profile)# udp idle-time 75	(Optional) Configures the idle timeout of User Datagram Protocol (UDP) sessions going through the firewall.
Step 16	exit Example: Router(config-profile)# exit	Returns to global configuration mode.

Creating a URLFILTER Parameter Map

To create a URLFILTER parameter map, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type urlfilter *parameter-map-name***
4. **alert {on | off}**
5. **allow-mode {on | off}**
6. **audit-trail {on | off}**

7. **cache** *number*
8. **exclusive-domain** {**deny** | **permit**} *domain-name*
9. **max-request** *number-of-requests*
10. **max-resp-pak** *number-of-requests*
11. **server vendor** {**n2h2** | **websense**} {*ip-address* | *hostname* [**port** *port-number*]} [**outside**] [**log**] [**retrans** *retransmission-count*] [**timeout** *seconds*]
12. **source-interface** *interface-name*
13. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	parameter-map type urlfilter <i>parameter-map-name</i> Example: Router(config)# parameter-map type urlfilter eng-network-profile	Creates or modifies a parameter map for URL filtering parameters. Enters URL parameter-map configuration mode.
Step 4	alert { on off } Example: Router(config-profile)# alert on	(Optional) Turns on and off Cisco IOS stateful packet inspection alert messages that are displayed on the console.
Step 5	allow-mode { on off } Example: Router(config-profile)# allow-mode on	(Optional) Turns on or off the default mode of the filtering algorithm.
Step 6	audit-trail { on off } Example: Router(config-profile)# audit-trail on	(Optional) Turns audit trail messages on or off.
Step 7	cache <i>number</i> Example: Router(config-profile)# cache 5	(Optional) Controls how the URL filter handles the cache it maintains of HTTP servers.

	Command or Action	Purpose
Step 8	exclusive-domain {deny permit} domain-name Example: Router(config-profile)# exclusive-domain permit cisco.com	(Optional) Adds or removes a domain name to or from the exclusive domain list so that the Cisco IOS firewall does not have to send look up requests to the vendor server.
Step 9	max-request number-of-requests Example: Router(config-profile)# max-request 80	(Optional) Specifies the maximum number of outstanding requests that can exist at a time.
Step 10	max-resp-pak number-of-requests Example: Router(config-profile)# max-resp-pak 200	(Optional) Specifies the maximum number of HTTP responses that the Cisco IOS firewall can keep in its packet buffer.
Step 11	server vendor {n2h2 websense} {ip-address hostname [port port-number]} [outside] [log] [retrans retransmission-count] [timeout seconds] Example: Router(config-profile)# server vendor n2h2 10.193.64.22 port 3128 outside retrans 9 timeout 8	Specifies the URL filtering server. Note This command is mandatory if you want anything from the urlfilter configuration.
Step 12	source-interface interface-name Example: Router(config-profile)# source-interface ethernet0	(Optional) Specifies the interface whose IP address will be used as the source IP address while making a TCP connection to the URL filter server (Websense or N2H2).
Step 13	exit Example: Router(config-profile)# exit	Returns to global configuration mode.

Configuring a Protocol-Specific Parameter Map

Use this task to configure a Layer 7, protocol-specific parameter map.



Note

Protocol-specific parameter maps can be created only for Instant Messenger applications (AOL, ICQ, MSN Messenger, Yahoo Messenger, and Windows Messenger).

Prerequisites

To enable name resolution to occur, you must also enable the **ip domain name** command and the **ip name-server** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type protocol-info** *parameter-map-name*
4. **server** {name *string* [snoop] | ip {*ip-address* | range *ip-address-start ip-address-end*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	parameter-map type protocol-info <i>parameter-map-name</i> Example: Router(config)# parameter-map type protocol-info ymsg	Defines an application-specific parameter map. Enters parameter-map type configuration mode. Note Protocol-specific parameter maps can be created only for Instant Messenger applications (AOL, ICQ, MSN Messenger, Yahoo Messenger, and Windows Messenger).
Step 4	server {name <i>string</i> [snoop] ip { <i>ip-address</i> range <i>ip-address-start ip-address-end</i> } Example: Router(config-profile)# server name sdsc.msg.yahoo.com Router(config-profile)# server ip 10.1.1.1	Configures a set of Domain Name System (DNS) servers for which a given instant messenger application will be interacting. Note If at least one server instance is not configured, the parameter map will not have any definitions to enforce; that is, the configured instant messenger policy cannot be enforced. Note To configure more than one set of servers, you can issue the server command multiple times within an instant messenger's parameter map. Multiple entries are treated cumulatively.

Troubleshooting Tips

To display details of an IM protocol-specific parameter map, use the **show parameter-map type protocol-info** command.

Configuring Layer 7 Firewall Policies

Configure Layer 7 policy maps if you are interested in extra provisioning for Layer 7 inspection modules. It is not necessary that you configure all of the Layer 7 policy maps.

Use one of the following tasks to configure a Layer 7, protocol-specific firewall policy:

- [Configuring an HTTP Firewall Policy, page 21](#)
- [Configuring an IMAP Firewall Policy, page 26](#)
- [Configuring an Instant Messenger \(IM\) Policy, page 28](#)
- [Configuring a Peer-to-Peer \(P2P\) Policy, page 30](#)
- [Configuring a POP3 Firewall Policy, page 33](#)
- [Configuring an SMTP Firewall Policy, page 34](#)
- [Configuring a SUNRPC Firewall Policy, page 36](#)

Layer 7 Class Map and Policy Map Restrictions

- Deep packet inspection (DPI) class maps for Layer 7 can only be used in inspect policy maps of the respective type. For example, **class-map type inspect http** can only be used in **policy-map type inspect http**.
- DPI policies require an **inspect** action at the parent level.
- A Layer 7 (DPI) policy map must be nested at the second level in a Layer 3 or Layer 4 inspect policy map, whereas a Layer 3 or Layer 4 inspect policy can be attached at the first level. Therefore, a Layer 7 policy map cannot be attached directly to a zone-pair.
- If no action is specified in the hierarchical path of an inspect service-policy, the packet is dropped. Traffic matching class-default in the top-level policy is dropped if there are no explicit actions configured in class-default. If the traffic does not match any class in a Layer 7 policy, the traffic is not dropped; control returns to the parent policy and subsequent actions (if any) in the parent policy are executed on the packet.
- Layer 7 policy maps include class maps only of the same type.
- You can specify the **reset** action only for TCP traffic; it resets the TCP connection.

Configuring an HTTP Firewall Policy

Use these tasks to configure an HTTP firewall policy—a class map and a policy map, respectively.

If you want to configure match criteria on the basis of an element within a parameter map, you must configure a parameter map as shown in the task “[Creating an Inspect Parameter Map](#).”

You must specify at least one match criterion; otherwise, the firewall policy will not be effective.

Configuring an HTTP Class Map

Use this task to configure an HTTP firewall class map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **class-map type inspect http** [match-any | match-all] *class-map-name*
4. **match response body java-applet**
5. **match req-resp protocol violation**
6. **match req-resp body length** {lt *bytes* | gt *bytes*}
7. **match req-resp header content-type** {violation | mismatch | unknown}
8. **match {request | response | req-resp} header** [*header-name*] **count gt** *number*
9. **match {request | response | req-resp} header** [*header-name*] **length gt** *bytes*
10. **match request {uri | arg} length gt** *bytes*
11. **match request method** {connect | copy | delete | edit | get | getattribute | getattributenames | getproperties | head | index | lock | mkdir | move | options | post | put | revadd | revlabel | revlog | revnum | save | setattribute | startrev | stoprev | trace | unedit | unlock}
12. **match request port-misuse** {im | p2p | tunneling | any}
13. **match req-resp header transfer-encoding** {chunked | compress | deflate | gzip | identity | all}
14. **match {request | response | req-resp} header** [*header-name*] **regex** *parameter-map-name*
15. **match request {uri | arg} regex** *parameter-map-name*
16. **match {request | response | req-resp} body regex** *parameter-map-name*
17. **match response status-line regex** *parameter-map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	class-map type inspect http [match-any match-all] <i>class-map-name</i> Example: Router(config)# class-map type inspect http http-class	Creates a class map for the HTTP protocol so that you can enter match criteria. Enters class-map configuration mode.
Step 4	match response body java-applet Example: Router(config-cmap)# match response body java-applet	(Optional) Identifies Java applets in an HTTP connection.

	Command or Action	Purpose
Step 5	match req-resp protocol violation Example: Router(config-cmap)# match req-resp protocol violation	(Optional) Configures an HTTP class map to allow HTTP messages to pass through the firewall or to reset the TCP connection when HTTP noncompliant traffic is detected.
Step 6	match req-resp body length {lt bytes gt bytes} Example: Router(config-cmap)# match req-resp body length gt 35000	(Optional) Configures an HTTP class map to use the minimum or maximum message size, in bytes, as a match criterion for permitting or denying HTTP traffic through the firewall. The number of bytes can be from 0 to 65535.
Step 7	match req-resp header content-type {violation mismatch unknown} Example: Router(config-cmap)# match req-resp header content-type mismatch	(Optional) Configures an HTTP class map based on the content type of HTTP traffic.
Step 8	match {request response req-resp} header [header-name] count gt number Example: Router(config-cmap)# match req-resp header count gt 16	(Optional) Configure an HTTP firewall policy to permit or deny HTTP traffic on the basis of request, response, or both request and response messages whose header count does not exceed a maximum number of fields.
Step 9	match {request response req-resp} header [header-name] length gt bytes Example: Router(config-cmap)# match response header length gt 50000	(Optional) Permits or denies HTTP traffic based on the length of the HTTP request header. <ul style="list-style-type: none"> <i>header-name</i>—Specific line in the header field. If a specific line is defined, only that specific field length will be used as match criteria. gt bytes—Maximum number of bytes that can be in the header of the HTTP request. Number of bytes range: 0 to 65535.
Step 10	match request {uri arg} length gt bytes Example: Router(config-cmap)# match request uri length gt 500	(Optional) Configures an HTTP firewall policy to use the uniform resource identifier (URI) or argument length in the request message as a match criterion for permitting or denying HTTP traffic.
Step 11	match request method {connect copy delete edit get getattribute getattributenames getproperties head index lock mkdir move options post put revadd revlabel revlog revnum save setattribute startrev stoprev trace unedit unlock} Example: Router(config-cmap)# match request method connect	(Optional) Configures an HTTP firewall policy to use the request methods or the extension methods as a match criterion for permitting or denying HTTP traffic.

	Command or Action	Purpose
Step 12	<pre>match request port-misuse {im p2p tunneling any}</pre> <p>Example: Router(config-cmap)# match request port-misuse any</p>	(Optional) Identifies applications misusing the HTTP port.
Step 13	<pre>match req-resp header transfer-encoding {chunked compress deflate gzip identity all}</pre> <p>Example: Router(config-cmap)# match req-resp header transfer-encoding compress</p>	(Optional) Permits or denies HTTP traffic according to the specified transfer encoding of the message. <ul style="list-style-type: none"> • chunked—Encoding format (specified in RFC 2616, Hypertext Transfer Protocol—HTTP/1) in which the body of the message is transferred in a series of chunks; each chunk contains its own size indicator. • compress—Encoding format produced by the UNIX compress utility. • deflate—ZLIB format defined in RFC 1950, ZLIB Compressed Data Format Specification Version 3.3, combined with the deflate compression mechanism described in RFC 1951, DEFLATE Compressed Data Format Specification Version 1.3. • gzip—Encoding format produced by the gzip (GNU zip) program. • identity—Default encoding, which indicates that no encoding has been performed. • all—All of the transfer encoding types.
Step 14	<pre>match {request response req-resp} header [header-name] regex parameter-map-name</pre> <p>Example: Router(config-cmap)# match req-resp header regex non_ascii_regex</p>	(Optional) Configures HTTP firewall policy match criteria on the basis of headers that match the regular expression defined in a parameter map.
Step 15	<pre>match request {uri arg} regex parameter-map-name</pre> <p>Example: Router(config-cmap)# match request uri regex uri_regex_cm</p>	(Optional) Configure an HTTP firewall policy to permit or deny HTTP traffic on the basis of request messages whose URI or arguments (parameters) match a defined regular expression.

	Command or Action	Purpose
Step 16	match {request response req-resp} body regex <i>parameter-map-name</i> Example: Router(config-cmap)# match response body regex body_regex	(Optional) Configures a list of regular expressions that are to be matched against the body of the request, response or both the request and response message.
Step 17	match response status-line regex <i>parameter-map-name</i> Example: Router(config-cmap)# match response status-line regex status_line_regex	(Optional) Specifies a list of regular expressions that are to be matched against the status-line of a response message.

Configuring an HTTP Policy Map

Use this task to configure an HTTP firewall policy map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type inspect http** *policy-map-name*
4. **class-type inspect http** *http-class-name*
5. **allow**
6. **log**
7. **reset**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy-map type inspect http <i>policy-map-name</i> Example: Router(config)# policy-map type inspect http myhttp-policy	Creates a Layer 7 HTTP policy map. Enters policy-map configuration mode.
Step 4	class-type inspect http <i>http-class-name</i> Example: Router(config-pmap)# class-type inspect http http-class	Creates a class map for the HTTP protocol.
Step 5	allow Example: Router(config-pmap)# allow	(Optional) Allows traffic class matching the class.
Step 6	log Example: Router(config-pmap)# log	Generates a log (messages).
Step 7	reset Example: Router(config-pmap)# reset	(Optional) Resets a TCP connection if the data length of the SMTP body exceeds the value that you configured in the class-map type inspect smtp command.

Configuring an IMAP Firewall Policy

Use these tasks to configure an IMAP firewall policy—a class map and a policy map, respectively.

Configuring an IMAP Class Map

Use this task to configure an IMAP class map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type inspect imap** [*match-any*] *class-map-name*

4. **log**
5. **match invalid-command**
6. **match login clear-text**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	class-map type inspect imap [match-any] class-map-name Example: Router(config)# class-map type inspect imap imap-class	Creates a class map for the IMAP protocol so that you can enter match criteria. Enters class-map configuration mode.
Step 4	log Example: Router(config-cmap)# log	Generates a log of messages.
Step 5	match invalid-command Example: Router(config-cmap)# match invalid-command	(Optional) Locates invalid commands on an IMAP connection.
Step 6	match login clear-text Example: Router(config-cmap)# match login clear-text	(Optional) Finds a nonsecure login when using an IMAP server.

Configuring an IMAP Policy Map

Use this task to configure an IMAP firewall policy map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type inspect imap policy-map-name**
4. **class-type inspect imap imap-class-name**
5. **log**
6. **reset**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy-map type inspect imap <i>policy-map-name</i> Example: Router(config)# policy-map type inspect imap myimap-policy	Creates a Layer 3 IMAP policy map. Enters policy-map configuration mode.
Step 4	class-type inspect imap <i>imap-class-name</i> Example: Router(config-pmap)# class-type inspect imap pimap	Creates a class map for the IMAP protocol.
Step 5	log Example: Router(config-pmap)# log	Generates a log (messages).
Step 6	reset Example: Router(config-pmap)# reset	(Optional) Resets a TCP connection if the data length of the SMTP body exceeds the value that you configured in the class-map type inspect smtp command.

Configuring an Instant Messenger (IM) Policy

Use this task to configure an IM policy—a class map and a policy map.

You can create an IM policy for the following IM applications: America Online (AOL), ICQ, MSN Messenger, Yahoo Messenger, and Windows Messenger.

Configuring an IM Class Map

Use this task to configure a class map for any supported IM application.

SUMMARY STEPS

- enable**
- configure terminal**
- class map type inspect { aol | msnmsgr | ymsgr | icq | winmsgr } [match-any] class-map-name**
- match service { any | text-chat }**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	class map type inspect {aol msnmsgr ymsgr icq winmsgr} [match-any] class-map-name Example: Router(config)# class map type inspect aol myaolclassmap	Creates a IM type class map so you can begin adding match criteria. This command puts the router in class-map configuration mode.
Step 4	match service {any text-chat} Example: Router(config-cmap)# match service text-chat	(Optional) Creates a match criterion on the basis of text chat messages (text-chat) or for any available service within a given IM protocol (any).

Configuring an IM Policy Map

Use this task to configure a policy map for any supported IM application.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy map type inspect** *protocol-name policy-map-name*
4. **class type inspect {aol | msnmsgr | ymsgr | icq | winmsgr}** *class-map-name*
5. **reset**
6. **log**
7. **allow**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy map type inspect <i>protocol-name</i> <i>policy-map-name</i> Example: Router(config)# policy map type inspect aol myaolpolicymap	Creates an IM policy map. This command puts the router in policy-map configuration mode.
Step 4	class type inspect { <i>aol</i> <i>msnmsgr</i> <i>ymsgr</i> <i>icq</i> <i>winmsgr</i> } <i>class-map-name</i> Example: Router(config-pmap)# class type inspect aol myaolclassmap	Specifies a traffic class on which an action is to be performed. <ul style="list-style-type: none"> <i>class-map-name</i>—This class map name should match the class map specified via the class-map type inspect command.
Step 5	reset Example: Router(config-pmap)# reset	(Optional) Resets the connection.
Step 6	log Example: Router(config-pmap)# log	(Optional) Generates a log message for the matched parameters.
Step 7	allow Example: Router(config-pmap)# allow	(Optional) Allows the connection.

What to Do Next

If you have not done so already, you must configure an IM-specific parameter map as shown in the task [“Configuring a Protocol-Specific Parameter Map.”](#)

Configuring a Peer-to-Peer (P2P) Policy

Use this task to configure a P2P firewall policy—a class map and a policy map, respectively.

You can create a P2P policy for the following P2P applications: eDonkey, FastTrack, Gnutella, and Kazaa Version 2.

Configuring a P2P Class Map

Use this task to configure a class map for any supported P2P application.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class map type inspect** {edonkey | fasttrack | gnutella | kazaa2} [match-any] *class-map-name*
4. **match file-transfer** [regular-expression]
5. **match search-file-name** [regular-expression]
6. **match text-chat** [regular-expression]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	class map type inspect {edonkey fasttrack gnutella kazaa2} [match-any] <i>class-map-name</i> Example: Router(config)# class map type inspect edonkey myclassmap	Creates a P2P type class map so you can begin adding match criteria. This command puts the router in class-map configuration mode.
Step 4	match file-transfer [regular-expression] Example: Router(config-cmap)# match file-transfer *	(Optional) Matches file transfer connections within any supported P2P protocol. Note To specify that all file transfer connections be identified by the traffic class, use "*" as the regular expression.
Step 5	match search-file name [regular-expression] Example: Router(config-cmap)# match search-file-name	(Optional) Blocks filenames within a search request for clients using the eDonkey P2P application. Note This command is available only for the eDonkey P2P application.
Step 6	match text-chat [regular-expression] Example: Router(config-cmap)# match text-chat	(Optional) Blocks text chat messages between clients using the eDonkey P2P application. Note This command is available only for the eDonkey P2P application.

Configuring a P2P Policy Map

Use this task to configure a policy map for any supported P2P application.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy map type inspect p2p** *policy-map-name*
4. **class type inspect {edonkey | fasttrack | gnutella | kazaa2}** *class-map-name*
5. **reset**
6. **log**
7. **allow**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy map type inspect p2p <i>policy-map-name</i> Example: Router(config)# policy map type inspect p2p mypolicymap	Creates a P2P policy map. This command puts the router in policy-map configuration mode.
Step 4	class type inspect {edonkey fasttrack gnutella kazaa2} <i>class-map-name</i> Example: Router(config-pmap)# class type inspect edonkey myclassmap	Specifies a traffic class on which an action is to be performed. Enters the policy map configuration mode. <ul style="list-style-type: none"> <i>class-map-name</i>—This class map name should match the class map specified via the class-map type inspect command.
Step 5	reset Example: Router(config-pmap)# reset	(Optional) Resets the connection.
Step 6	log Example: Router(config-pmap)# log	(Optional) Generates a log message for the matched parameters.
Step 7	allow Example: Router(config-pmap)# allow	(Optional) Allows the connection.

Configuring a POP3 Firewall Policy

Use these tasks to configure a POP3 firewall policy—a class map and a policy map, respectively.

Configuring a POP3 Class Map

Use this task to configure a POP3 firewall class map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type inspect pop3 [match-any] *class-map-name***
4. **match invalid-command**
5. **match login clear-text**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	class-map type inspect pop3 [match-any] <i>class-map-name</i> Example: Router(config)# class-map type inspect pop3 pop3-class	Creates a class map for the POP3 protocol so that you can enter match criteria. Enters class-map configuration mode.
Step 4	match invalid-command Example: Router(config-cmap)# match invalid-command	(Optional) Locates invalid commands on a POP3 server.
Step 5	match login clear-text Example: Router(config-cmap)# match login clear-text	(Optional) Finds a non-secure login when using a POP3 server.

Configuring a POP3 Firewall Policy Map

Use this task to configure a POP3 firewall policy map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type inspect pop3** *policy-map-name*
4. **class-type inspect pop3** *pop3-class-name*
5. **log**
6. **reset**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy-map type inspect pop3 <i>policy-map-name</i> Example: Router(config)# policy-map type inspect pop3 mypop3-policy	Creates a Layer 7 POP3 policy map. Enters policy-map configuration mode.
Step 4	class-type inspect pop3 <i>pop3-class-name</i> Example: Router(config-pmap)# class-type inspect pop3 pcl	Creates a class map for the POP3 protocol.
Step 5	log Example: Router(config-pmap)# log	Generates a log (messages).
Step 6	reset Example: Router(config-pmap)# reset	(Optional) Resets a TCP connection if the data length of the SMTP body exceeds the value that you configured in the class-map type inspect smtp command.

Configuring an SMTP Firewall Policy

Use these tasks to configure an SMTP firewall policy—a class map and a policy map, respectively.

Configuring an SMTP Firewall Class Map

Use this task to configure an SMTP firewall class map.

**Note**

To enable inspection for extended SMTP (ESMTP), the match filter for the traffic class must contain the extended keyword. For example, **match protocol smtp extended**.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type inspect smtp [match-all | match-any] *class-map-name***
4. **match data-length gt *max-data-value***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	class-map type inspect smtp [match-all match-any] <i>class-map-name</i> Example: Router(config)# class-map type inspect smtp smtp-class	Creates a class map for the SMTP protocol so that you can enter match criteria. Enters class-map configuration mode.
Step 4	match data-length gt <i>max-data-value</i> Example: Router(config-cmap)# match data-length gt 200000	Determines if the amount of data transferred in a Simple Mail Transfer Protocol (SMTP) connection is above the configured limit.

Configuring an SMTP Firewall Policy Map

Use this task to configure an SMTP firewall policy map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type inspect smtp *policy-map-name***
4. **class-type inspect smtp *smtp-class-name***
5. **reset**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy-map type inspect smtp <i>policy-map-name</i> Example: Router(config)# policy-map type inspect smtp mysmtp-policy	Creates a Layer 7 SMTP policy map. Enters policy-map configuration mode.
Step 4	class-type inspect smtp <i>smtp-class-name</i> Example: Router(config-pmap)# class-type inspect smtp sc	Configures inspection parameters for the SMTP protocol.
Step 5	reset Example: Router(config-pmap)# reset	(Optional) Resets the TCP connection if the data length of the SMTP body exceeds the value that you configured in the class-map type inspect smtp command.

Configuring a SUNRPC Firewall Policy

Use these tasks to configure a SUNRPC firewall policy—a class map and a policy map, respectively.

**Note**

If you are inspecting an RPC protocol (that is, you specified the **match protocol sunrpc** command in the Layer 4 class map) the Layer 7 SUNRPC policy map is required.

Configuring a SUNRPC Firewall Class Map

Use this task to configure a SUNRPC firewall class map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type inspect sunrpc** [**match-any**] *class-map-name*
4. **match program-number** *program-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	class-map type inspect sunrpc [match-any] <i>class-map-name</i> Example: Router(config)# class-map type inspect sunrpc long-urls	Creates a class map for the SUNRPC protocol so that you can enter match criteria. Enters class-map configuration mode.
Step 4	match program-number <i>program-number</i> Example: Router(config-cmap)# match program-number 2345	(Optional) Specifies the allowed Remote Procedure Call (RPC) protocol program number as a match criteria.

Configuring a SUNRPC Firewall Policy Map

Use this task to configure an SUNRPC firewall policy map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type inspect sunrpc** *policy-map-name*
4. **class-type inspect sunrpc** *sunrpc-class-name*
5. **allow** [wait-time *minutes*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy-map type inspect sunrpc <i>policy-map-name</i> Example: Router(config)# policy-map type inspect sunrpc my-rpc-policy	Creates a Layer 7 SUNRPC policy map. Enters policy-map configuration mode.
Step 4	class-type inspect sunrpc <i>sunrpc-class-name</i> Example: Router(config-pmap)# class-type inspect sunrpc cs1	Configures inspection parameters for the SUNRPC protocol.
Step 5	allow [wait-time <i>minutes</i>] Example: Router(config-pmap)# allow wait-time 10	(Optional) Allows the configured program number. Specifies the number of minutes to keep a small hole in the firewall to allow subsequent connections from the same source address and to the same destination address and port. The default wait time is zero minutes. This keyword is available only for the RPC protocol.

Creating Security Zones, Zone-Pairs, and Attaching a Policy Map to a Zone-Pair

You need two security zones to create a zone-pair. However, you can create only one security zone and use a system-defined security zone called “self.” Note that if you select a self zone, you cannot configure inspect policing.

Use this process to complete the following tasks:

- Create at least one security zone
- Define zone-pairs
- Assign interfaces to security zones
- Attach a policy map to a zone-pair.

**Tip**

Before you create zones, think about what should constitute the zones. The general guideline is that you should group together interfaces that are similar when they are viewed from a security perspective.

Security Zone Restrictions

- An interface cannot be part of a zone and legacy inspect policy at the same time.

- An interface can be a member of only one security zone.
- When an interface is a member of a security zone, all traffic to and from that interface is blocked unless you configure an explicit interzone policy on a zone-pair involving that zone.
- Traffic cannot flow between an interface that is a member of a security zone and an interface that is not a member of a security zone because a policy can be applied only between two zones.
- For traffic to flow among all the interfaces in a router, all the interfaces must be members of one security zone or another. This is particularly important because after you make an interface a member of a security zone, a policy action (such as **inspect** or **pass**) must explicitly allow packets. Otherwise, packets are dropped.
- If an interface on a router cannot be part of a security zone or firewall policy, you may have to put that interface in a security zone and configure a “pass all” policy (that is, a “dummy” policy) between that zone and other zones to which a traffic flow is desired.
- You cannot apply an access control list (ACL) between security zones or on a zone-pair.
- An ACL cannot be applied between security zones and zone-pairs. Include the ACL configuration in a class map, and use policy maps to drop traffic.
- An ACL on an interface that is a zone member should not be restrictive (strict).
- All interfaces in a security zone must belong to the same virtual routing and forwarding (VRF).
- You can configure policies between security zones whose member interfaces are in separate VRFs. However, traffic may not flow between these VRFs if the configuration does not allow it.
- If traffic does not flow between VRFs (because route-leaking between VRFs is not configured), the policy across the VRFs is not executed. This is a misconfiguration on the routing side, not on the policy side.
- Traffic between interfaces in the same security zone is not subjected to any policy; the traffic passes freely.
- The source and the destination zones in a zone pair must be the type security.
- The same zone cannot be defined as both the source and the destination.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **zone security** *zone-name*
4. **description** *line-of-description*
5. **exit**
6. **zone-pair security** *zone-pair-name* { **source** *source-zone-name* | **self** } **destination** [**self** | *destination-zone-name*]
7. **description** *line-of-description*
8. **exit**
9. **interface** *type number*
10. **zone-member security** *zone-name*
11. **exit**
12. **zone-pair security** *zone-pair-name* { **source** *source-zone-name* | **self** } **destination** [**self** | *destination-zone-name*]

13. **service-policy type inspect** *policy-map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	zone security zone-name Example: Router(config)# zone security zone1	Creates a security zone to which interfaces can be assigned. Enters security zone configuration mode.
Step 4	description line-of-description Example: Router(config-sec-zone)# description Internet Traffic	(Optional) Describes the zone.
Step 5	exit Example: Router(config-sec-zone)# exit	Returns to global configuration mode.
Step 6	zone-pair security zone-pair name {source source-zone-name self} destination [self destination-zone-name] Example: Router(config)# zone-pair security zp source z1 destination z2	Creates a zone-pair. Note To apply a policy, you must configure a zone-pair Enters security zone configuration mode.
Step 7	description line-of-description Example: Router(config-sec-zone)# description accounting network	(Optional) Describes the zone-pair.
Step 8	exit Example: Router(config-sec-zone)# exit	Returns to global configuration mode.
Step 9	interface type number Example: Router(config)# interface ethernet 0	Specifies an interface for configuration. Enters interface configuration mode.

	Command or Action	Purpose
Step 10	zone-member security zone-name Example: Router(config-if)# zone-member security zone1	Assigns an interface to a specified security zone. Note When you make an interface a member of a security zone, all traffic into and out of that interface (except traffic bound for the router or initiated by the router) is dropped by default. To let traffic through the interface, you must make the zone part of a zone-pair to which you apply a policy. If the policy permits traffic, traffic can flow through that interface.
Step 11	exit Example: Router(config-if)# exit	Returns to interface configuration mode.
Step 12	zone-pair security zone-pair-name {source source-zone-name self} destination [self destination-zone-name] Example: Router(config)# zone-pair security zp source z1 destination z2	Creates a zone-pair. Enters security zone-pair configuration mode.
Step 13	service-policy type inspect policy-map-name Example: Router(config-sec-zone-pair)# service-policy type inspect p2	Attaches a firewall policy map to the destination zone-pair. Note If a policy is not configured between a pair of zones, traffic is dropped by default.

Configuration Examples for Zone-Based Policy Firewall

- [Configuring Layer 3 and Layer 4 Firewall Policies: Example, page 41](#)
- [Configuring Layer 7 Firewall Policies: Example, page 42](#)
- [Configuring a Security Zone: Example, page 42](#)
- [Configuring a Zone-Pair: Example, page 42](#)
- [Assigning an Interface to a Security Zone: Example, page 42](#)
- [Attaching a Policy Map to a Zone-Pair: Example, page 43](#)

Configuring Layer 3 and Layer 4 Firewall Policies: Example

The following example shows a Layer 3 / Layer 4 top-level policy. Traffic is matched to access control list 199. There is deep-packet HTTP inspection.

```
class-map type inspect match-all http-traffic
 match protocol http
 match access-group 199
policy-map type inspect mypolicy
 class type inspect http-traffic
 inspect
```

```
service-policy http http-policy
```

Configuring Layer 7 Firewall Policies: Example

The following example matches HTTP sessions that have a URL length greater than 500. The Layer 7 policy action is **reset**.

```
class-map type inspect http long-urls
  match request uri length gt 500
policy-map type inspect http http-policy
  class type inspect http long-urls
    reset
```

The following example enables inspection for ESMTP by including the **extended** keyword:

```
class-map type inspect c1
  match protocol smtp extended

policy-map type inspect p1
  class type inspect c1
    inspect
```

Now the **service-policy type inspect smtp** command is optional and can be entered after the **inspect** command.

Configuring a Security Zone: Example

The following example creates security zone z1 which is called Internet Traffic.

```
zone security z1
  description Internet Traffic
```

Configuring a Zone-Pair: Example

The following example creates zones z1 and z2, describes the zones, and specifies that the firewall policy map will be applied in zone z2 for traffic flowing between the zones:

```
zone security z1
  description finance department networks

zone security z2
  description engineering services network

zone-pair security zp source z1 destination z2
```

Assigning an Interface to a Security Zone: Example

The following example attaches interface ethernet0 to zone z1:

```
interface ethernet0
  zone-member security z1
```


Attaching a Policy Map to a Zone-Pair: Example

The following example attaches a firewall policy map to the target zone-pair p1:

```
zone-pair security zp source z1 destination z2
service-policy type inspect p1
```

Additional References

The following sections provide references related to Zone-Based Policy Firewall.

Related Documents

Related Topic	Document Title
Security commands	<i>Cisco IOS Security Command Reference</i> , Release 12.4
Quality of Service commands	<i>Cisco IOS Quality of Service Solutions Command Reference</i> , Release 12.4

Standards

Standard	Title
No new or modified standards are supported by this release.	—

MIBs

MIB	MIBs Link
•	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this release.	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html.

- **class-map type inspect**
- **class type inspect**
- **clear parameter-map type protocol-info**
- **debug policy-firewall**
- **match body regex**
- **match file-transfer**
- **match header count**
- **match header length**
- **match header regex**
- **match protocol (zone)**
- **match request length**
- **match request regex**
- **match response status-line regex**
- **match search-file-name**
- **match service**
- **match text-chat**
- **parameter-map type**

- **policy-map type inspect**
- **server (parameter-map)**
- **service-policy (policy-map)**
- **service-policy type inspect**
- **show parameter-map type protocol-info**

Replaced Commands

Command in Cisco IOS Release 12.4(6)T	Replacement Command in Cisco IOS Release 12.4(20)T
debug ip inspect	debug policy-firewall
service-policy inspect	service-policy (policy-map)

Feature Information for Zone-Based Policy Firewall

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Zone-Based Policy Firewall

Feature Name	Releases	Feature Configuration Information
Zone-Based Policy Firewall	12.4(6)T	This feature provides a Cisco IOS unidirectional firewall policy between groups of interfaces known as zones.
Application Inspection And Control for HTTP—Phase 2	12.4(9)T	<p>This feature extends support for HTTP application firewall policies.</p> <p>The following section provides information about this feature: Configuring an HTTP Firewall Policy, page 21</p> <p>The following commands were introduced or modified by this feature: match body regex, match header count, match header length, match header regex, match request length, match request regex, match response status-line regex</p>

Table 1 **Feature Information for Zone-Based Policy Firewall (continued)**

Feature Name	Releases	Feature Configuration Information
P2P Application Inspection and Control—Phase 1	12.4(9)T, 12.4(20)T	<p>This feature introduces support for identifying and enforcing a configured policy for the following peer-to-peer applications: eDonkey, FastTrack, Gnutella Version 2, and Kazaa Version 2.</p> <p>Support for identifying and enforcing a configured policy for the following Instant Messenger applications is also introduced: AOL, MSN Messenger and Yahoo Messenger.</p> <p>In Release 12.4(20)T, support was added for the following applications: H.323 VoIP and SIP.</p> <p>In Release 12.4(20)T, support for the following IM applications was also added: ICQ and Windows Messenger.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Configuring a Protocol-Specific Parameter Map, page 19 • Configuring an Instant Messenger (IM) Policy, page 28 • Configuring a Peer-to-Peer (P2P) Policy, page 30 <p>The following commands were introduced or modified by this feature: class-map type inspect, class type inspect, clear parameter-map type protocol-info, debug policy-firewall, match file-transfer, match protocol (zone), match search-file-name, match service, match text-chat, parameter-map type, policy-map type inspect, server (parameter-map), show parameter-map type protocol-info</p>

Table 1 **Feature Information for Zone-Based Policy Firewall (continued)**

Feature Name	Releases	Feature Configuration Information
Rate-limiting Inspected Traffic	12.4(9)T	<p>This feature allows users to rate limit traffic within a Cisco IOS firewall (inspect) policy. Also, users can limit the absolute number of sessions that can exist on a zone-pair.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Rate Limiting (Policing) Traffic Within a Layer 3 and Layer 4 Policy Map, page 9 • Creating an Inspect Parameter Map, page 15 <p>The following commands were introduced by this feature: police (zone policy), sessions maximum</p>

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2006–2008 Cisco Systems, Inc. All rights reserved.



Cisco IOS Intrusion Prevention System (IPS)



Configuring Cisco IOS Intrusion Prevention System (IPS)

First Published: May 2, 2005

Last Updated: August 7, 2007

This module describes how to configure the Cisco IOS Intrusion Prevention System (IPS), which helps to protect a network from internal and external attacks and threats. Cisco IOS IPS restructures and replaces the existing Cisco IOS Intrusion Detection System (IDS).

Cisco IOS IPS allows customers to choose between any of the following options when loading IPS signatures onto a device:

- Loading the default, built-in signatures.

Download the SDF on the router by using the Cisco Router and Security Device Manager (SDM) to have the latest available detection of security threats. Go to the following link to download the SDF:

<http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup>



Note

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module.

[“Feature Information for Configuring Cisco IOS IPS” section on page 36.](#)

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Contents

-
-
-
- [How to Configure Cisco IOS IPS on a Device, page 16](#)
[Configuration Examples, page 33](#)
[Additional References, page 34](#)
[Feature Information for Configuring Cisco IOS IPS, page 36](#)

Prerequisites for Configuring Cisco IOS IPS

Compatibility with VMS IDS MC 2.3 and Cisco Router SDM

VMS IDS MC provides a web-based interface for configuring, managing, and monitoring multiple IDS sensors. SDM is a web-based device-management tool that allows users to import and edit SDFs from Cisco.com to the router. VMS IDS MC is for network-wide management while SDM is for single-device management. It is strongly recommended that customers download the SDF to an IDS MC 2.3 network management device or an SDM.

Customers can choose to download the SDF to a device other than VMS IDS MC or SDM (such as a router) via command-line interface (CLI); however, this approach is not recommended because it requires that the customer know which signatures come from which signature engines.

Restrictions for Configuring Cisco IOS IPS

Signature Support Deprecation

Effective Cisco IOS Release 12.(8)T, the following signatures are no longer supported by Cisco IOS IPS:

1100 IP Fragment Attack (Attack, Atomic)

Triggers when any IP datagram is received with the “more fragments” flag set to 1 or if there is an offset indicated in the offset field. (To scan for application layer signatures across fragments, you can enable virtual fragment reassembly.)

1105 Broadcast Source Address (Compound/Attack)

Triggers when an IP packet with a source address of 255.255.255.255 is detected. This signature may be an indicator of an IP spoof attack or an attempt to subvert a firewall, proxy, or gateway.

1106 Multicast IP Source Address (Compound/Attack)

Triggers when an IP packet with a source address of 224.x.x.x is detected. This signature may be an indicator of an IP spoof attack or an attempt to subvert a firewall, proxy, or gateway.

8000 FTP Retrieve Password File (Attack, Atomic) SubSig ID: 2101

Triggers on string “passwd” issued during an FTP session. May indicate that someone is attempting to retrieve the password file from a machine to try and gain unauthorized access to system resources.

Memory Impact on Low-End to Midrange Routers

Action Configuration via CLI No Longer Supported

Restrictions for Transparent Cisco IOS IPS

-
-
-

Information About Cisco IOS IPS

-
-
-
-
-
-

Cisco IOS IPS Overview

flow through the router and scanning each packet to match any of the Cisco IOS IPS signatures. When Cisco IOS IPS detects suspicious activity, it responds before network security can be compromised and logs the event through Cisco IOS syslog messages or Security Device Event Exchange (SDEE). The network administrator can configure Cisco IOS IPS to choose the appropriate response to various threats. When packets in a session match a signature, Cisco IOS IPS can take any of the following actions, as appropriate:

- Send an alarm to a syslog server or a centralized management interface
- Drop the packet
- Reset the connection
- Deny traffic from the source IP address of the attacker for a specified amount of time
- Deny traffic on the connection for which the signature was seen for a specified amount of time

Transparent Cisco IOS IPS Overview

Transparent Bridging Overview

Transparent and Non-Transparent IPS Devices Configured on the Same Router

Benefits of Cisco IOS IPS

Dynamic IPS Signatures

Parallel Signature Scanning

Named and Numbered Extended ACL Support

one of the following commands—**ip ips *ips-name* list** **ip ips signature *signature-id* list *acl-list***

The Signature Definition File

- **attack-drop.sdf**

128MB.sdf

256MB.sdf

attack-drop.sdf 128MB.sdf 256MB.sdf



SDF files can be used only with 12.4(9)Tx or earlier IOS Images and mainline images.

To help detect the latest vulnerabilities, Cisco provides signature updates on Cisco.com on a regular basis. Users can use VMS or SDM to download these signature updates, tune the signature parameters as necessary, and deploy the new SDF to a Cisco IOS IPS router.

Signature Microengines: Overview and Lists of Supported Engines

Lists of Supported Signature Engines



Note

Table 1 *Supported Signature Engines for Cisco IOS IPS*

Signature Engine	Initial Supported Cisco IOS Release	Parameter Exceptions ¹
ATOMIC.L3.IP	12.3(8)T	—
ATOMIC.ICMP	12.3(8)T	—
ATOMIC.IPOPTIONS	12.3(8)T	—
ATOMIC.TCP	12.3(8)T	—
ATOMIC.UDP	12.3(8)T	—
SERVICE.DNS	12.3(8)T	—
SERVICE.HTTP	12.3(8)T	ServicePorts (applicable only in Cisco IOS Release 12.3(8)T)
SERVICE.FTP	12.3(8)T	ServicePorts
SERVICE.SMTP	12.3(8)T	ServicePorts
SERVICE.RPC	12.3(8)T	ServicePorts, Unique, and isSweep
STRING.ICMP	12.3(14)T	—
STRING.TCP	12.3(14)T	—
STRING.UDP	12.3(14)T	—

1. The following parameters, which are defined in all signature engines, are currently not supported: AlarmThrottle=Summarize (all other values are supported), MaxInspectLength, MaxTTL, Protocol, ResetAfterIdle, StorageKey, and SummaryKey.

[Table 2](#) lists support for the 100 signatures that are available in Cisco IOS IDS prior to Cisco IOS Release 12.3(8)T. As of Cisco IOS Release 12.3(8)T, these 100 signatures are a part of the Cisco IOS IPS built-in SDF. By default, signatures are loaded from this built-in SDF. [Table 2](#) lists support for these 100 signatures under Cisco IOS IPS.



Because Cisco IOS IPS counts signatures on the basis of signature-id and subsignature-id, the 100 signatures under Cisco IOS IDS are counted as 132 signatures under Cisco IOS IPS.

Table 2 *Support for Signatures Available in Cisco IOS IDS (prior to 12.3(8)T)*

Signature ID	Count	Signature Engine
1000–1006	7	ATOMIC.IPOPTIONS
1101, 1102	2	ATOMIC.L3.IP
1004, 1007	2	ATOMIC.L3.IP

2000–2012, 2150	14	ATOMIC.ICMP
2151, 2154	2	ATOMIC.L3.IP
3038–3043	6	ATOMIC.TCP
3100–3107	8	SERVICE.SMTP
3153, 3154	2	SERVICE.FTP
4050–4052, 4600	4	ATOMIC.UDP
6100–6103	4	SERVICE.RPC
6150–6155	6	SERVICE.RPC
6175, 6180, 6190	3	SERVICE.RPC
6050–6057	8	SERVICE.DNS
6062–6063	2	SERVICE.DNS
3215, 3229, 3223	3	SERVICE.HTTP
5034–5035	2	SERVICE.HTTP
5041, 5043–5045	4	SERVICE.HTTP
5050, 5055, 5071	3	SERVICE.HTTP
5081, 5090, 5123	3	SERVICE.HTTP
5114, 5116–5118	4	SERVICE.HTTP
1100	1	Not applicable. Signature is replaced by 12xx series.
1105–1106	2	Cisco IOS IPS deprecates these signatures, which do not appear in the SDF.
1201–1208	10	OTHER ¹ (fragment attack signatures)
3050	2	OTHER ¹ (SYN attack signatures)
3150–3152	3	STRING.TCP
4100	1	STRING.UDP
8000	1	Cisco IOS IPS deprecates these signatures, which do not appear in the SDF.

1. The OTHER engine contains existing, hard-coded signatures. Although the standard SDF contains an entry for these signatures, the engine is not dynamically updated. If the SDF that is loaded onto the engine does not contain the signature, the signature will be treated as though it has been disabled.

Supported Cisco IOS IPS Signatures in the attack-drop.sdf File

- [Cisco IOS IPS Signatures in the attack-drop.sdf File](#). (You must have a valid Cisco.com account to access this web page.)
- Download the attack-drop.sdf file, which contains the signatures that are identified in [Table 3](#).

Cisco IOS IPS Signatures Supported in Cisco IOS Release 12.3(8)T

Signature ID: SubSig ID	Signature Name	Action ¹	SME	Signature Description
				Control Message Protocol [ICMP]), the Last Fragment bit is set. The IP offset (which represents the starting position of this fragment in the original packet and which is in 8-byte units) plus the rest of the packet is greater than the maximum size for an IP packet.
3038:0	Fragmented NULL TCP Packet	A, D	ATOMIC.TCP	Triggers when a single, fragmented TCP packet with none of the SYN, FIN, ACK, or RST flags set has been sent to a specific host. A reconnaissance sweep of your network may be in progress.
3039:0	Fragmented Orphaned FIN packet	A, D	ATOMIC.TCP	Triggers when a single, fragmented, orphan TCP FIN packet is sent to a privileged port (having a port number less than 1024) on a specific host. A reconnaissance sweep of your network may be in progress.
3040:0	NULL TCP Packet	A, D	ATOMIC.TCP	Triggers when a single TCP packet with none of the SYN, FIN, ACK, or RST flags set has been sent to a specific host. A reconnaissance sweep of your network may be in progress.
3041:0	SYN/FIN Packet	A, D	ATOMIC.TCP	Triggers when a single TCP packet with the SYN and FIN flags set is sent to a specific host. A reconnaissance sweep of your network may be in progress. The use of this type of packet indicates an attempt to conceal the sweep.
3043:0	Fragmented SYN/FIN Packet	A, D	ATOMIC.TCP	Triggers when a single, fragmented TCP packet with the SYN and FIN flags set is sent to a specific host. A reconnaissance sweep of your network may be in progress. The use of this type of packet indicates an attempt to conceal the sweep.

3129:0	Mimail Virus C Variant File Attachment	A, D, R	SERVICE.SMTP	Fires when an e-mail attachment matching the C Variant of the Mimail virus is detected. The virus sends itself to recipients as the e-mail attachment “photos.zip” that contains the file “photos.jpg.exe” and has “our private photos” in the e-mail subject line. If launched, the virus harvests e-mail addresses and possible mail servers from the infected system.
3140:3	Bagle Virus Activity²	A, D, R	SERVICE.HTTP	Fires when HTTP propagation using .jpeg associated with the .Q variant is detected.
3140:4	Bagle Virus Activity³	A, D, R	SERVICE.HTTP	Fires when HTTP propagation using .php associated with the .Q variant is detected.
3300:0	NetBIOS OOB Data	A, D	ATOMIC.TCP	Triggers when an attempt to send Out Of Band data to port 139 is detected.
5045:0	WWW xterm display attack	A, D, R	SERVICE.HTTP	Triggers when any cgi-bin script attempts to execute the command xterm -display. An attempt to illegally log into your system may be in progress.
5047:0	WWW Server Side Include POST attack	A, D, R	SERVICE.HTTP	Triggers when an attempt is made to embed a server side include (SSI) in an http POST command. An attempt to illegally access system resources may be in progress.
5055:0	HTTP Basic Authentication Overflow	A, D	SERVICE.HTTP	A buffer overflow can occur on vulnerable web servers if a very large username and password combination is used with basic authentication.
5071:0	WWW msacds.dll Attack	A, D, R	SERVICE.HTTP	An attempt has been made to execute commands or view secured files, with privileged access. Administrators are highly recommended to check the affected systems to ensure that they have not been illicitly modified.
5081:0	WWW WinNT cmd.exe Access	A, D, R	SERVICE.HTTP	Triggers when the use of the Windows NT cmd.exe is detected in a URL. This signature can detect the NIMDA attack.
5114: 0 5114:1 5114:2	WWW IIS Unicode Attack	A, D, R	SERVICE.HTTP	Triggers when an attempt to exploit the Unicode ../ directory traversal vulnerability is detected. Looks for the commonly exploited combinations that are included in publicly available exploit scripts. SubSig 2 is know to detect the NIMDA attack.
5126:0	WWW IIS .ida Indexing Service Overflow	A, D, R	SERVICE.HTTP	Alarms if web traffic is detected with the ISAPI extension .ida? and a data size of greater 200 characters.
5159:0	phpMyAdmin Cmd Exec	A, D, R	SERVICE.HTTP	Triggers when access to sql.php with the arguments goto and btnDrop=No is detected.

	⁴ SubSig 0: GotomyPC	A, D, R	SERVICE.HTTP	Triggers when a computer connects to gotomyPC site.
5188:1	HTTP Tunneling SubSig 1: FireThru	A, D, R	SERVICE.HTTP	Triggers when an attempt to use /cgi-bin/proxy is detected. The /cgi-bin/proxy is used to tunnel connections to other ports using web ports.
5188:2	HTTP Tunneling SubSig 2: HTTP Port	A, D, R	SERVICE.HTTP	Triggers when a connection is made to exectech-va.com. The site runs a server, which connects to the requested resource and passes the information back to the client on web ports.
5188:3	HTTP Tunneling SubSig 3: httptunnel	A, D, R	SERVICE.HTTP	Triggers when /index/html? is detected on POST request.
5245:0	HTTP 1.1 Chunked Encoding Transfer	A, D, R	SERVICE.HTTP	Fires when HTTP 1.1 chunked encoding transfer activity is detected. This signature is known to detect the Scalper Worm.
5326:0	Root.exe access	A, D, R	SERVICE.HTTP	Alarms upon detecting an HTTP request for root.exe. This signature is known to detect the NIMDA attack.
5329:0	Apache/mod_ssl Worm Probe	A, D, R	SERVICE.HTTP	Fires when a probe by the Apache/mod_ssl worm is detected. If the worm detects a vulnerable web server, a buffer overflow attack is sent to HTTPS port (TCP 443) of the web server. The worm then attempts to propagate itself to the newly infected web server and begins scanning for new hosts to attack.
5364:0	IIS WebDAV Overflow	A, D, R	SERVICE.HTTP	Fires when a long HTTP request (65000+ characters) is detected with an HTTP header option "Translate:". An attack to exploit a weakness in the WebDAV component of the IIS web server may be in progress.
5390:0	Sven Worm HTTP Counter Update Attempt	A, D, R	SERVICE.HTTP	Triggers when an attempt to access the URL "/bin/counter.gif/link=bacillus" is detected. A system may be infected by the Sven worm trying the update a counter on a web page located on the server "ww2.fce.vutbr.cz."
5400:0	Beagle.B (Bagle.B) Web Beacon	A, D, R	SERVICE.HTTP	Fires when a request is made for the script 1.php or 2.php residing on the hosts "www.47df.de" or "www.strato.de," followed by the argument indicating the trojan's listening port number, p=8866.

6055:0 6055:1 6055:2	DNS Inverse Query Buffer Overflow	A, D R for subsig 1, 2	SERVICE.DNS	Triggers when an IQUERY request arrives with a data section that is greater than 255 characters.
6056:0 6056:1 6056:2	DNS NXT Buffer Overflow	A, D R for subsig 1, 2	SERVICE.DNS	Triggers when a Domain Name System (DNS) server response arrives with a long NXT resource where the length of the resource data is greater than 2069 bytes or the length of the TCP stream containing the NXT resource is greater than 3000 bytes.
6057:0 6057:1 6057:2	DNS SIG Buffer Overflow	A, D R for subsig 1, 2	SERVICE.DNS	Triggers when a DNS server response arrives with a long SIG resource where the length of the resource data is greater than 2069 bytes or the length of the TCP stream that contains the SIG resource is greater than 3000 bytes.
6058:0 6058:1	DNS SRV DoS	A, D R for subsig 1	SERVICE.DNS	Alarms when a DNS query type SRV and DNS query class IN is detected with more than ten pointer jumps in the SRV resource record.
6059:0 6059:1 6059:2	DNS TSIG Overflow	A, D R for subsig 2	SERVICE.DNS	Alarms when a DNS query type TSIG is detected and the domain name is greater than 255 characters. This signature is known to detect the Lion work.
6060:0 6060:1 6060:2 6060:3	DNS Complan Overflow	A, D R for subsig 2, 3	SERVICE.DNS	Alarms when a Name Server (NS) record is detected with a domain name greater than 255 characters and the IP address is 0.0.0.0, 255.255.255.255 or a multicast address of the form 224.x.x.x.
6100:0 6100:1	RPC Port Registration	A, D R for subsig 1	SERVICE.RPC	Triggers when attempts are made to register new RPC services on a target host. Port registration is the method used by new services to report their presence to the portmapper and to gain access to a port. Their presence is then advertised by the portmapper.
6101:0 6101:1	RPC Port Unregistration	A, D R for subsig 1	SERVICE.RPC	Triggers when attempts are made to unregister existing Remote Procedure Call (RPC) services on a target host. Port unregistration is the method used by services to report their absence to the portmapper and to remove themselves from the active port map.
6104:0 6104:1	RPC Set Spoof	A, D R for subsig 1	SERVICE.RPC	Triggers when an RPC set request with a source address of 127.x.x.x is detected.

6105:0 6105:1	RPC Unset Spoof	A, D R for subsig 1	SERVICE.RPC	Triggers when an RPC unset request with a source address of 127.x.x.x is detected.
6188:0	statd dot dot	A, D	SERVICE.RPC	Alarms upon detecting a dot dot slash (../) sequence sent to the statd RPC service.
6189:0 6189:1	statd automount attack	A, D R for subsig 1	SERVICE.RPC	Alarms upon detecting a statd bounce attack on the automount process. This attack targets a vulnerability in the automount process that could be exploited only via localhost.
6190:0 6190:1	statd Buffer Overflow	A, D R for subsig 1	SERVICE.RPC	Triggers when a large statd request is sent. This attack could be an attempt to overflow a buffer and gain access to system resources.
6191:0 6191:1	RPC.tooltalk buffer overflow	A, D R for subsig 1	SERVICE.RPC	Fires when an attempt is made to overflow an internal buffer in the tooltalk rpc program.
6192:0 6192:1	RPC mountd Buffer Overflow	A, D R for subsig 1	SERVICE.RPC	Triggers on an attempt to overflow a buffer in the RPC mountd application. This attack may result in unauthorized access to system resources.
6193:0 6193:1	RPC CMSD Buffer Overflow	A, D R for subsig 1	SERVICE.RPC	Fires when an attempt is made to overflow an internal buffer in the Calendar Manager Service Daemon, rpc.cmsd.
6194:0 6194:1	sadmind RPC Buffer Overflow	A, D R for subsig 1	SERVICE.RPC	Fires when a call to RPC program number 100232 procedure 1 with a UDP packet length greater than 1024 bytes is detected.
6195:0 6195:1	RPC amd Buffer Overflow	A, D R for subsig 1	SERVICE.RPC	Detects the exploitation of the RPC AMD Buffer Overflow vulnerability. The trigger for this signature is an RPC call to the berkeley automounter daemons rpc program (300019) procedure 7 that has a UDP length greater than 1024 bytes or a TCP stream length greater than 1024 bytes. The TCP stream length is defined by the contents of the two bytes preceding the RPC header in a TCP packet.
6196:0 6196:1	snmpXdmid Buffer Overflow	A, D R for subsig 1	SERVICE.RPC	Fires when an abnormally long call to the RPC program 100249 (snmpXdmid) and procedure 257 is detected.
6197:0 6197:1	rpc yppaswdd overflow	A, D R for subsig 0	SERVICE.RPC	Fires when an overflow attempt is detected. This alarm looks for an abnormally large argument in the attempt to access yppaswdd.

[illegible]

				the Bagle.H-J virus.
9240:0	Back Door Response (TCP 2556)	A, D	ATOMIC.TCP	Fires upon detecting a TCP SYN/ACK packet from port 2556, which is a known trojan port for the Bagle (.M.N.O.P) virus.
9241:0	Back Door Response (TCP 4751)	A, D	ATOMIC.TCP	Fires upon detecting a TCP SYN/ACK packet from port 4751, which is a known trojan port for the Bagle.U virus.

1. A = alarm, D = drop, R = reset
2. This signature requires port to application mapping (PAM) configuration via the command **ip port-map http port 81**
3. This signature requires PAM configuration via the command **ip port-map http port 81.**
4. This signature requires PAM configuration via the command **8200**

How to Configure Cisco IOS IPS on a Device

-

SDM Intrusion Prevention System (IPS)

Configuring a Bridge Group for Transparent Cisco IOS IPS


Note

BVI Configuration Requirements

-
-
-
-

Restrictions

-
-

SUMMARY STEPS

- enable
- configure terminal
- bridge-group { | | vlan-bridge}
-
-
- exit
-
-
-
- ip-address mask
-

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	
	Example: Router> enable	
	configure terminal	
	Router# configure terminal	
	bridge bridge-group protocol { vlan-bridge}	
	Router(config)# bridge 1 protocol ieee type number	
	Router(config)# interface Ethernet0	

bridge-group	
exit	
Router(config-if)# exit	
bridge irb	
Router(config)# bridge irb	
bridge route protocol	
<i>type number</i>	
ip address <i>ip-address mask</i>	
Router(config-if) ip address 10.1.1.1 255.255.255.0	
no shutdown	
Router(config-if)# no shutdown	

Examples

```

                bridge 1 protocol ieee
                interface ethernet0
Router(config-if)# bridge-group 1
Router(config-if)# interface ethernet1
Router(config-if)# bridge-group 1
Router(config-if)# exit
! Configure the BVI.
Router(config)#
Router(config)#
Router(config)# interface BVI1

```

```
Router(config-if)# ip address 10.1.1.1 255.255.255.0
no shutdown
```

Troubleshooting Tips

```
show bridge
show bridge-group
```

What to Do Next

Installing Cisco IOS IPS on a New Router


Note

SUMMARY STEPS

- 1.
- 2.
- 3.
- 4.
- 5. : delete disable list
- 6. ip ips deny-action ips-interface
interface
ip ips in out
exit
show ip ips configuration

disk2:attack-drop.sdf	
[]	
Router(config)# ip ips name MYIPS	
[:] {delete disable list }	
Router(config)# ip ips signature 1000 disable	
ip ips deny-action ips-interface	
Router(config)# ip ips deny-action ips-interface	
Router(config)# interface GigabitEthernet0/1	

	Command or Action	Purpose
Step 8	Example:	Note
Step 9	Example: Example:	
Step 10	Example:	

Upgrading to the Latest Cisco IOS IPS Signature Definition File (SDF)



Note


Prerequisites

SUMMARY STEPS

- 1.
- 2.

- 3.
- 4.
- 5.
- 6.
- 7.
- 8.
- 9.
- 10.
- 11.
- 12.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Example:	•
Step 2	Example:	
Step 3	Example:	
Step 4	Example:	
Step 5	Example:	<div>  </div> <div>Caution</div>
Step 6	Example:	<ul style="list-style-type: none"> • •

	Command or Action	Purpose
Step 7	Example:	Note
Step 8	Example:	
Step 9	Example:	<ul style="list-style-type: none"> Note
Step 10	Example:	
Step 11	Example:	
Step 12	Example:	


Merging Built-In Signatures with the attack-drop.sdf File

Prerequisites

SUMMARY STEPS

- 1.
- 2.
- 3.
- 4.
- 5.
6. `/erase ips-sdf`
7. `copy ips-sdf`
8. `configure terminal`
9. `ip ips signature : delete disable list`
10. `ip ips sdf location`
- 11.
12. `interface`
13. `ip ips in out`
- 14.
- 15.
16. `show ip ips signatures detailed`

DETAILED STEPS

	Command or Action	Purpose
Step 1	Example:	<ul style="list-style-type: none">
Step 2	Example:	
Step 3	Example:	<div> Caution</div>
Step 4	Example:	<ul style="list-style-type: none">
Step 5	Example:	

Step 6

Example:

`/erase` `/erase`

Note

Note

Step 7

Example:

Step 8

Example:

Step 9

Example:

```
Router(config)# ip ips signature 1107 disable
ip ips sdf location
```

```
Router(config)# ip ips sdf location
disk2:my-signatures.sdf
```

	<i>acl</i>

Monitoring Cisco IOS IPS Signatures via Syslog Messages or SDEE

Cisco IOS Configuration Fundamentals Configuration Guide



Cisco IOS Security Configuration Guide

Storing SDEE Events in the Buffer

-
-
-

Prerequisites

SUMMARY STEPS

- 1.
- 2.
- 3.
4. *events*
5. *subscriptions*
- 6.
- 7.

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>Example:</p>	<ul style="list-style-type: none">
Step 2	<p>Example:</p>	
Step 3	<p>Example:</p>	
Step 4	<p><i>events</i></p> <p>Router(config)# ip sdee events 500</p> <p>Router(config)# ip sdee subscriptions 1</p> <p>Router(config)# exit</p> <pre>{[] [] [] [] } [] [] [] [] }</pre> <p>Router# show ip sdee configuration</p>	

Troubleshooting Tips

Troubleshooting Cisco IOS IPS

.

Interpreting Cisco IOS IPS System Messages

Table 4 *Cisco IOS IPS System Messages*

System Message	Description
Alarm Messages	
%IPS-4-SIGNATURE:Sig:1107 Subsig:0 Sev:2 RFC1918 address [192.168.121.1:137 -> 192.168.121.255:137]	
%IPS-5-SIGNATURE:Sig:1107 Subsig:0 Global Summary:50 alarms in this interval	
%IPS-6-ENGINE_READY:SERVICE.HTTP - 183136 ms - packets for this engine will be scanned	
%IPS-6-ENGINE_BUILD_SKIPPED:STRING.UDP - there are no new signature definitions for this engine	
%IPS-5-PACKET_DROP:SERVICE.DNS - packets dropped while engine is building	
%IPS-5-PACKET_UNSCANNED:SERVICE.DNS - packets passed unscanned while engine is building	
%IPS-6-SDF_LOAD_SUCCESS:SDF loaded successfully from flash:sdf_8http.xml	
Error Messages	
%IPS-3-BUILTIN_SIGS:Configured to load builtin signatures	
%IPS-3-BUILTIN_SIGS:Not Configured to load builtin signatures	
%IPS-3-BUILTIN_SIGS:Failed to load builtin signatures	

<pre>%IPS-5-ENGINE_UNKNOWN: SERVICE.GENERIC - unknown engine encountered while parsing SDF</pre>	
<pre>%IPS-5-UNSUPPORTED_PARAM: SERVICE.RPC 6275:1 isSweep=False - bad parameter - removing parameter</pre>	
<pre>%IPS-3-ENGINE_BUILD_FAILED: SERVICE.HTTP - 158560 ms - engine build</pre>	
<pre>%IPS-4-SDF_PARSE_FAILED: not well-formed (invalid token) at Line 1 Col 0 Byte 0 Len 1006</pre>	
<pre>%IPS-4-SDF_LOAD_FAILED: failed to parse SDF from tftp://tftp-server/sdf.xml</pre>	
<pre>%IPS-2-DISABLED: IPS removed from all interfaces - IPS disabled</pre>	

Conditions of an SME Build Failure

-

-

-



Note

Configuration Examples

-

-

-

Loading the Default Signatures: Example

```
media-type rj45
no negotiation auto
!
```

Loading the attack-drop.sdf: Example

```
!
ip ips sdf location disk2:attack-drop.sdf
ip ips name MYIPS
!
```

Merging the attack-drop.sdf File with the Default, Built-in Signatures: Example

```
copy disk2:attack-drop.sdf ips-sdf

copy ips-sdf disk2:my-signatures.sdf

! Configure the router to use the new file, my-signatures.sdf
Router#
Router(config)#
! Reinitialize the IPS by removing the IPS rule set and reapplying the rule set.
Router(config-if)# interface gig 0/1
Router(config-if)# no ip ips MYIPS in

*Apr 8 14:05:38.243:%IPS-2-DISABLED:IPS removed from all interfaces - IPS disabled
!
Router(config-if)# ip ips MYIPS in
!
Router(config-if)# exit
```

Additional References

Related Documents

Related Topic	Document Title
	Cisco IOS Security Command Reference
	Cisco IOS Configuration Fundamentals Configuration Guide
	Virtual Fragmentation Reassembly
	Transparent Cisco IOS Firewall

Standards

MIBs

MIBs	MIBs Link

RFCs

RFCs	Title
	—

Technical Assistance

Description	Link

Feature Information for Configuring Cisco IOS IPS



Note

Table 5 *Feature Information for Configuring Cisco IOS IPS*

	Software Releases	Feature Configuration Information
		<ul style="list-style-type: none"> • •

Feature Name	Software Releases	Feature Configuration Information
		<ul style="list-style-type: none">•••
		<ul style="list-style-type: none">••

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





Cisco IOS IPS 5.x Signature Format Support and Usability Enhancements

First Published: November 17, 2006

Last Updated: November 17, 2006

This feature introduces support for Cisco IOS Intrusion Prevention System (IPS) version 5.0, which is a version-based signature definition XML format. In Cisco IOS Release 12.4(11)T, Cisco IOS IPS 4.x format signatures are replaced by the 5.x format signatures that are used by all other Cisco IPS devices.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Cisco IOS 5.x Format Signatures with Cisco IOS IPS](#)” section on page 31.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Cisco IOS 5.x Format Signatures with Cisco IOS IPS, page 2](#)
- [Restrictions for Cisco IOS 5.x Format Signatures with Cisco IOS IPS](#)
- [Information About Cisco IOS 5.x Format Signatures with Cisco IOS IPS, page 3](#)
- [How to Use Cisco IOS 5.x Format Signatures with Cisco IOS IPS, page 6](#)
- [Configuration Examples, page 25](#)
- [Additional References, page 28](#)
- [Command Reference, page 29](#)
- [Feature Information for Cisco IOS 5.x Format Signatures with Cisco IOS IPS, page 31](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for Cisco IOS 5.x Format Signatures with Cisco IOS IPS

System and Image Requirements for Cisco IOS IPS 5.x

- Cisco IOS IPS signature categories are available in two formats—Basic and Advanced.
- Cisco IOS IPS system requirements depend on the type of deployment, the bandwidth requirements, and security requirements. The larger the number of signatures, the larger the amount of memory consumed.
- You must generate a RSA crypto key and load the public signature on your router for signature decryption.

This following cisco public key configuration can be cut and pasted directly into your router configuration:

```
crypto key pubkey-chain rsa
named-key realm-cisco.pub signature
key-string
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
50437722 FFBEB85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
F3020301 0001
quit
```



Note You can also access the public key configuration at the following URL:
<http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup>

- You must load one of the following images on your router to install Cisco IOS IPS 5.x: `adventerprisek9`, `advsecurityk9`, and `advipservicesk9`.



Note To check the current system version, use the **show subsys name ips** command.

IPS 4.x uses a version format of 2.xxx.xxx; IPS 5.x uses a version format of 3.xxx.xxx.

Upgrading from Cisco IOS IPS 4.x to Cisco IOS IPS 5.x Signatures

Cisco IOS IPS 5.x format signatures are not backward compatible with Cisco IOS IPS 4.x. You must reconfigure your Cisco IOS IPS features for use with the IPS 5.x signature format command-line interface (CLI) and features.

When reconfiguring Cisco IOS IPS on a router to convert to the 5.x signature format, you must have the following Cisco IOS IPS 4.x information:

- Cisco IOS IPS rule name (which was specified via the **ip ips name ips-name** command)
- Interfaces for which the Cisco IOS IPS rule has been applied
- User-created and customized signature definition files (SDFs)

To gather this information, issue the **show ip ips configuration** command, which displays a copy of the existing output.

```
Router# show ip ips configuration
Configured SDF Locations:
disk2:my-signatures.sdf
Builtin signatures are enabled but not loaded
Last successful SDF load time: 05:31:54 MST Sep 20 2003
IPS fail closed is disabled
Fastpath ips is enabled
Quick run mode is enabled
Event notification through syslog is enabled
Event notification through SDEE is enabled
Total Active Signatures: 13
Total Inactive Signatures: 0
Signature 50000:0 disable
Signature 50000:1 disable
Signature 50000:2 disable
IPS Rule Configuration
IPS name MYIPS
Interface Configuration
Interface GigabitEthernet0/1
Inbound IPS rule is MYIPS
Outgoing IPS rule is not set
```

**Note**

Detailed or customized changes to specific signatures may be lost. IPS 4.x SDF files will not load under the Cisco IOS IPS 5.x version.

Restrictions for Cisco IOS 5.x Format Signatures with Cisco IOS IPS

Backward Compatibility

Cisco IOS IPS 5.x format signatures are not backward compatible with Cisco IOS IPS 4.x SDFs.

Cisco 870 Series Platform Support

The 870 series platform with Cisco IOS IPS in Cisco IOS Release 12.4(11)T may experience lower performance relative to previous releases (CSCsg57228). The Cisco IOS IPS performance on the 870 series platform will be enhanced in a later 12.4(11)T image rebuild.

On the 870 series platform, Cisco IOS IPS is supported only on the adv-ipservices and the adv-enterprise images. Cisco IOS IPS is the same on both images.

Information About Cisco IOS 5.x Format Signatures with Cisco IOS IPS

Before using Cisco IOS 5.x format signatures with Cisco IOS IPS, you should understand the following concepts:

- [Cisco IOS IPS Overview, page 4](#)
- [Signature Categories, page 4](#)

- [Benefits of Cisco IOS 5.x Format Signatures with Cisco IOS IPS, page 5](#)
- [Signature Update Accessibility, page 5](#)

Cisco IOS IPS Overview

The Cisco IOS IPS acts as an in-line intrusion prevention sensor, watching packets and sessions as they flow through the router and scanning each packet to match any of the Cisco IOS IPS signatures. When it detects suspicious activity, it responds before network security can be compromised and logs the event through Cisco IOS syslog messages or Security Device Event Exchange (SDEE). The network administrator can configure Cisco IOS IPS to choose the appropriate response to various threats. The Signature Event Action Processor (SEAP) can dynamically control actions that are to be taken by a signature event on the basis of parameters such as fidelity, severity, or target value rating. These parameters have default values but can also be configured via CLI. When packets in a session match a signature, Cisco IOS IPS can take any of the following actions, as appropriate:

- Send an alarm to a syslog server or a centralized management interface
- Drop the packet
- Reset the connection
- Deny traffic from the source IP address of the attacker for a specified amount of time
- Deny traffic on the connection for which the signature was seen for a specified amount of time

Cisco developed its Cisco IOS software-based intrusion-prevention capabilities and Cisco IOS Firewall with flexibility in mind, so that individual signatures could be disabled in case of false positives. Generally, it is preferable to enable both the firewall and Cisco IOS IPS to support network security policies. However, each of these features may be enabled independently and on different router interfaces.

Signature Categories

Cisco IPS appliances and Cisco IOS IPS with Cisco 5.x format signatures operate with signature categories. All signatures are pregrouped into categories; the categories are hierarchical. An individual signature can belong to more than one category. Top-level categories help to define general types of signatures. Subcategories exist beneath each top-level signature category. (For a list of supported top-level categories, use your router CLI help (?).)

Router Configuration Files and Signature Event Action Processor (SEAP)

As of Cisco IOS Release 12.4(11)T, SDFs are no longer used by Cisco IOS IPS. Instead, routers access signature definition information via a directory that contains three configuration files—the default configuration, the delta configuration, and the SEAP configuration. Cisco IOS accesses this directory via the **ip ips config location** command.



Note

You must issue the **ip ips config location** command; otherwise, the configuration files are not saved to any location.

SEAP is the control unit responsible for coordinating the data flow of a signature event. It allows for advanced filtering and signature overrides on the basis of the Event Risk Rating (ERR) feedback. ERR is used to control the level in which a user chooses to take actions in an effort to minimize false positives.

Signatures once stored in NVRAM, will now be stored in the delta configuration file; thus, support for access control lists (ACLs) is no longer necessary.

Additional Risk Rating Algorithms

The ERR characterizes the risk of an attack and allows users to make decisions on the basis of the risk control signature event actions. To help further control signature event actions, the following additional rating categories are now supported:

- **Attack Severity Rating (ASR)**—Determines the severity of an attack. The attack-severity rating values are hard-coded in Cisco IOS IPS as follows: high, medium, low, and informational. The ASR can be changed via the **alert-rating** command. To change the ASF, see the section “[Tuning Signature Parameters](#).”
- **Signature Fidelity Rating (SFR)**—Determines the confidence level of detecting a true positive. The SFR can be changed via the **fidelity-rating** command. To change the SFR, see the section “[Tuning Signature Parameters](#).”
- **Target Value Rating (TVR)**—Allows users to develop security policies that can be more strict for some resources than others. The security policy is applied to a table of hosts that are protected by Cisco IOS IPS. A host can be a single IP address or a range of IP addresses with an associated target value rating. To configure the TVR, see the task “[Setting the Target Value Rating](#).”

Benefits of Cisco IOS 5.x Format Signatures with Cisco IOS IPS

Automatic Signature Update

With Cisco IOS IPS 5.0, customers can now configure automatic signature updates from local servers.

Network administrators can either preserve the user's current configuration of signature actions or override the user's current configuration of signature actions with the current IPS configuration.

Auto update can also update the CLI signature package.

If this feature is enabled, signatures are delivered in either a Basic signature file or an Advanced signature file.

Signature Category-Based Configuration

Top-level signature categories help to classify signatures for easy grouping and tuning; that is, group-wide parameters, such as signature event action, can be applied to a group via CLI, so the user does not have to modify each individual signature.

Encrypted Signature Support

Cisco IOS IPS introduces support for encrypted (NDA) signatures.

Signature Update Accessibility

To help detect the latest vulnerabilities, Cisco provides the following signature update options:

- Download the latest signature file package from Cisco.com at the following URL:
<http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup>
- Configure automatic signature updates via the **ip ips autoupdate** command. Updates can be configured to run on the basis of a preset time. For more information, see the task “[Enabling Automatic Signature Updates](#).”

- Issue the **copy url idconf** command to instruct the router where to load a signature file. (The file can be saved in a location specified via the **ip ips config location** command.)

How to Use Cisco IOS 5.x Format Signatures with Cisco IOS IPS

This section contains the following procedures:

- [Retiring All Signatures and Selecting a Category of Signatures, page 6](#)
- [Configuring Cisco IOS IPS on Your Router, page 8](#)
- [Loading a Signature File into Cisco IOS IPS, page 11](#)
- [Tuning Signature Parameters, page 12](#)
- [Setting the Target Value Rating, page 18](#)
- [Enabling Automatic Signature Updates, page 19](#)
- [Monitoring Cisco IOS IPS Signatures via Syslog Messages or SDEE, page 22](#)

Retiring All Signatures and Selecting a Category of Signatures

Router memory and resource constraints prevent a router from loading all Cisco IOS IPS signatures. Thus, it is recommended that you load only a selected set of signatures that are defined by the categories. Because the categories are applied in a “top-down” order, you should first retire all signatures, followed by “unretiring” specific categories. Retiring signatures enables the router to load information for all signatures, but the router will not build the parallel scanning data structure.

Retired signatures are not scanned by Cisco IOS IPS, so they will not fire alarms. If a signature is irrelevant to your network or if you want to save router memory, you should retire signatures, as appropriate.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ips signature-category**
4. **category category [sub-category]**
5. **retired {true | false}**
6. **exit**
7. **category category [sub-category]**
8. **retired {true | false}**
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip ips signature-category Example: Router(config)# ip ips signature-category	Enters enters IPS category configuration mode.
Step 4	category category [sub-category] Example: Router(config-ips-category)# category all	Specifies that all categories (and all signatures) will be retired in the following step and enters IPS category action configuration mode.
Step 5	retired {true false} Example: Router(config-ips-category-action)# retired true	Specifies that the router should retire all categories (and all signatures). <ul style="list-style-type: none"> true—Retires all signatures within a given category. false —“Unretires” all signatures within a given category.
Step 6	exit Example: Router(config-ips-category-action)# exit	Exits IPS category action configuration mode.
Step 7	category category [sub-category] Example: Router(config-ips-category)# category ios_ips basic	Specifies the basic category (and a set of signatures) that are to be “unretired” in the following step.
Step 8	retired {true false} Example: Router(config-ips-category-action)# retired false	Specifies that all signatures within the basic category are to be unretired; that is, signatures will be enabled for the basic category.
Step 9	exit Example: Router(config-ips-category-action)# exit Router(config-ips-category)# exit	Exits IPS category action and IPS category configuration modes.

What to Do Next

After you have configured the basic category, you should enable Cisco IOS IPS on your router as shown in the section “[Configuring Cisco IOS IPS on Your Router](#).”

You can customize (or tune) the entire category or individual signatures within a category to addresses the needs of your network. For information on tuning signatures, see the section “[Tuning Signature Parameters](#).”

Configuring Cisco IOS IPS on Your Router

After you have set up a “load definition” for the signature package file to be copied to the idconf, you must configure an IPS rule name. Use this task to configure an IPS rule name and start the IPS configuration.

You can also use this task to configure a Cisco IOS IPS signature location, which tells Cisco IOS IPS where to save signature information.

The configuration location is used to restore the IPS configuration in case the router reboots or IPS is disabled or reenabled. Files, such as signature definition, signature-type definitions, and signature category information, are written in XML format, compressed, and saved to the specified IPS signature location.

SUMMARY STEPS

1. **enable**
2. **mkdir flash:/ips5**
3. **configure terminal**
4. **ip ips name *ips-name***
5. **ip ips config location *url***
6. **interface *type name***
7. **ip ips *ips-name* {in | out}**
8. **exit**
9. **show ip ips configuration**
10. **show ip ips signature *count***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	mkdir flash:/ips5 Example: Router# mkdir flash:/ips5	Create a directory for which Cisco IOS IPS will save signature information. <p>Note The directory location will be specified via the ip ips config location command.</p>
Step 3	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 4	ip ips name ips-name Example: Router(config)# ip ips name myips	Creates an IPS rule.
Step 5	ip ips config location url Example: Router(config)# ip ips config location flash:/ips5	Specifies the location where Cisco IOS IPS will save the signature information, and, if necessary, access the signature configuration information. <p>Note You must specify a location; otherwise, the signature package will not be saved.</p> <p>Note If the specified location is a URL, such as an FTP server, the user must have writer privileges.</p>
Step 6	interface type name Example: Router(config)# interface gigbitEthernet 0/0	Identifies the interface in which to enable Cisco IOS IPS and enters interface configuration mode.
Step 7	ip ips ips-name {in out} Example: Router(config-if)# ip ips MYIPS in	Applies an IPS rule at an interface and automatically loads the signatures and builds the signature engines. <p>Note Whenever signatures are replaced or merged, the router prompt is suspended while the signature engines for the newly added or merged signatures are being built. The router prompt will be available again after the engines are built.</p> <p>Depending on your platform and how many signatures are being loaded, building the engine can take up to several minutes. It is recommended that you enable logging messages to monitor the engine building status.</p>

	Command or Action	Purpose
Step 8	<pre>exit</pre> <p>Example: <pre>Router(config-if)# exit Router(config)# exit</pre></p>	Exits interface and global configuration modes.
Step 9	<pre>show ip ips configuration</pre> <p>Example: <pre>Router# show ip ips configuration</pre></p>	(Optional) Verifies that Cisco IOS IPS is properly configured.
Step 10	<pre>show ip ips signature count</pre> <p>Example: <pre>Router# show ip ips signature</pre></p>	(Optional) Verifies the number of signatures that are loaded into each signature micro engine (SME).

Examples

The following sample output displays the number of signatures that have been loaded into each SME:

```
Router# show ip ips signature count

Cisco SDF release version S247.0
Trend SDF release version V1.2
Signature Micro-Engine: multi-string
Total Signatures: 7
Enabled: 7
Retired: 2
Compiled: 5
Signature Micro-Engine: service-http
Total Signatures: 541
Enabled: 284
Retired: 336
Compiled: 205
Signature Micro-Engine: string-tcp
Total Signatures: 487
Enabled: 332
Retired: 352
Compiled: 135
Signature Micro-Engine: string-udp
Total Signatures: 50
Enabled: 3
Retired: 23
Compiled: 27
Signature Micro-Engine: state
Total Signatures: 26
Enabled: 15
Retired: 23
Compiled: 3
Signature Micro-Engine: atomic-ip
Total Signatures: 140
Enabled: 87
Retired: 93
Compiled: 46
Inactive - invalid params: 1
Signature Micro-Engine: string-icmp
Total Signatures: 2
Enabled: 0
```

```
Retired: 1
Compiled: 1
Signature Micro-Engine: service-ftp
Total Signatures: 3
Enabled: 3
Compiled: 3
Signature Micro-Engine: service-rpc (INACTIVE)
Signature Micro-Engine: service-dns
Total Signatures: 1
Enabled: 1
Retired: 1
Signature Micro-Engine: normalizer
Total Signatures: 9
Enabled: 9
Compiled: 9
Total Signatures: 1266
Total Enabled Signatures: 741
Total Retired Signatures: 831
Total Compiled Signatures: 434
Total Signatures with invalid parameters: 1
```

Loading a Signature File into Cisco IOS IPS

Use this task to load a signature package into Cisco IOS IPS. You may wish to load a new signature package into Cisco IOS IPS if a signature (or signatures) with the current signature package is not providing your network with adequate protection from security threats.

Prerequisites

You must enable Cisco IOS IPS (as shown in the task “[Configuring Cisco IOS IPS on Your Router](#)”) before loading a new signature package.

Flexible Signatures: Ordered and Incremental

Each signature is compiled incrementally into the scanning tables at the same time. Thus, Cisco IOS IPS can deactivate signatures that fail to compile. (Prior to Cisco IOS Release 12.4(11)T, Cisco IOS IPS deactivated the entire signature microengine (SME) if a single signature failed to compile.)

Signatures are loaded into the scanning table on the basis of importance. Parameters such as signature severity, signature fidelity rating, and time lapsed since signatures were last released allow Cisco IOS IPS to compile the most important signatures first, followed by less important signatures, thereby, creating a load order and prioritizing which signatures are loaded first.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ips config location *url***
4. **interface *type name***
5. **ip ips *ips-name* {in | out}**
6. **exit**
7. **copy *url idconf***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip ips config location url Example: Router(config)# ip ips config location flash:/ips5	Specifies the location where Cisco IOS IPS will save the signature information, and, if necessary, access the signature configuration information.
Step 4	interface type name Example: Router(config)# interface gigbitEthernet 0/0	Identifies the interface in which to enable Cisco IOS IPS.
Step 5	ip ips ips-name {in out} Example: Router(config-if)# ip ips MYIPS in	Applies an IPS rule at an interface and automatically loads the signatures and builds the signature engines.
Step 6	exit Example: Router(config-if)# exit Router(config)# exit	Exits interface and global configuration modes.
Step 7	copy url idconf Example: Router# copy tftp://tftp_server/sig.xml idconf	Loads a signature package into Cisco IOS IPS. After the package is loaded, all signature information is saved to the location specified via the ip ips config location command.

Tuning Signature Parameters

You can tune signature parameters on the basis of a signature ID (for an individual signature), or you can tune signature parameters on the basis of a category (that is, all signatures that are within a specified category). To tune signature parameters, use the following tasks, as appropriate:

- [Tuning Signatures Per Signature ID, page 13](#)
- [Tuning Signatures Per Category, page 15](#)

**Note**

Some changes to the signature definitions are not shown in the run time config because the changes are recorded in the sigdef-delta.xml file, which can be located via the **ip ips config location** command.

Tuning Signatures Per Signature ID

Use this task to change default signature parameters for a specified signature ID.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ips signature-definition**
4. **signature** *signature-id* [*subsignature-id*]
5. **engine**
6. **event-action** *action*
7. **exit**
8. **alert-severity** {**high** | **medium** | **low** | **informational**}
9. **fidelity-rating** *rating*
10. **status**
11. **enabled** {**true** | **false**}
12. **exit**
13. **show ip ips signature**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip ips signature-definition Example: Router(config)# ip ips signature-definition	Enters signature-definition-signature configuration mode.
Step 4	signature <i>signature-id</i> [<i>subsignature-id</i>] Example: Router(config-sigdef-sig)# signature 9000:0	Specifies a signature for which the CLI user tunings will be changed and enters signature-definition-action configuration mode.
Step 5	engine Example: Router(config-sigdef-action)# engine	(Optional) Enters signature-definition-action-engine configuration mode, which allows you to change router actions for a specified signature.
Step 6	event-action <i>action</i> Example: Router(config-sigdef-action-engine)# event-action deny-attacker-inline	Changes router actions for a specified signature. The <i>action</i> argument can be any of the following options: <ul style="list-style-type: none">• deny-attacker-inline• deny-connection-inline• deny-packet-inline• produce-alert• reset-tcp-connection Note Signature event actions must be entered on a single line. Note You must enter the engine command before issuing this command.
Step 7	exit Example: Router(config-sigdef-action-engine)# exit	Exits the signature-definition-action-engine configuration mode. This step is required only if the engine and event-action commands are issued.
Step 8	alert-severity { high medium low informational } Example: Router(config-sigdef-action)# alert-severity medium	(Optional) Changes the alert severity rating for a given signature.

	Command or Action	Purpose
Step 9	fidelity-rating <i>rating</i> Example: Router(config-sigdef-action)# fidelity-rating	(Optional) Changes the signature fidelity rating for a given signature.
Step 10	status Example: Router(config-sigdef-action)# status	(Optional) Enters the signature-definition-status configuration mode, which allows you to change the enabled status of a signature.
Step 11	enabled { true false } Example: Router(config-sigdef-status)# enabled true	(Optional) Changes the enabled status of a given signature or signature category.
Step 12	exit Example: Router(config-sigdef-sta)# exit Router(config-sigdef-action)# exit Router(config-sigdef-sig)# exit Router(config)# exit	Returns to EXEC mode, which allows you to later verify the configuration.
Step 13	show ip ips signature Example: Router# show ip ips signature	(Optional) Verifies the signature changes that have been made.

Tuning Signatures Per Category

Use this task to change default signature parameters for a category of signatures. Categories such as operating systems; Layer 2, Layer 3, or Layer 4 protocols; or service-based categories can be configured to provide wider changes to a group of signatures.



Tip

Category configuration information is processed in the order that it is entered. Thus, it is recommended that the process of retiring all signatures (as shown in the task “[Retiring All Signatures and Selecting a Category of Signatures](#)”) occur before all other category tuning.

If a category is configured more than once, the parameters entered in the second configuration will be added to or will replace the previous configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ips signature-category**
4. **category** *category* [*sub-category*]
5. **event-action** *action*
6. **alert-severity** {**high** | **medium** | **low** | **informational**}

7. **fidelity-rating** *rating*
8. **enabled** {true | false}
9. **retired** {true | false}
10. **exit**
11. **show ip ips signature**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip ips signature-category Example: Router(config)# ip ips signature-category	Enters IPS category (config-ips-category) configuration mode.
Step 4	category category [sub-category] Example: Router(config-ips-category)# category attack adware/spyware	Specifies a category that is to be used for multiple signature actions or conditions and enters IPS category action configuration mode.
Step 5	event-action action Example: Router(config-ips-category-action)# event-action produce-alert	Changes router actions for a specified signature category. The <i>action</i> argument can be any of the following options: <ul style="list-style-type: none"> deny-attacker-inline deny-connection-inline deny-packet-inline produce-alert reset-tcp-connection Note Event actions associated with a category can be entered separately or on a single line.
Step 6	alert-severity {high medium low informational} Example: Router(config-ips-category-action)# alert-severity medium	(Optional) Changes the alert severity rating for a given signature category.
Step 7	fidelity-rating rating Example: Router(config-ips-category-action)# fidelity-rating	(Optional) Changes the signature fidelity rating for a signature given category.
Step 8	enabled {true false} Example: Router(config-ips-category-action)# enabled true	(Optional) Changes the enabled status of a given signature or signature category.

	Command or Action	Purpose
Step 9	retired { true false }	(Optional) Specifies whether or not the router should retire a signature category.
	Example: Router(config-ips-category-action)# retired true	
Step 10	exit	Returns to EXEC mode, which allows you to later verify the configuration.
	Example: Router(config-ips-category-action)# exit Router(config-ips-category)# exit Router(config)# exit	
Step 11	show ip ips signature	(Optional) Verifies the signature category changes that have been made.
	Example: Router# show ip ips signature	

Setting the Target Value Rating

Use this task to set the target value rating, which allows users to develop security policies that can be more strict for some resources than others. The security policy is applied to a table of hosts that are protected by Cisco IOS IPS. A host can be a single IP address or a range of IP addresses with an associated target value rating.



Note

Changes to the target value rating is not shown in the run time config because the changes are recorded in the seap-delta.xml file, which can be located via the **ip ips config location** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ips event-action-rules**
4. **target-value** {**mission-critical** | **high** | **medium** | **low**} **target-address** *ip-address* [*/nn* | *to ip-address*]
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip ips event-action-rules Example: Router(config)# ip ips event-action-rules	Enters the config-rule configuration mode, which allows users to change the target value rating.
Step 4	target-value {mission-critical high medium low} target-address ip-address [/nn to ip-address] Example: Router(config-rul)# target-value medium target-address 10.12.100.53	Sets the target value rating for a host.
Step 5	exit Example: Router(config-rul)# exit	Exits config-rule configuration mode.

Enabling Automatic Signature Updates

Automatic signature updates allow users to override the existing configuration and automatically keep signatures up to date on the basis of a preset time, which can be configured to a preferred setting.

Time can be updated via the hardware clock or the configurable software clock (which ever option is available on your system). Although Network Time Protocol (NTP) is typically used for automated time synchronization, Cisco IOS IPS updates use the local clock resources as a reference for update intervals. Thus, NTP should be configured to update the local time server of the router, as appropriate.

Use this task to enable Cisco IOS IPS to automatically update the signature file on the system.

Automatic Signature Update Guidelines

When enabling automatic signature updates, it is recommended that you ensure the following configuration guidelines have been met:

- The router's clock is set up with the proper relative time.
- The frequency for Cisco IOS IPS to obtain updated signature information has been defined.
- The URL in which to retrieve the Cisco IOS IPS signature configuration files has been specified.
- Optionally, the username and password for which to access the files from the server have been specified.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ips auto-update**
4. **occur-at** *min:hour date day*
5. **username** *name* **password** *password*
6. **url** *url*
7. **exit**
8. **show ip ips auto-update**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip ips auto-update Example: Router(config)# ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS and enters IPS auto-update configuration mode.
Step 4	occur-at min:hour date day Example: Router(config-ips-auto-update)# occur-at 0 0-23 1-31 1-5	(Optional) Defines a preset time for which the Cisco IOS IPS signature files are automatically updated.
Step 5	username name password password Example: Router(config-ips-auto-update)# username myips password secret	(Optional) Defines a username and password for the automatic signature update function.
Step 6	url url Example: Router(config-ips-auto-update)# url tftp://192.168.0.2/jdoe/ips-auto-update/IOS_req Seq-dw.xml	(Optional) URL in which the router retrieves the Cisco IOS IPS signature configuration files.
Step 7	exit Example: Router(config-ips-auto-update)# exit Router(config)# exit	Exits IPS auto-update and global configuration modes.
Step 8	show ip ips auto-update Example: Router# show ip ips auto-update	Verifies the automatic signature update configuration.

Examples

The following example shows how to configure automatic signature updates and issue the **show ip ips auto-update** command to verify the configuration. In this example, the signature package file is pulled from the TFTP server at the start of every hour or every day, Sunday through Thursday. (Note that adjustments are made for months without 31 days and daylight savings time.)

```

Router# clock set ?
      hh:mm:ss Current Time
Router# clock set 10:38:00 20 apr 2006
Router#
*Apr 20 17:38:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:37:55 MST
Thu Apr 20 2006 to 10:38:00 MST Thu Apr 20 2006, configured from console by cisco on
console.

Router(config)# ip ips auto-update
Router(config-ips-auto-update)# occur-at 0 0-23 1-31 1-5
Router(config-ips-auto-update)# $s-auto-update/IOS_reqSeq-dw.xml
Router(config-ips-auto-update)# ^Z
Router#
*May 4 2006 15:50:28 MST: IPS Auto Update: setting update timer for next update: 0 hrs 10
min
*May 4 2006 15:50:28 MST: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#
Router# show ip ips auto-update

IPS Auto Update Configuration
  URL : tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml
  Username : not configured
  Password : not configured
  Auto Update Intervals
    minutes (0-59) : 0
    hours (0-23) : 0-23
    days of month (1-31) : 1-31
    days of week: (0-6) : 1-5

```

Monitoring Cisco IOS IPS Signatures via Syslog Messages or SDEE

Cisco IOS IPS provides two methods to report IPS intrusion alerts—Cisco IOS logging (syslog) and SDEE. Perform this task to enable SDEE to report IPS intrusion alerts.

To configure syslog messages, see the chapter “[Troubleshooting and Fault Management](#)” in the *Cisco IOS Network Management Configuration Guide*, Release 12.4.

SDEE Overview

SDEE is an application-level communication protocol that is used to exchange IPS messages between IPS clients and IPS servers. SDEE is always running, but it does not receive and process events from IPS unless SDEE notification is enabled. If SDEE notification is not enabled and a client sends a request, SDEE will respond with a fault response message, indicating that notification is not enabled.

Storing SDEE Events in the Buffer

When SDEE notification is enabled (via the **ip ips notify sdee** command), 200 events can automatically be stored in the buffer. When SDEE notification is disabled, all stored events are lost. A new buffer is allocated when the notifications are reenabled.

When specifying the size of an events buffer, note the following functionality:

- It is circular. When the end of the buffer is reached, the buffer will start overwriting the earliest stored events. (If overwritten events have not yet been reported, you will receive a buffer overflow notice.)
- If a new, smaller buffer is requested, all events that are stored in the previous buffer will be lost.
- If a new, larger buffer is requested, all existing events will be saved.

Prerequisites

To use SDEE, the HTTP server must be enabled (via the **ip http server** command). If the HTTP server is not enabled, the router cannot respond to the SDEE clients because it cannot not “see” the requests.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ips notify sdee**
4. **ip sdee events** *events*
5. **ip sdee subscriptions** *subscriptions*
6. **ip sdee messages** *messages*
7. **ip sdee alerts** *alerts*
8. **exit**
9. **show ip sdee** {[alerts] [all] [errors] [events] [configuration] [status] [subscriptions]}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip ips notify sdee Example: Router(config)# ip ips notify sdee	Enables SDEE event notification on a router.
Step 4	ip sdee events events Example: Router(config)# ip sdee events 500	(Optional) Sets the maximum number of SDEE events that can be stored in the event buffer. <ul style="list-style-type: none">• Maximum value: 1000 events. Note By default, 200 events can be stored in the buffer when SDEE is enabled. When SDEE is disabled, all stored events are lost; a new buffer is allocated when the notifications are reenabled.
Step 5	ip sdee subscriptions subscriptions Example: Router(config)# ip sdee subscriptions 1	(Optional) Sets the maximum number of SDEE subscriptions that can be open simultaneously. <ul style="list-style-type: none">• Valid value ranges from 1 to 3.
Step 6	ip sdee messages messages Example: Router(config)# ip sdee messages 500	(Optional) Sets the maximum number of SDEE messages that can be stored in the buffer at one time.
Step 7	ip sdee alerts alerts Example: Router(config)# ip sdee alerts 2000	(Optional) Sets the maximum number of SDEE alerts that can be stored in the buffer at one time.
Step 8	exit Example: Router(config)# exit	Exits global configuration mode.
Step 9	show ip sdee {[alerts] [all] [errors] [events] [configuration] [status] [subscriptions]} Example: Router# show ip sdee configuration	(Optional) Verifies SDEE configuration information and notification functionality.

Examples

The following example shows how to configure and verify SDEE on your router:

```
Router(config)# ip ips notify SDEE
Router(config)# ip sdee event 500
Router(config)# ip sdee subscriptions 1
Router(config)# ip sdee messages 500
Router(config)# ip sdee alerts 2000
router(config)# exit
*Nov 9 21:41:33.171: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router# show ip sdee all
Configured concurrent subscriptions: 1
No currently open subscriptions.
Alert storage: 2000 alerts using 560000 bytes of memory
Message storage: 500 messages using 212000 bytes of memory
SDEE Events
Time Type Description
Router#
```

Troubleshooting Tips

To print out new SDEE alerts on the router console, issue the **debug ip sdee** command.

To clear the event buffer or SDEE subscriptions from the router (which helps with error recovery), issue the **clear ip sdee** command.

Configuration Examples

This section contains the following configuration example:

- [Cisco IOS IPS Configuration: Example, page 25](#)

Cisco IOS IPS Configuration: Example

The following example shows how to enable and verify Cisco IOS IPS on your router:

```
Router# mkdir flash:/ips5
Create directory filename [ips5]?
Created dir flash:/ips5
Router#
Router#
Router#
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips name MYIPS
Router(config)# ip ips config location flash:/ips5
Router(config)# ip ips signature-category
Router(config-ips-category)# category all
Router(config-ips-category-action)# retired true
Router(config-ips-category-action)# exit
Router(config-ips-category)# category ios_ips advanced
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# exit
Router(config-ips-category)# exit
Do you want to accept these changes? [confirm]
Router(config)# d
*Nov 14 2006 17:16:42 MST: Applying Category configuration to signatures ..
Router(config)#
Router(config)# do show ip interface brief
```

```

Interface          IP-Address      OK?    Method  Status        Protocol
GigabitEthernet0/0 10.0.20.120    YES    NVRAM    up            up
GigabitEthernet0/1 10.12.100.120  YES    NVRAM    administratively down down
NVIO               unassigned     NO     unset    up            up
Router(config)#
Router(config)# interface gigabits 0/0
Router(config-if)# ip ips MYIPS in
Router(config-if)#
*Nov 14 2006 17:17:07 MST: %IPS-6-ENGINE_BUILDS_STARTED: 17:17:07 MST Nov 14 2006
*Nov 14 2006 17:17:07 MST: %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13
engines
*Nov 14 2006 17:17:07 MST: %IPS-6-ENGINE_READY: atomic-ip - build time 0 ms - packets for
this engine will be scanned
*Nov 14 2006 17:17:07 MST: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 0 ms
Router(config-if)#
Router(config-if)# ip ips MYIPS out
Router(config-if)#
Router(config-if)#
Router(config-if)#^Z
Router#
*Nov 14 2006 17:17:23 MST: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router# wr
Building configuration...
[OK]
Router#
Router# show ip ips signature count
Cisco SDF release version S0.0

Signature Micro-Engine: multi-string (INACTIVE)
Signature Micro-Engine: service-http (INACTIVE)
Signature Micro-Engine: string-tcp (INACTIVE)
Signature Micro-Engine: string-udp (INACTIVE)
Signature Micro-Engine: state (INACTIVE)
Signature Micro-Engine: atomic-ip
    Total Signatures: 3
        Enabled: 0
        Compiled: 3
Signature Micro-Engine: string-icmp (INACTIVE)
Signature Micro-Engine: service-ftp (INACTIVE)
Signature Micro-Engine: service-rpc (INACTIVE)
Signature Micro-Engine: service-dns (INACTIVE)
Signature Micro-Engine: normalizer (INACTIVE)
Signature Micro-Engine: service-smb-advanced (INACTIVE)
Signature Micro-Engine: service-msrpc (INACTIVE)
    Total Signatures: 3
    Total Enabled Signatures: 0
    Total Retired Signatures: 0
    Total Compiled Signatures: 3
Router#
Router# copy flash:IOS-S258-CLI-kd.pkg idconf
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_BUILDS_STARTED: 17:19:47 MST Nov 14 2006
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_BUILDING: multi-string - 3 signatures - 1 of 13
engines
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_READY: multi-string - build time 4 ms - packets
for this engine will be scanned
*Nov 14 2006 17:19:47 MST: %IPS-6-ENGINE_BUILDING: service-http - 611 signatures - 2 of 13
engines
*Nov 14 2006 17:20:00 MST: %IPS-6-ENGINE_READY: service-http - build time 12932 ms -
packets for this engine will be scanned
*Nov 14 2006 17:20:00 MST: %IPS-6-ENGINE_BUILDING: string-tcp - 864 signatures - 3 of 13
engines
*Nov 14 2006 17:20:02 MST: %IPS-6-ENGINE_READY: string-tcp - build time 2692 ms - packets
for this engine will be scanned

```

```

*Nov 14 2006 17:20:02 MST: %IPS-6-ENGINE_BUILDING: string-udp - 74 signatures - 4 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: string-udp - build time 316 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: state - 28 signatures - 5 of 13 engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: state - build time 24 ms - packets for
this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: atomic-ip - 252 signatures - 6 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-4-META_ENGINE_UNSUPPORTED: atomic-ip 2154:0 - this
signature is a component of the unsupported META engine
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: atomic-ip - build time 232 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: string-icmp - 3 signatures - 7 of 13 e
Router# engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: string-icmp - build time 12 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-ftp - 3 signatures - 8 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-ftp - build time 8 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-rpc - 75 signatures - 9 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-rpc - build time 80 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-dns - 38 signatures - 10 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-dns - build time 20 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: normalizer - 9 signatures - 11 of 13
engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: normalizer - build time 0 ms - packets for
this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_BUILDING: service-msrpc - 22 signatures - 12 of
13 engines
*Nov 14 2006 17:20:03 MST: %IPS-6-ENGINE_READY: service-msrpc - build time 8 ms - packets
for this engine will be scanned
*Nov 14 2006 17:20:03 MST: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 16344 ms
Router#
Router#
Router# show ip ips signature count
Cisco SDF release version S258.0

```

```

Signature Micro-Engine: multi-string
  Total Signatures: 3
    Enabled: 3
    Retired: 3
Signature Micro-Engine: service-http
  Total Signatures: 611
    Enabled: 159
    Retired: 428
    Compiled: 183
Signature Micro-Engine: string-tcp
  Total Signatures: 864
    Enabled: 414
    Retired: 753
    Compiled: 111
Signature Micro-Engine: string-udp
  Total Signatures: 74
    Enabled: 1
    Retired: 44
    Compiled: 30
Signature Micro-Engine: state
  Total Signatures: 28

```

```
Enabled: 16
Retired: 25
Compiled: 3
Signature Micro-Engine: atomic-ip
Total Signatures: 252
Enabled: 56
Retired: 148
Compiled: 103
Inactive - invalid params: 1
Signature Micro-Engine: string-icmp
Total Signatures: 3
Enabled: 0
Retired: 2
Compiled: 1
Signature Micro-Engine: service-ftp
Total Signatures: 3
Enabled: 1
Compiled: 3
Signature Micro-Engine: service-rpc
Total Signatures: 75
Enabled: 44
Retired: 44
Compiled: 31
Signature Micro-Engine: service-dns
Total Signatures: 38
Enabled: 30
Retired: 5
Compiled: 33
Signature Micro-Engine: normalizer
Total Signatures: 9
Enabled: 8
Retired: 5
Compiled: 4
Signature Micro-Engine: service-smb-advanced (INACTIVE)
Signature Micro-Engine: service-msrpc
Total Signatures: 22
Enabled: 22
Retired: 22
```

Additional References

The following sections provide references related to the Cisco IOS IPS 5.0 Enhancements feature.

Related Documents

Related Topic	Document Title
IPS and firewall	<i>Cisco IOS Security Configuration Guide</i> , Release 12.4
IPS and firewall commands	<i>Cisco IOS Security Command Reference</i> , Release 12.4T
Loading images and file systems	The chapter “Loading and Managing System Images” in the <i>Cisco IOS Configuration Fundamentals Configuration Guide</i> , Release 12.4

Standards

Standard	Title
No new or modified standards are supported by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and technical documentation. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **alert-severity**
- **category**
- **copy idconf**
- **enabled (IPS)**
- **engine (IPS)**
- **event-action**
- **fidelity-rating**
- **ip ips auto-update**
- **ip ips config location**
- **ip ips event-action-rules**
- **ip ips signature-category**
- **ip ips signature-definition**
- **occur-at (ips-auto-update)**
- **retired (IPS)**
- **show ip ips auto-update**
- **signature**
- **status**
- **target-value**
- **url (ips-auto-update)**
- **username (ips-autoupdate)**

Feature Information for Cisco IOS 5.x Format Signatures with Cisco IOS IPS

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Cisco IOS 5.x Format Signatures with Cisco IOS IPS

Feature Name	Releases	Feature Information
Cisco IOS IPS 5.x Signature Format and Usability Enhancements	12.4(11)T	This feature introduces support for Cisco IOS Intrusion Prevention System (IPS) version 5.0, which is a version-based signature definition XML format. Cisco IOS IPS 4.x format signatures are replaced by the 5.x format signatures that are used by all other Cisco IPS devices.

service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Cisco IOS IPS Support for Microsoft Engines

First Published: June 28, 2007

Last Updated: June 28, 2007

The Cisco IOS IPS Support for Microsoft Engines feature extends Cisco IOS Intrusion Prevention Systems (IPS) to support Microsoft RPC (Remote Procedure Call) and Microsoft SMB (Server Message Block) protocols. IPS signatures can now scan for, detect, and take proper action against vulnerabilities in MSRPC and SMB protocols.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Cisco IOS IPS Support for Microsoft Engines](#)” section on page 7.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Information About Cisco IOS IPS Support for Microsoft Engines, page 2](#)
- [How to Use Cisco IOS IPS, page 2](#)
- [Configuration Examples for Cisco IOS IPS, page 2](#)
- [Additional References, page 4](#)
- [Command Reference, page 5](#)
- [Feature Information for Cisco IOS IPS Support for Microsoft Engines, page 7](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Information About Cisco IOS IPS Support for Microsoft Engines

Before using IPS, you should understand the following concept:

- [Cisco IOS IPS Overview, page 2](#)

Cisco IOS IPS Overview

The Cisco IOS IPS acts as an in-line intrusion prevention sensor, watching packets and sessions as they flow through the router and scanning each packet to match any of the Cisco IOS IPS signatures. When it detects suspicious activity, it responds before network security can be compromised and logs the event through Cisco IOS syslog messages or Security Device Event Exchange (SDEE). The network administrator can configure Cisco IOS IPS to choose the appropriate response to various threats. The Signature Event Action Processor (SEAP) can dynamically control actions that are to be taken by a signature event on the basis of parameters such as fidelity, severity, or target value rating. These parameters have default values but can also be configured via CLI. When packets in a session match a signature, Cisco IOS IPS can take any of the following actions, as appropriate:

- Send an alarm to a syslog server or a centralized management interface
- Drop the packet
- Reset the connection
- Deny traffic from the source IP address of the attacker for a specified amount of time
- Deny traffic on the connection for which the signature was seen for a specified amount of time

Cisco developed its Cisco IOS software-based intrusion-prevention capabilities and Cisco IOS Firewall with flexibility in mind, so that individual signatures could be disabled in case of false positives. Generally, it is preferable to enable both the firewall and Cisco IOS IPS to support network security policies. However, each of these features may be enabled independently and on different router interfaces.

How to Use Cisco IOS IPS

The addition of the MSRPC and MSB protocol support does not change the way in which Cisco IOS IPS is defined and enabled in your network. For information on how to enable IPS on your network via command-line interface (CLI), see the section “[How to Use Cisco IOS 5.x Format Signatures with Cisco IOS IPS](#)” within the document *Cisco IOS IPS 5.x Signature Format Support and Usability Enhancements*.

Configuration Examples for Cisco IOS IPS

This section contains the following example:

- [show ip ips signature Output to Verify MS Engines:Example, page 3](#)

show ip ips signature Output to Verify MS Engines:Example

The following sample output from the **show ip ips signature** command displays output for the service-msrpc and service-smb-advanced signatures:

```
Signature Micro-Engine: service-msrpc: Total Signatures 21
service-msrpc enabled signatures: 21
service-msrpc compiled signatures: 21
SigID:SubID En Cmp Action Sev Trait EC AI GST SI SM SW SFR Rel
-----
3330:0 Y Y A HIGH 0 1 0 0 0 FA N 100 S148
3332:0 Y Y A HIGH 0 35 0 0 0 FA N 100 S148
3337:0 Y Y A HIGH 0 8 2 0 0 FA N 100 S85
3331:2 Y Y A HIGH 0 1 0 0 0 FA N 90 S215
3327:12 Y Y A HIGH 0 1 0 0 0 FA N 85 S214
3328:3 Y Y A MED 0 1 0 0 0 FA N 85 S170
3328:1 Y Y A MED 0 1 0 0 0 FA N 85 S148
3327:8 Y Y A INFO 0 1 0 0 0 FA N 85 S214
3334:6 Y Y A HIGH 0 1 0 0 0 FA N 80 S215
3327:0 Y Y A HIGH 0 1 0 0 0 FA N 80 S165
6232:0 Y Y A HIGH 0 1 0 0 0 FA N 75 S209
3327:4 Y Y A HIGH 0 1 0 0 0 FA N 75 S188
3334:5 Y Y A HIGH 0 2 2 0 0 FA N 75 S179
3338:2 Y Y A HIGH 0 40 3 0 0 FA N 75 S175
3338:3 Y Y A HIGH 0 1 0 0 0 FA N 75 S175
6130:0 Y Y A HIGH 0 1 0 0 0 FA N 75 S167
6130:6 Y Y A INFO 0 1 0 0 0 FA N 75 S192
5567:1 Y Y A INFO 0 1 0 0 0 FA N 55 S187
5567:2 Y Y A INFO 0 1 0 0 0 FA N 55 S187
5567:3 Y Y A INFO 0 1 0 0 0 FA N 55 S187
5567:4 Y Y A INFO 0 1 0 0 0 FA N 55 S187

Signature Micro-Engine: service-smb-advanced: Total Signatures 31
service-smb-advanced enabled signatures: 31
service-smb-advanced compiled signatures: 31
SigID:SubID En Cmp Action Sev Trait EC AI GST SI SM SW SFR Rel
-----
5593:0 Y Y A HIGH 0 1 0 0 0 FA N 100 S262
5592:0 Y Y A HIGH 0 1 0 0 0 FA N 100 S262
5582:0 Y Y A HIGH 0 1 0 0 0 FA N 100 S262
5599:0 Y Y A HIGH 0 1 0 0 0 FA N 100 S262
5595:0 Y Y A MED 0 1 0 0 0 FA N 100 S262
5579:0 Y Y A INFO 0 1 0 0 0 FA N 100 S264
5581:0 Y Y A INFO 0 1 0 0 0 FA N 100 S264
5580:0 Y Y A INFO 0 1 0 0 0 FA N 100 S264
5584:0 Y Y A INFO 0 1 0 0 0 FA N 100 S262
5576:0 Y Y A INFO 0 1 0 0 0 FA N 100 S262
5577:0 Y Y A INFO 0 1 0 0 0 FA N 100 S262
5583:0 Y Y A INFO 0 1 0 0 0 FA N 100 S262
5591:0 Y Y A INFO 0 1 0 0 0 FA N 100 S262
5590:0 Y Y A INFO 0 1 0 0 0 FA N 100 S262
5598:0 Y Y A HIGH 0 1 0 0 0 FA N 85 S264
5588:0 Y Y A HIGH 0 1 0 0 0 FA N 85 S262
5586:0 Y Y A HIGH 0 1 0 0 0 FA N 85 S262
5585:0 Y Y A MED 0 1 0 0 0 FA N 85 S264
5579:1 Y Y A MED 0 1 0 0 0 FA N 85 S264
5602:0 Y Y A MED 0 1 0 0 0 FA N 85 S262
5589:0 Y Y A LOW 0 1 0 0 0 FA N 85 S262
5578:0 Y Y A INFO 0 1 0 0 0 FA N 85 S264
5605:0 Y Y A INFO 0 1 0 0 0 FA N 85 S262
5600:0 Y Y A HIGH 0 1 0 0 0 FA N 75 S262
5597:0 Y Y A HIGH 0 50 0 0 0 FA N 75 S262
5594:0 Y Y A HIGH 0 1 0 0 0 FA N 75 S262
```

```
5587:0 Y Y A HIGH 0 1 0 0 0 FA N 75 S262
5603:0 Y Y A MED 0 1 0 0 0 FA N 75 S262
5591:1 Y Y A INFO 0 1 0 0 0 FA N 75 S262
5575:0 Y Y A INFO 0 1 0 0 0 FA N 75 S262
5590:1 Y Y A INFO 0 1 0 0 0 FA N 75 S262
```

Additional References

The following sections provide references related to the Cisco IOS IPS Support for Microsoft Engines feature.

Related Documents

Related Topic	Document Title
Cisco IOS IPS configuration tasks and commands	<i>Cisco IOS IPS 5.x Signature Format Support and Usability Enhancements</i> , Cisco IOS Release 12.4(11)T feature module

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug ip ips**

Feature Information for Cisco IOS IPS Support for Microsoft Engines

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Cisco IOS IPS Support for Microsoft Engines

Feature Name	Releases	Feature Information
Cisco IOS IPS Support for Microsoft Engines	12.4(15)T	The Cisco IOS IPS Support for Microsoft Engines feature extends Cisco IPS to support MSRPC and SMB protocols.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Network Admission Control



Network Admission Control

First Published: May 27, 2004

Last Updated: July 19, 2007

The Network Admission Control feature addresses the increased threat and impact of worms and viruses to networked businesses. This feature is part of the Cisco Self-Defending Network Initiative that helps customers identify, prevent, and adapt to security threats.

In its initial phase, the Cisco Network Admission Control (NAC) functionality enables Cisco routers to enforce access privileges when an endpoint attempts to connect to a network. This access decision can be on the basis of information about the endpoint device, such as its current antivirus state. The antivirus state includes information such as version of antivirus software, virus definitions, and version of scan engine.

Network admission control systems allow noncompliant devices to be denied access, placed in a quarantined area, or given restricted access to computing resources, thus keeping insecure nodes from infecting the network.

The key component of the Cisco Network Admission Control program is the Cisco Trust Agent, which resides on an endpoint system and communicates with Cisco routers on the network. The Cisco Trust Agent collects security state information, such as what antivirus software is being used, and communicates this information to Cisco routers. The information is then relayed to a Cisco Secure Access Control Server (ACS) where access control decisions are made. The ACS directs the Cisco router to perform enforcement against the endpoint.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Network Admission Control](#)” section on page 76.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Contents

- [Prerequisites for Network Admission Control, page 2](#)
- [Restrictions for Network Admission Control, page 2](#)
- [Information About Network Admission Control, page 2](#)
- [How to Configure Network Admission Control, page 7](#)
- [Configuration Examples for Network Admission Control, page 24](#)
- [Additional References, page 27](#)
- [Command Reference, page 29](#)
- [Feature Information for Network Admission Control, page 76](#)
- [Glossary, page 33](#)

Prerequisites for Network Admission Control

- You must have a Cisco IOS router that is running Cisco IOS software, Release 12.3(8)T or later.
- You must have Cisco Trust Agent installed on the endpoint devices (for example, on PCs and laptops).
- You must have a Cisco Secure ACS for authentication, authorization, and accounting (AAA).
- You must be familiar with configuring access control lists (ACLs).
- You should be familiar with configuring AAA.

Restrictions for Network Admission Control

- This feature is available only on Cisco IOS firewall feature sets.

Information About Network Admission Control

Before configuring the Network Admission Control feature, you should understand the following concepts:

- [Virus Infections and Their Effect on Networks, page 3](#)
- [How Network Admission Control Works, page 3](#)
- [Network Access Device, page 3](#)
- [Cisco Trust Agent, page 4](#)
- [Cisco Secure ACS, page 4](#)
- [Remediation, page 5](#)
- [Network Admission Control and Authentication Proxy, page 5](#)
- [NAC MIB, page 5](#)

Virus Infections and Their Effect on Networks

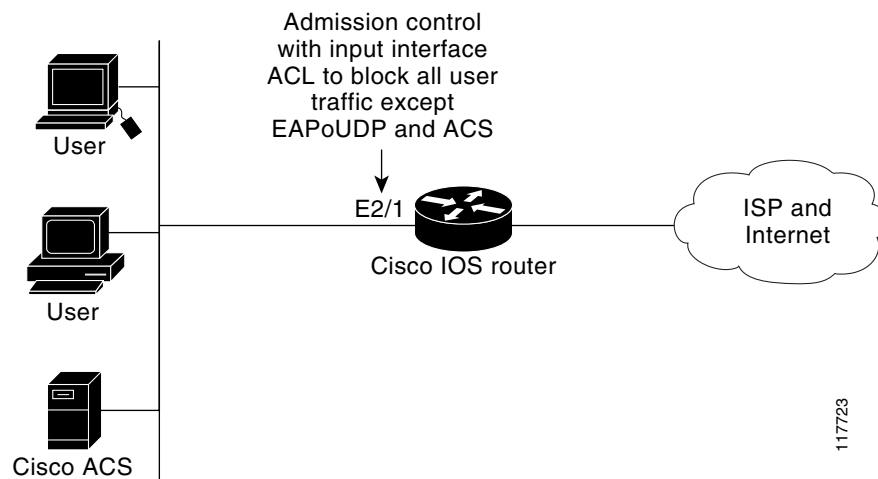
Virus infections are the single largest cause of serious security breaches for networks and often result in huge financial losses. Sources of virus infections are insecure endpoints (for example, PCs, laptops, and servers). Although the endpoints may have antivirus software installed, the software is often disabled. Even if the software is enabled, the endpoints may not have the latest virus definitions and scan engines. A larger security risk is from devices that do not have any antivirus software installed. Although antivirus vendors today are making it more difficult to disable the antivirus software, they are not addressing the risk of outdated virus definitions and scan engines.

How Network Admission Control Works

Endpoint systems, or clients, are normally hosts on the network, such as PCs, laptops, workstations, and servers. The endpoint systems are a potential source of virus infections, and their antivirus states have to be validated before they are granted network access. When an endpoint attempts an IP connection to a network through an upstream Cisco network access device (typically a Cisco IOS router), the router challenges the endpoint for its antivirus state. The endpoint systems run a client called Cisco Trust Agent, which collects antivirus state information from the end device and transports the information to the Cisco network access device. This information is then communicated to a Cisco Secure ACS where the antivirus state of the endpoint is validated and access control decisions are made and returned to Cisco network access devices. The network devices either permit, deny, or quarantine the end device. The Cisco Secure ACS may in turn use back-end antivirus vendor-specific servers for evaluating the antivirus state of the endpoint.

Figure 1 illustrates how Cisco Network Admission Control works.

Figure 1 Cisco IOS Network Admission Control System



Network Access Device

A network access device (NAD) is typically a Cisco IOS router (a Layer 3 Extensible Authentication Protocol over User Datagram Protocol [EAPoUDP] access point) that provides connectivity to external networks, such as the Internet or remote enterprise networks. Cisco Network Admission Control

functionality may have an Intercept ACL, which determines connections that are intercepted for network admission. Connections from endpoints that match the access list are intercepted by Network Admission Control and are challenged for their antivirus states over a Layer 3 association before they are granted network access.

Cisco Trust Agent

Cisco Trust Agent is a specialized software that runs on endpoint systems. Cisco Trust Agent responds to challenges from the router about the antivirus state of an endpoint system. If an endpoint system is not running the Cisco Trust Agent, the network access device (router) classifies the endpoint system as “clientless.” The network access device uses the EOU clientless username and EOU clientless password that are configured on the network access device as the credentials of the endpoint system for validation with Cisco Secure ACS. The policy attributes that are associated with this username are enforced against the endpoint system.

Cisco Secure ACS

Cisco Secure ACS provides authentication, authorization, and accounting services for network admission control using industry-standard RADIUS authentication protocol. Cisco Secure ACS returns access control decisions to the network access device on the basis of the antivirus credentials of the endpoint system.

Using RADIUS cisco_av_pair vendor-specific attributes (VSAs), you can set the following attribute-value pairs (AV pairs) on the Cisco Secure ACS. These AV pairs will be sent to the network access device along with other access-control attributes.

- **url-redirect**—Enables the AAA client to intercept an HTTP request and redirect it to a new URL. This redirection is especially useful if the result of posture validation indicates that the network access control endpoint requires an update or patch that you have made available on a remediation web server. For example, a user can be redirected to a remediation web server to download and apply a new virus Directory Administration Tool (DAT) file or an operating system patch. (See the following example.)

```
url-redirect=http://10.1.1.1
```

- **posture-token**—Enables Cisco Secure ACS to send a text version of a system posture token (SPT) that is derived by posture validation. The SPT is always sent in numeric format, and using the posture-token AV pair makes it easier to view the result of a posture validation request on the AAA client. (See the following example.)

```
posture-token=Healthy
```

Valid SPTs, in order of best to worst, are as follows:

- Healthy
 - Checkup
 - Quarantine
 - Infected
 - Unknown
- **status-query-timeout**—Overrides the status-query default value of the AAA client with the value you specify, in seconds. (See the following example.)

```
status-query-timeout=150
```

For more information about AV pairs that are supported by Cisco IOS software, see the documentation for the releases of Cisco IOS software that are implemented on your AAA clients.

Remediation

Network Admission Control supports HTTP redirection that redirects any HTTP request from the endpoint device to a specified redirect address. This support mechanism redirects all HTTP requests from a source to a specified web page (URL) to which the latest antivirus files can be downloaded. For the HTTP redirection to work, you have to set the value of the “url-redirect” VSA on the ACS and, correspondingly, associate an access control entry in the downloadable ACL that permits the access of the endpoint system to the redirect URL address. After the value of the url-redirect VSA has been set and the access control entry has been associated, any HTTP request that matches the IP admission Intercept ACL will be redirected to the specified redirect URL address.

Network Admission Control and Authentication Proxy

It is possible that network admission control and authentication proxy can be configured for the same set of hosts on a given interface. In each case, the Intercept ACL should be the same for IP admission EAPoUDP and authentication proxy. IP admission proxy with proxy authentication should be configured first, followed by IP admission control.

NAC MIB

The NAC MIB feature adds Simple Network Management Protocol (SNMP) support for the NAC subsystem. Using SNMP commands (get and set operations), an administrator can monitor and control NAC sessions on the network access device (NAD).

For more information about SNMP get and set operations, see the subsection “[Related Documents](#)” in the section “[Additional References](#).”

Correlation Between SNMP Get and Set Operations and the Cisco CLI

Most of the objects in the object tables in the NAC MIB (CISCO-NAC-NAD-MIB.my) describe various EAPoUDP and session parameters that are applicable to the setup of a NAD. These properties can be viewed and modified by performing various SNMP get and set operations. Many of the values of the table objects can also be viewed or modified by configuring corresponding command-line interface (CLI) commands on a router. For example, you can perform an SNMP get operation on the `cnnEOUGlobalObjectsGroup` table or you can configure the **show eou** command on a router. The parameter information obtained from the SNMP get operation is the same as the output from the **show eou** command. Similarly, performing an SNMP get operation on the table `cnnEouIfConfigTable` provides interface-specific parameters that can also be viewed in output from the **show eou** command.

SNMP set operations are allowed for table objects that have corresponding CLI commands, which can be used to modify table object values. For example, to change the value range for the `cnnEouHostValidateAction` object in the `cnnEouHostValidateAction` MIB table to 2, you can either perform the SNMP set operation or configure the **eou initialize all** command on a router.

For examples of NAC MIB output, see the subsection “[NAC MIB Output: Examples](#)” in the section “[Configuration Examples for Network Admission Control](#).”

Initializing and Revalidating Sessions

NAC allows administrators to initialize and revalidate sessions using the following CLI commands:

- **euo initialize all**
- **euo initialize authentication clientless**
- **euo initialize authentication eap**
- **euo initialize authentication static**
- **euo initialize ip** {*ip-address*}
- **euo initialize mac** {*mac-address*}
- **euo initialize posturetoken** {*string*}
- **euo revalidate all**
- **euo revalidate authentication clientless**
- **euo revalidate authentication eap**
- **euo revalidate authentication static**
- **euo revalidate ip** {*ip-address*}
- **euo revalidate mac** {*mac-address*}
- **euo revalidate posturetoken** {*string*}

The initialization and revalidation actions can also be accomplished by performing SNMP set operations on the objects of the `cnnEuoHostValidateAction` table. For more information about initializing and revalidating sessions, see the section [“CLI Commands That Correlate to `cnnEuoHostValidateAction` Table Objects.”](#)

For examples of CLI commands that correlate to changes that can be made to `cnnEuoHostValidateAction` table objects, see the subsection [“NAC MIB Output: Examples”](#) in the section [“Configuration Examples for Network Admission Control.”](#)

Session-Specific Information

The NAC MIB provides a way to view session-specific details using the `cnnEuoHostQueryTable` and `cnnEuoHostResultTable`. The `cnnEuoHostQueryTable` is used to build the query. The query is the same format as the **show euo ip** {*ip-address*} command (that is, the IP address would be shown as in the **show euo ip** command—for example, 10.1.1.1). Administrators must use the SNMP set operation on the objects of the `cnnEuoHostQueryTable` to create the query. The results of the query are stored as a row in the `cnnEuoHostResultTable`. For more information about viewing session-specific details, see the section [“Viewing MIB Query Results.”](#)

Using show Commands to View MIB Object Information

The CLI commands **show euo**, **show euo all**, **show euo authentication**, **show euo initialize**, **show euo ip**, **show euo mac**, **show euo posturetoken**, **show euo revalidate**, and **show ip device tracking all** provide the same output information as that in the CISCO-NAC-NAD-MIB tables using SNMP get operations.

For examples of **show** command output information that can also be viewed in MIB object tables, see the subsection [“NAC MIB Output: Examples”](#) in the section [“Configuration Examples for Network Admission Control.”](#)

How to Configure Network Admission Control

This section contains the following procedures:

- [Configuring the ACL and Admission Control, page 7](#) (required)
- [Configuring Global EAPoUDP Values, page 10](#) (optional)
- [Configuring an Interface-Specific EAPoUDP Association, page 11](#) (optional)
- [Configuring AAA for EAPoUDP, page 12](#) (optional)
- [Configuring the Identity Profile and Policy, page 13](#) (required)
- [Clearing EAPoUDP Sessions That Are Associated with an Interface, page 16](#) (optional)
- [Verifying Network Admission Control, page 16](#) (optional)
- [Troubleshooting Network Admission Control, page 17](#) (optional)
- [Monitoring and Controlling NAC with the CISCO-NAC-NAD-MIB, page 18](#) (optional)

Configuring the ACL and Admission Control

Network admission control is applied in the inbound direction at any interface. Applying network admission control inbound at an interface causes network admission control to intercept the initial IP connections of the intercept end system through the router.

[Figure 1](#) shows that IP admission control is applied at the LAN interface. All network devices must be validated for their antivirus states upon their initial IP connections through the router. Until then, all traffic from endpoint systems (except for EAPoUDP and Cisco Secure ACS traffic) is blocked at the interface.

The endpoint system is then challenged for its antivirus state over an EAPoUDP association. The endpoint system gains access to the network if it complies with the network admission control policy as evaluated by the Cisco Secure ACS. If the endpoint system does not comply, the device is either denied access or quarantined.

To configure an intercept ACL, perform the DETAILED STEPS below.

In this configuration, an intercept ACL is defined as “101,” and the Intercept ACL is associated with the IP admission control rule “greentree.” Any IP traffic that is destined to the 192.50.0.0 network will be subjected to validation. In addition, beginning with Step 5, an intercept ACL is applied inbound to the interface that is associated with network admission control. This ACL typically blocks access to endpoint systems until they are validated. This ACL is referred to as the default access list.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**permit** | **deny**} *protocol source destination*
4. **ip admission name** *admission-name* [**capouudp** | **proxy** {**ftp** | **http** | **telnet**}] [**list** {*acl* | *acl-name*}]
5. **interface** *type slot/port*
6. **ip address** *ip-address mask*
7. **ip admission** *admission-name*
8. **exit**

9. **access-list** *access-list-number* {**permit** | **deny**} *protocol source destination*
10. **ip access-group** {*access-list-number* | *access-list-name*} **in**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	access-list <i>access-list-number</i> { permit deny } <i>protocol source destination</i> Example: Router (config)# access-list 101 permit ip any 192.50.0.0 0.0.0.255	Defines a numbered access list.
Step 4	ip admission name <i>admission-name</i> [eapoudp proxy {ftp http telnet}] [list { <i>acl</i> <i>acl-name</i> }] Example: Router (config)# ip admission name greentree eapoudp list 101	Creates IP network admission control rules. The rules define how you apply admission control. The rules are as follows: <ul style="list-style-type: none"> eapoudp—Specifies IP network admission control using EAPoUDP. proxy ftp—Specifies FTP to trigger authentication proxy. proxy http—Specifies HTTP to trigger authentication proxy. proxy telnet—Specifies Telnet to trigger authentication proxy. <p>You can associate the named rule with an ACL, providing control over which hosts use the admission control feature. If no standard access list is defined, the named admission rule intercepts IP traffic from all hosts whose connection-initiating packets are received at the configured interface.</p> <p>The list option allows you to apply a standard, extended (1 through 199) or named access list to a named admission control rule. IP connections that are initiated by hosts in the access list are intercepted by the admission control feature.</p>
Step 5	interface <i>type slot/port</i> Example: Router (config)# interface ethernet 2/1	Defines an interface and enters interface configuration mode.
Step 6	ip address <i>ip-address mask</i> Example: Router (config-if)# ip address 192.0.0.1 255.255.255.0	Sets a primary or secondary IP address for an interface.

	Command or Action	Purpose
Step 7	ip admission <i>admission-name</i> Example: Router (config-if)# ip admission greentree	Applies the named admission control rule at the interface.
Step 8	exit Example: Router (config-if)# exit	Exits interface configuration mode.
Step 9	access-list <i>access-list-number</i> { permit deny } <i>protocol source destination</i> Example: Router (config)# access-list 105 permit udp any any or Router (config)# access-list 105 permit ip host 192.168.0.2 any or Router (config)# access-list 105 deny ip any any	Defines a numbered access list. Note In the first two examples (under “Command or Action”), ACL “105” denies all IP traffic except UDP and access to 192.168.0.2 (Cisco Secure ACS). Note In the third example (under “Command or Action,” ACL “105” will be applied on the interface that is configured for network admission control, and access to endpoint systems (except for EAPoUDP traffic and access to Cisco Secure ACS [192.168.0.2 in the example] is blocked until their antivirus states are validated. This ACL (“105”) is referred to as “Interface ACL.”
Step 10	ip access-group { <i>access-list-number</i> <i>access-list-name</i> } in Example: Router (config)# ip access-group 105 in	Controls access to an interface.

Configuring Global EAPoUDP Values

To configure global EAPoUDP values, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **eou {allow | clientless | default | initialize | logging | max-retry | port | rate-limit | revalidate | timeout}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	eou {allow clientless default initialize logging max-retry port rate-limit revalidate timeout} Example: Router (config)# eou initialize	Specifies EAPoUDP values. <ul style="list-style-type: none"> For a breakout of available keywords and arguments for the eou command, see the following commands: <ul style="list-style-type: none"> eou allow eou clientless eou default eou initialize eou logging eou max-retry eou port eou rate-limit eou revalidate eou timeout

Configuring an Interface-Specific EAPoUDP Association

To configure an EAPoUDP association that can be changed or customized for a specific interface that is associated with network admission control, perform the following steps.

SUMMARY STEPS

- enable**
- configure terminal**
- interface** *type slot/port*
- eou** [**default** | **max-retry** | **revalidate** | **timeout**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type slot/port</i> Example: Router (config)# interface ethernet 2/1	Defines an interface and enters interface configuration mode.
Step 4	eou [default max-retry revalidate timeout] Example: Router (config-if)# eou revalidate	Enables an EAPoUDP association for a specific interface. <ul style="list-style-type: none"> For a breakout of available keywords and arguments for the eou command, see the following commands: <ul style="list-style-type: none"> eou default eou max-retry eou revalidate eou timeout

Configuring AAA for EAPoUDP

To set up AAA for EAPoUDP, perform the following steps.

SUMMARY STEPS

- enable**
- configure terminal**
- aaa new-model**
- aaa authentication eou default enable group radius**
- aaa authorization network default group radius**
- radius-server host** {*hostname* | *ip-address*}
- radius-server key** {**0** *string* | **7** *string* | *string*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Router (config)# aaa new-model	Enables the AAA access control model.
Step 4	aaa authentication eou default enable group radius Example: Router (config)# aaa authentication eou default enable group radius	Sets authentication lists for an EAPoUDP association.
Step 5	aaa authorization network default group radius Example: Router (config)# aaa authorization network default group radius	Uses the list of all RADIUS servers for authentication.
Step 6	radius-server host {hostname ip-address} Example: Router (config)# radius-server host 192.0.0.40	Specifies a RADIUS server host.
Step 7	radius-server key {0 string 7 string string} Example: Router (config)# radius-server key cisco	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

Configuring the Identity Profile and Policy

Identity is a common infrastructure that is used to specify local profile and policy configurations. The identity profile allows you to statically authorize or validate individual devices on the basis of IP address, MAC address, or device type. Each statically authenticated device can be associated with a local policy that specifies the network access control attributes. Hosts are added to this “exception list” using the **identity profile** command, and corresponding policies are associated with these hosts using the **identity policy** command.

If the client is part of the identity (that is, the client is on the exception list), the status of the client is set on the basis of the identity configuration. The client does not have to go through the posture validation process, and the associated identity policy is applied for the client.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **identity profile eapoudp**
4. **device {authorize {ip address *ip-address* {policy *policy-name*} | mac-address *mac-address* | type {cisco | ip | phone}} | not-authorize}**
5. **exit**
6. **identity policy *policy-name* [access-group *group-name* | description *line-of-description* | redirect *url* | template [virtual-template *interface-name*]]**
7. **access-group *group-name***
8. **exit**
9. **exit**
10. **ip access-list extended *access-list-name***
11. **{permit | deny} *source source-wildcard destination destination-wildcard***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	identity profile eapoudp Example: Router (config)# identity profile eapoudp	Creates an identity profile and enters identity profile configuration mode.
Step 4	device {authorize {ip address ip-address {policy policy-name} mac-address mac-address type {cisco ip phone}} not-authorize} Example: Router (config-identity-prof)# device authorize ip address 10.10.142.25 policy bluemoon	Statically authorizes an IP device and applies an associated policy to the device.
Step 5	exit Example: Router (config-identity-prof)# exit	Exits identity profile configuration mode.
Step 6	identity policy policy-name [access-group group-name description line-of-description redirect url template [virtual-template interface-name]] Example: Router (config-identity-prof)# identity policy bluemoon	Creates an identity policy and enters identity policy configuration mode.
Step 7	access-group group-name Example: Router (config-identity-policy)# access-group exempt-acl	Defines network access attributes for the identity policy.
Step 8	exit Example: Router (config-identity-policy)# exit	Exits identity policy configuration mode.
Step 9	exit Example: Router (config-identity-prof)# exit	Exits identity profile configuration mode.

	Command or Action	Purpose
Step 10	ip access-list extended <i>access-list-name</i> Example: Router (config)# ip access-list extended exempt-acl	Defines access control for statically authenticated devices (and enters network access control configuration mode).
Step 11	{permit deny} <i>source source-wildcard destination destination-wildcard</i> Example: Router (config-ext-nacl)# permit ip any 192.50.0.0. 0.0.0.255	Set conditions to allow a packet to pass a named IP access list.

Clearing EAPoUDP Sessions That Are Associated with an Interface

To clear EAPoUDP sessions that are associated with a particular interface or that are on the NAD, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **clear eou all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	clear eou all Example: Router# clear eou all	Clears all EAPoUDP sessions on the NAD.

Verifying Network Admission Control

To verify EAP and EAPoUDP messages or sessions, perform the following steps. The **show** commands may be used in any order or independent of the other **show** command.

SUMMARY STEPS

1. **enable**
2. **show eou all**
3. **show ip admission eapoudp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	show eou all Example: Router# show eou all	Displays information about EAPoUDP sessions on the network access device.
Step 3	show ip admission eapoudp Example: Router# show ip admission eapoudp	Displays the network admission control configuration or network admission cache entries.

Troubleshooting Network Admission Control

The following commands may be used to display information about EAP and EAPoUDP messages or sessions. The **debug** commands may be used in any order or independent of the other **debug** commands.

SUMMARY STEPS

1. **enable**
2. **debug eap {all | errors | packets | sm}**
3. **debug eou {all | eap | errors | packets | sm}**
4. **debug ip admission eapoudp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	debug eap {all errors packets sm} Example: Router# debug eap all	Displays information about EAP messages.
Step 3	debug eou {all eap errors packets sm} Example: Router# debug eou all	Displays information about EAPoUDP messages.
Step 4	debug ip admission eapoudp Example: Router# debug ip admission eapoudp	Displays information about IP admission events.

Monitoring and Controlling NAC with the CISCO-NAC-NAD-MIB

This section includes the following tasks:

- [CLI Commands That Correlate to cnnEouHostValidateAction Table Objects, page 19](#)
- [CLI Commands That Correlate to cnnEouIfConfigTable Objects, page 19](#)
- [CLI Commands That Correlate to cnnEouHostValidateAction Table Objects, page 19](#)
- [Creating MIB Query Tables, page 20](#)
- [Viewing MIB Query Results, page 23](#)

CLI Commands That Correlate to cnnEouGlobalObjectsGroup Table Objects

An SNMP get or set operation can be performed to obtain or change information about value ranges for objects in the cnnEouGlobalObjectsGroup table. The same information can be viewed in output from the **show eou** command. [Table 1](#) displays examples of some global configuration objects and the SNMP get and set operations required to obtain or change their values.

For an example of **show eou** command output, see the section “[show eou](#)” section on [page 26](#).

Table 1 *Obtaining and Changing Global Configuration Values Using SNMP Get and Set Operations*

Global Configuration Objects	SNMP Operation
EAPoUDP version	Performs a get operation on the cnnEouVersion object. (The object value will be “1.”)

Table 1 *Obtaining and Changing Global Configuration Values Using SNMP Get and Set Operations*

Global Configuration Objects	SNMP Operation
EAPoUDP port	Performs a get operation on the <code>cnnEouPort</code> object.
Enabling logging (enable EOU logging)	Sets the <code>cnnEouLoggingEnable</code> object. (The object value will be “true.”)

CLI Commands That Correlate to `cnnEouIfConfigTable` Objects

An SNMP get operation is performed to obtain information about value ranges for objects in the `cnnEouIfConfigTable`. The same information can be viewed in output from the **show eou** command. [Table 2](#) displays examples of some interface-specific configuration objects and the SNMP get operations required to obtain their values.

Table 2 *Obtaining Interface-Specific Configuration Values Using SNMP Get Operations*

Interface-Specific Object	SNMP Operation
AAA timeout	Performs a get operation on the <code>cnnEouIfTimeoutAAA</code> object. <ul style="list-style-type: none"> Format: GET <code>cnnEouIfTimeoutAAA.IfIndex</code> You must specify the corresponding index number of the specific interface.
Maximum retries	Performs a get operation on the <code>cnnEouIfMaxRetry</code> object. <ul style="list-style-type: none"> Format: GET <code>cnnEouIfMaxRetry.IfIndex</code>

CLI Commands That Correlate to `cnnEouHostValidateAction` Table Objects

EOU sessions can be initialized or revalidated by the CLI or by using the SNMP set operation on the table `cnnEouHostValidateAction`.

Following are some examples (listed by CLI command) that correlate to MIB objects.

eou initialize all

EOU initialization can be accomplished for all sessions by using the **eou initialize all** command or by using an SNMP set operation on the object `cnnEouHostValidateAction`. This object must be set to the numeric value 2.

eou initialize authentication clientless

EOU initialization can be accomplished for sessions having an authentication type “clientless” using the **eou initialize authentication clientless** command or an SNMP set operation on the object `cnnEouHostValidateAction`. This object must be set to the numeric value 3.

eou initialize ip

EOU initialization can be accomplished for a particular session using the **eou initialize ip** *{ip-address}* command.

To achieve the same result using an SNMP operation, three objects have to be set in the `cnnEouHostValidateAction` MIB table:

- `cnnEouHostValidateAction`—The value range must be set.
- `cnnEouHostValidateIpAddressType`—The IP address type must be set. This value must be set to IPv4 because IPv4 is currently the only address type supported by NAC. (This value is the type of address being set for the `cnnEouHostValidateIPAddr` object.)
- `cnnEouHostValidateIPAddr`—The IP address must be set.



Note The three MIB objects should be set in a single SNMP set operation.

euo initialize posturetoken

All sessions having a particular posturetoken can be initialized using the **euo initialize posturetoken** {*string*} command. The default value range for this command is 8.

To achieve the same result using an SNMP set operation, you must set the following objects:

- `cnnEouHostValidateAction`—Set this value to 8.
- `cnnEouHostValidatePostureTokenStr`—Set the string value.



Note The two MIB objects should be set in a single SNMP set operation.

Creating MIB Query Tables

The MIB table `cnnEouHostQueryTable` is used to create, or build, MIB queries.

MIB Query Correlating to the CLI **show euo all** Command

To build a query that provides the same results as using the **show euo all** command, perform the following SNMP get operation.

The object `cnnEouHostQueryMask` in the table `cnnEouHostQueryTable` indicates the kind of query. The corresponding value of the `cnnEouHostQueryMask` object in output from the **show euo all** command is 8 (the integer value).

SUMMARY STEPS

1. Set the `cnnEouHostQueryStatus` object to `createandgo`.
2. Set the `cnnEouHostQueryMask` object to 8.
3. Set the `cnnEouHostQueryStatus` object to `active` to indicate that query creation is complete.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Set the <code>cnnEouHostQueryStatus</code> object to <code>createandgo</code> .	Creates a query row.
Step 2	Set the <code>cnnEouHostQueryMask</code> object to 8.	Corresponds in value to the show euo all command.
Step 3	Set the <code>cnnEouHostQueryStatus</code> object to <code>active</code> .	Indicates that you have finished building the query.

**Note**

Examples are not shown in the previous table because the format differs depending on the software you are using.

What to Do Next

View the results. See the section “[Viewing MIB Query Results Correlating to the show eou all Command](#).”

Viewing MIB Query Results Correlating to the show eou all Command

After the MIB query has been built and you have indicated that you are finished (with the “active” status), the results can be viewed. A query in the `cnnEouHostQueryTable` is represented by a row. The row number is the Query Index. Similarly, the `cnnEouHostResultTable` is composed of result rows. Each row in the `cnnEouHostResultTable` is uniquely identified by a combination of Query Index and Result Index. The results of the `cnnEouHostQueryTable` index and the `cnnEouHostResultTable` have to be matched. Match one row in the Query table to one of the rows in the Result table. For example, if a query that corresponds to a **show** command results in ten sessions, the Result table has ten rows, each row corresponding to a particular session. The first row in the Result table is R1.1. The second row is R1.2, and so on to R1.10. If another query is created in the Query table, and it results in five sessions, five rows are created in the Result table (R2.1, R2.2, R2.3, R2.4, and R2.5).

[Table 3](#) illustrates how the above Query table sessions are mapped to Result table rows.

Table 3 Query Table-to-Result Table Mapping

Query Table	Result Table Rows
Q1 (10 sessions)	R1.1, R1.2, R1.3, R1.4, R1.5, R1.6, R1.7, R1.8, R1.9, R1.10
Q2 (5 sessions)	R2.1, R2.2, R2.3, R2.4, R2.5

Creating the SNMP Query

To create an SNMP query that provides the same information as output from the **show eou ip {ip-address}** command, perform the following steps.

SUMMARY STEPS

1. Set `cnnEouHostQueryStatus` to `createandgo`.
2. Set `cnnEouHostQueryIpAddrType` to `IPv4` and the IP address (for example, 10.2.3.4).
3. Set `cnnEouHostQueryStatus` to `active`.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Set <code>cnnEouHostQueryStatus</code> to <code>createandgo</code> .	Creates a query row.
Step 2	Set <code>cnnEouHostQueryIpAddrType</code> to <code>IPv4</code> and the IP address (for example, 10.2.3.4).	Sets the address type. <ul style="list-style-type: none"> The only address type currently supported by NAC is IPv4.
Step 3	Set <code>cnnEouHostQueryStatus</code> to <code>active</code> .	Indicates you have finished building the query.



Note

Examples are not shown in the previous table because the format differs depending on the software you are using.

Viewing the Results

To view the results in the `cnnEouHostResultTable`, perform the following steps.

SUMMARY STEPS

1. Perform a get operation on `cnnEouHostQueryRows`.
2. Perform a get operation on the `cnnEouHostResultTable` objects in the format `resultTableObjectName.QueryIndex.ResultIndex`.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Perform a get operation on <code>cnnEouHostQueryRows</code> .	Finds how many rows will be created in a Result table for a particular query. <ul style="list-style-type: none"> If a query row is a negative number, the query is still being processed.
Step 2	Perform a get operation on the <code>cnnEouHostResultTable</code> objects in the format <code>resultTableObjectName.QueryIndex.ResultIndex</code> .	Finds the value of a particular object in a Result table that matches a particular query. <ul style="list-style-type: none"> For multiple rows in the Result table for a single query, the <code>ResultIndex</code> ranges from 1 to the value of <code>cnnEouHostQueryRows</code>.



Note

Examples are not shown in the above table because the format differs depending on the software you are using.

MIB Query Correlating to the `show eou ip` Command

To build a MIB query that provides the same results as the `show eou ip {ip-address}` command, perform the following SNMP get operation.

SUMMARY STEPS

1. Set the `cnnEouHostQueryStatus` object to `createandgo`.
2. Set the `cnnEouHostQueryIpAddrType` object to “IPv4”.
3. Set the `cnnEouHostQueryIpAddr` object to IP address (for example, 10.2.3.4).
4. Set the `cnnEouHostQueryStatus` object to `active`.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Set the <code>cnnEouHostQueryStatus</code> object to <code>createandgo</code> .	Sets the query status.
Step 2	Set the <code>cnnEouHostQueryIpAddrType</code> object to “IPv4”.	Sets the address type. Note The only address type currently supported by NAC is IPv4.
Step 3	Set the <code>cnnEouHostQueryIpAddr</code> object to IP address (for example, 10.2.3.4).	Sets the IP address.
Step 4	Set the <code>cnnEouHostQueryStatus</code> object to <code>active</code> .	Indicates that you have finished building the query.



Note

Examples are not shown in the previous table because the format differs depending on the software you are using.

Viewing MIB Query Results

After the MIB query has been built, the results can be viewed in `cnnEouHostResultTable`. For information about how to review the results, see the subsection “[Viewing MIB Query Results Correlating to the show eou all Command](#)” in the previous section “[Creating MIB Query Tables](#).”

Splitting a Query into Subqueries

If you are doing a MIB query that correlates to the **show eou all** command, there could possibly be as many as 2,000 rows of output. To ensure that you can view all the information in a MIB query, you can split the query into subqueries. For example, for a query having 2,000 rows of output, you could split the query into four subqueries to view the results in a page-by-page format. The first subquery would include rows 1 through 500 (the first 500 sessions); the second subquery would include rows 501 through 1,000; the third subquery would include rows 1,001 through 1,500; and the fourth subquery would include rows 1,501 through 2,000.



Note

The `cnnEouHostQueryTotalHosts` object provides the total number of hosts (number of rows) that match a query criterion. By looking at this number, you can determine how many subqueries are necessary. However, you cannot get the `cnnEouHostQueryTotalHosts` object number until you have built your first query.

Build your query by performing the following steps.

SUMMARY STEPS

1. Set the `cnnEouHostQueryStatus` object to `createandgo`.
2. Set the `cnnEouHostQueryMask` object to 8.
3. Set `cnnEouHostQueryRows` to 500.
4. Set `cnnEouHostQuerySkipNHosts` to 0.
5. Set the `cnnEouHostQueryStatus` object to active.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Set the <code>cnnEouHostQueryStatus</code> object to <code>createandgo</code> .	Sets the query status.
Step 2	Set the <code>cnnEouHostQueryMask</code> object to 8.	Correlates to the default of the show eou all command.
Step 3	Set <code>cnnEouHostQueryRows</code> to 500.	Identifies the maximum number of rows to be built in the result table for this query.
Step 4	Set <code>cnnEouHostQuerySkipNHosts</code> to 0.	Corresponds to the result rows to be created.
Step 5	Set the <code>cnnEouHostQueryStatus</code> object to active.	Indicates that you have finished building the query.



Note

Examples are not shown in the previous table because the format differs depending on the software you are using. The table is on the basis of a query having 2,000 sessions (rows).

What to Do Next

After you have performed the above task, you will have query information for the first 500 hosts (rows). To view query information for the next 500 hosts (rows), you have to perform the same five steps, but you must change the Step 4 (`cnnEouHostQuerySkipNHosts` object) value to 500. This task will result in query information for rows 501 through 1000. In the same way, to obtain query information for the remaining hosts (through 2000), you have to perform the same five steps again but with `cnnEouHostQuerySkipNHosts` object values of 1000 and 1500, respectively.

Configuration Examples for Network Admission Control

This section includes the following example.

- [Network Admission Control: Example, page 24](#)
- [NAC MIB Output: Examples, page 26](#)

Network Admission Control: Example

The following output example shows that IP admission control has been configured on a Cisco IOS router:

```
Router# show running-config
```

Building configuration...

Current configuration: 1240 bytes

```
!  
version 12.3  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname Router  
!  
boot-start-marker  
boot-end-marker  
!  
aaa new-model  
!  
!  
aaa authentication eou default group radius  
aaa session-id common  
ip subnet-zero  
ip cef  
!  
! The following line creates a network admission rule. A list is not specified; therefore,  
! the rule intercepts all traffic on the applied interface.  
ip admission name avrule eapoudp  
!  
eou logging  
!  
!  
interface FastEthernet0/0  
 ip address 10.13.11.106 255.255.255.0  
 duplex auto  
 speed auto  
!  
interface FastEthernet0/1  
 ip address 10.0.0.1 255.255.255.0  
 ip access-group 102 in  
! The following line configures an IP admission control interface.  
 ip admission avrule  
 duplex auto  
 speed auto  
!  
ip http server  
no ip http secure-server  
ip classless  
!  
!  
! The following lines configure an interface access list that allows EAPoUDP traffic  
! and blocks the rest of the traffic until it is validated.  
access-list 102 permit udp any any eq 21862  
access-list 102 deny ip any any  
!  
!  
! The following line configures RADIUS.  
radius-server host 10.13.11.105 auth-port 1645 acct-port 1646 key cisco  
!  
control-plane  
!  
!  
!  
line con 0  
 exec-timeout 0 0  
line aux 0
```

```

line vty 0 4
!
!
end

```

NAC MIB Output: Examples

The following are examples of **show** command output displaying MIB object information.

show eou

The **show eou** command provides output for information that can also be viewed in various CISCO-NAC-NAD-MIB tables. The information that follows the **show eou** command can also be found in the `cnnEouGlobalObjectsGroup` table and the information that follows the **show eou all** command can be found in the `cnnEouIfConfigTable`.

```
Router# show eou
```

```

Global EAPoUDP Configuration
-----
EAPoUDP Version      = 1
EAPoUDP Port         = 0x5566
Clientless Hosts     = Enabled
IP Station ID        = Disabled
Revalidation         = Enabled
Revalidation Period  = 36000 Seconds
ReTransmit Period    = 3 Seconds
StatusQuery Period   = 300 Seconds
Hold Period          = 30 Seconds
AAA Timeout          = 60 Seconds
Max Retries          = 3
EAP Rate Limit       = 20
EAPoUDP Logging      = Enabled
Clientless Host Username = clientless
Clientless Host Password = clientless

```

```
Router# show eou all
```

```

Interface Specific EAPoUDP Configurations
-----
Interface Vlan333
AAA Timeout          = 60 Seconds
Max Retries          = 3
eou initialize interface {interface-name}
eou revalidate interface {interface-name}

```

show ip device tracking all

The **show ip device tracking all** command provides output for information that can also be found in the `cnnIpDeviceTrackingObjectsGroup` MIB table. The following is an example of such **show** command output:

```
Router# show ip device tracking all
```

```

IP Device Tracking = Enabled
Probe Count: 2
Probe Interval: 10

```

Additional References

The following sections provide references related to Network Admission Control.

Related Documents

Related Topic	Document Title
Configuring ACLs	“ Access Control Lists: Overview and Guidelines ” chapter of the “Traffic Filtering and Firewalls” section of the <i>Cisco IOS Security Configuration Guide</i> , Release 12.3.
Authentication, authorization, and accounting	“ Authentication, Authorization, and Accounting ” section of <i>Cisco IOS Security Configuration Guide</i> , Release 12.3.
Interfaces, configuring	Cisco IOS Interface and Hardware Component Configuration Guide, Release 12.3.
SNMP and SNMP get and set operations	<ul style="list-style-type: none"> “Simple Network Management Protocol” section of the <i>Internetworking Technology Handbook</i> “Configuring SNMP Support” section of the <i>Cisco IOS Configuring Fundamentals Configuration Guide</i>, Release 12.4.

Standards

Standards	Title
No new or modified standards are supported by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	—

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **aaa authentication eou default enable group radius**
- **access-group (identity policy)**
- **auth-type**
- **clear eou**
- **clear ip admission cache**
- **debug eap**
- **debug eou**
- **debug ip admission eapoudp**
- **description (identity policy)**
- **description (identity profile)**
- **device (identity profile)**
- **eou allow**
- **eou clientless**
- **eou default**
- **eou initialize**
- **eou logging**
- **eou max-retry**
- **eou port**
- **eou rate-limit**
- **eou revalidate**
- **eou timeout**
- **identity policy**

- **identity profile eapoudp**
- **ip admission**
- **ip admission name**
- **redirect (identity policy)**
- **show eou**
- **show ip admission**
- **show ip device tracking**
- **template (identity policy)**

Feature Information for Network Admission Control

Table 4 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 4 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 4 Feature Information for Network Admission Control

Feature Name	Releases	Feature Information
Network Admission Control	12.3(8)T	<p>The Network Admission Control feature addresses the increased threat and impact of worms and viruses to networked businesses. This feature is part of the Cisco Self-Defending Network Initiative that helps customers identify, prevent, and adapt to security threats.</p> <p>In its initial phase, the Cisco Network Admission Control functionality enables Cisco routers to enforce access privileges when an endpoint attempts to connect to a network.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Prerequisites for Network Admission Control, page 2 • Restrictions for Network Admission Control, page 2 • Information About Network Admission Control, page 2 • How to Configure Network Admission Control, page 7 • Configuration Examples for Network Admission Control, page 24 <p>The following commands were introduced or modified by this feature: aaa authentication eou default enable group radius, access-group (identity policy), auth-type, clear eou, clear ip admission cache, debug eap, debug eou, debug ip admission eapoudp, description (identity policy), description (identity profile), device (identity profile), eou allow, eou clientless, eou default, eou initialize, eou logging, eou max-retry, eou port, eou rate-limit, eou revalidate, eou timeout, identity policy, identity profile eapoudp, ip admission, ip admission name, redirect (identity policy), show eou, show ip admission, template (identity policy).</p>

Table 4 **Feature Information for Network Admission Control (continued)**

Feature Name	Releases	Feature Information
NAC MIB	12.4(15)T	<p>Support was added for the CISCO-NAC-NAD-MIB. This MIB module is used to monitor and configure the NAD on the Cisco NAC system.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none">• “NAC MIB” section on page 5• “Monitoring and Controlling NAC with the CISCO-NAC-NAD-MIB” section on page 18 <p>The following commands were introduced or modified by this feature: show ip device tracking.</p>

Glossary

default access policy—Set of ACLs that are applied to a client device until its credentials are validated by the AAA server.

EAPoUDP—Extensible Authentication Protocol over User Datagram Protocol. EAP is a framework that supports multiple, optional authentication mechanisms for PPP, including clear-text passwords, challenge-response, and arbitrary dialogue sequences. UDP is a connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, and it requires that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

ip admission rule—Named rule that defines how IP admission control is applied. The IP admission rule is associated with an Intercept ACL and provides control over which hosts can use the IP admission feature. To create an IP admission control rule, use the **ip admission name** command.

posture token—Status that is used to convey the result of the evaluation of posture credentials. The AAA server maps the posture token (its status can be Healthy, Checkup, Quarantine, Infected, or Unknown) to a network access policy (ACL, URL, redirect, or status query timer) for the peer that the client wants to reach.

**Note**

See [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



NAC—Auth Fail Open

First Published: November 17, 2006

Last Updated: November 17, 2006

In network admission control (NAC) deployments, authentication, authorization, and accounting (AAA) servers validate the antivirus status of clients before granting network access. This process is called posture validation. If the AAA server is unreachable, clients will not have access to the network. The NAC—Auth Fail Open feature enables the administrator to apply a policy that allows users to have network access when the AAA server is unreachable. The administrator can configure a global policy that applies to a device, or a rule-based policy that applies to a specific interface.

When the AAA server returns to a reachable status, the posture validation process resumes for clients that are using the NAC—Auth Fail Open policy.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for NAC—Auth Fail Open](#)” section on page 29.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for NAC—Auth Fail Open, page 2](#)
- [Restrictions for NAC—Auth Fail Open, page 2](#)
- [Information About Network Admission Control, page 2](#)
- [How to Configure NAC—Auth Fail Open, page 3](#)
- [Configuration Examples for NAC—Auth Fail Open, page 12](#)
- [Additional References, page 15](#)
- [Command Reference, page 16](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Feature Information for NAC—Auth Fail Open, page 29](#)

Prerequisites for NAC—Auth Fail Open

You can configure this feature in networks using NAC and an AAA server for security. NAC is implemented on Cisco IOS routers running Cisco IOS Release 12.3(8)T or a later release.

Restrictions for NAC—Auth Fail Open

To apply local policies to a device or an interface when the AAA server is unreachable, you must configure the **aaa authorization network default local** command.

Information About Network Admission Control

You should understand the following concepts:

- [Controlling Admission to a Network, page 2](#)
- [Network Admission Control When the AAA Server Is Unreachable, page 2](#)

Controlling Admission to a Network

NAC protects networks from endpoint devices or clients (such as PCs or servers) that are infected with viruses by enforcing access control policies that prevent infected devices from adversely affecting the network. It checks the antivirus condition (called *posture*) of endpoint systems or clients before granting the devices network access. NAC keeps insecure nodes from infecting the network by denying access to noncompliant devices, placing them in a quarantined network segment or giving them restricted access to computing resources.

NAC enables network access devices (NADs) to permit or deny network hosts access to the network based on the state of the antivirus software on the host. This process is called posture validation.

Posture validation consists of the following actions:

- Checking the antivirus condition or credentials of the client.
- Evaluating the security posture credentials from the network client.
- Providing the appropriate network access policy to the NAD based on the system posture.

Network Admission Control When the AAA Server Is Unreachable

Typical deployments of NAC use a AAA server to validate the client posture and to pass policies to the NAD. If the AAA server is not reachable when the posture validation occurs, the typical response is to deny network access. Using NAC—Auth Fail Open, an administrator can configure a default policy that allows the host at least limited network access while the AAA server is unreachable.

This policy offers these two advantages:

- While AAA is unavailable, the host will still have connectivity to the network, although it may be restricted.

- When the AAA server is once again reachable, users can be revalidated, and their policies can be downloaded from the access control server (ACS).

**Note**

When the AAA server is unreachable, the NAC—Auth Fail Open policy is applied only when there is no existing policy associated with the host. Typically, when the AAA server becomes unreachable during revalidation, the policies already in effect for the host are retained.

How to Configure NAC—Auth Fail Open

You can configure NAC—Auth Fail Open policies per interface, or globally for a device. Configuring NAC—Auth Fail Open is optional, and includes the following tasks:

- [Configuring a NAC Rule-Associated Policy Globally for a Device, page 3](#)
- [Applying a NAC Policy to a Specific Interface, page 4](#)
- [Configuring Authentication and Authorization Methods, page 5](#)
- [Configuring RADIUS Server Parameters, page 6](#)
- [Displaying the Status of the Configured AAA Servers, page 10](#)
- [Enabling EOU Logging, page 11](#)

Configuring a NAC Rule-Associated Policy Globally for a Device

This task creates a NAC rule and associates a policy to be applied while the AAA server is unreachable. You can apply a policy globally to all interfaces on a network access device, if you want to provide the same level of network access to all users who access that device.

Prerequisites

An AAA server must be configured and NAC must be implemented on the NAD.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission name** *admission-name* [**eapoudp** [**bypass**] | **proxy** {**ftp** | **http** | **telnet**} | **service-policy type tag** {*service-policy-name*}] [**list** {*acl* | *acl-name*}] [**event**] [**timeout aaa**] [**policy identity** {*identity-policy-name*}]
4. **ip admission** *admission-name* [**event timeout aaa policy identity** *identity-policy-name*]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip admission name <i>admission-name</i> [eapoudp [bypass] proxy { ftp http telnet } service-policy type tag { <i>service-policy-name</i> }] [list { <i>acl</i> <i>acl-name</i> }] [event] [timeout aaa] [policy identity { <i>identity-policy-name</i> }] Example: Router (config)# ip admission name greentree event timeout aaa policy identity aaa-down	(Optional) Configures a rule-specific policy globally for the device. If a rule is configured, it will be applied instead of any other global event timeout policy configured on the device. To remove a rule that was applied globally to the device, use the no form of the command.
Step 4	ip admission <i>admission-name</i> [event timeout aaa policy identity <i>identity-policy-name</i>] Example: Router (config)# ip admission event timeout aaa policy identity AAA_DOWN	(Optional) Configures the specified IP NAC policy globally for the device. To remove IP NAC policy that was applied to the device, use the no form of the command. Note This policy will apply only if no rule-specific policy is configured.
Step 5	end Example: Router (config)# end	Exits the global configuration mode.

Applying a NAC Policy to a Specific Interface

An IP admission rule with NAC—Auth Fail Open policies can be attached to an interface. This task attaches a NAC—Auth Fail Open policy to a rule, and applies the rule to a specified interface on a device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip access-group** {*access-list-number* | *name*} **in**
5. **ip admission** *admission-name*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>interface-id</i> Example: Router (config)# interface fastEthernet 2/1	Enters interface configuration mode.
Step 4	ip access-group { <i>access-list-number</i> <i>name</i> } in Example: Router (config-if)# ip access-group ACL15 in	Controls access to the specified interface.
Step 5	ip admission <i>admission-name</i> Example: Router (config-if)# ip admission AAA_DOWN	Attaches the globally configured IP admission rule to the specified interface(s). To remove the rule on the interface, use the no form of the command.
Step 6	exit Example: Router (config)# exit	Returns to global configuration mode.

Configuring Authentication and Authorization Methods

This task configures the authentication and authorization methods for the device. The access granted using these methods will remain in effect for users who attempt reauthorization while the AAA server is unavailable. These methods must be configured before you configure any policy to be applied to users who try to access the network when the AAA server is unreachable.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication eou default group radius**
5. **aaa authorization network default local**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Router (config)# aaa new-model	Enables AAA.
Step 4	aaa authentication eou default group radius Example: Router (config)# aaa authentication eou default group radius	Sets authentication methods for Extensible Authorization Protocol over User Datagram Protocol (EAPoUDP). To remove the EAPoUDP authentication methods, use the no form of the command.
Step 5	aaa authorization network default local Example: Router (config)# aaa authorization network default local	Sets the authorization method to local. To remove the authorization method, use the no form of the command.

Configuring RADIUS Server Parameters

This task configures the identity and parameters of the RADIUS server that provides AAA services to the network access device. To configure RADIUS server parameters, you should understand the following concepts:

- [Identifying the RADIUS Server, page 6](#)
- [Determining When the RADIUS Server Is Unavailable, page 7](#)

Identifying the RADIUS Server

A RADIUS server can be identified by:

- hostname
- IP address
- hostname and a specific UDP port number
- IP address and a specific UDP port number

The combination of the RADIUS server IP address and a specific UDP port number creates a unique identifier, which enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, authentication—the second host entry configured acts as the backup to the first one. The RADIUS host entries are tried in the order that they were configured.

Determining When the RADIUS Server Is Unavailable

Because the NAC—Auth Fail Open feature applies a local policy when the RADIUS server is unavailable, you should configure “dead criteria” that identify when the RADIUS server is unavailable. There are two configurable dead criteria:

- **time**—the interval (in seconds) without a response to a request for AAA service
- **tries**—the number of consecutive AAA service requests without a response

If you do not configure the dead criteria, they will be calculated dynamically, based on the server configuration and the number of requests being sent to the server.

You can also configure the number of minutes to wait before attempting to resume communication with a RADIUS server after it has been defined as unavailable.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server dead-criteria** [**time** *seconds*] [**tries** *number-of-tries*]
4. **radius-server deadtime** *minutes*
5. **radius-server host** {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] [**idle-time** *seconds*]
6. **radius-server attribute 8 include-in-access-req**
7. **radius-server vsa send** [**accounting** | **authentication**]
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	radius-server dead-criteria [<i>time seconds</i>] [<i>tries number-of-tries</i>] Example: Router (config)# radius-server dead-criteria time 30 tries 20	(Optional) Sets the conditions that are used to decide when a RADIUS server is considered unavailable or <i>dead</i> . <ul style="list-style-type: none"> The range for <i>seconds</i> is from 1 to 120 seconds. The default is that the NAD dynamically determines the <i>seconds</i> value within a range from 10 to 60 seconds. The range for <i>number-of-tries</i> is from 1 to 100. The default is that the NAD dynamically determines the <i>number-of-tries</i> parameter within a range from 10 to 100.
Step 4	radius-server deadtime <i>minutes</i> Example: Router (config)# radius-server deadtime 60	(Optional) Sets the number of minutes that a RADIUS server is not sent requests after it is found to be dead. The range is from 0 to 1440 minutes (24 hours). The default is 0 minutes.

	Command or Action	Purpose
<p>Step 5</p>	<pre>radius-server host ip-address [acct-port udp-port] [auth-port udp-port] [key string] [test username name [idle-time time]</pre> <p>Example:</p> <pre>Router (config)# radius-server host 10.0.0.2 acct-port 1550 auth-port 1560 test username user1 idle-time 30 key abc1234</pre>	<p>(Optional) Configures the RADIUS server parameters by using these keywords:</p> <ul style="list-style-type: none"> • acct-port <i>udp-port</i>—Specifies the UDP port for the RADIUS accounting server. The range for the UDP port number is from 0 to 65536. The default is 1646. If the port number is set to 0, the host is not used for accounting. • auth-port <i>udp-port</i>—Specifies the UDP port for the RADIUS authentication server. The range for the UDP port number is from 0 to 65536. The default is 1645. If the port number is set to 0, the host is not used for authentication. <p>Note You should configure the UDP port for the RADIUS accounting server and the UDP port for the RADIUS authentication server to nondefault values.</p> <ul style="list-style-type: none"> • key <i>string</i>—Specifies the authentication and encryption key for all RADIUS communication between the NAD and the RADIUS daemon. <p>Note Always configure the key as the last item in the radius-server host command syntax because leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key. This key must match the encryption used on the RADIUS daemon.</p> <ul style="list-style-type: none"> • test username <i>name</i>—Enables automated testing of the RADIUS server status, and specify the username to be used. • idle-time <i>time</i>—Sets the interval of time in minutes after which the NAD sends test packets to the server. The range is from 1 to 35791 minutes. The default is 60 minutes (1 hour). <p>To configure multiple RADIUS servers, reenter this command.</p>
<p>Step 6</p>	<pre>radius-server attribute 8 include-in-access-req</pre> <p>Example:</p> <pre>Router (config)# radius-server attribute 8 include-in-access-req</pre>	<p>If the device is connected to nonresponsive hosts, configures the device to send the Framed-IP-Address RADIUS attribute (attribute[8]) in access-request or accounting-request packets.</p> <p>To configure the device to not send the Framed-IP-Address attribute, use the no radius-server attribute 8 include-in-access-req global configuration command.</p>

	Command or Action	Purpose
Step 7	radius-server vsa send authentication Example: Router (config)# radius-server vsa send authentication	Configures the network access server to recognize and use vendor-specific attributes (VSAs).
Step 8	end Example: Router (config)# end	Returns to privileged EXEC mode.

Displaying the Status of the Configured AAA Servers

This task displays the status of the AAA servers you have configured for the device.

SUMMARY STEPS

1. **enable**
2. **show aaa servers**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	show aaa servers Example: Router# show aaa servers	Displays the status of the AAA servers configured for the device.

Displaying the NAC Configuration

This task displays the current NAC configuration for the device.

SUMMARY STEPS

1. **enable**
2. **show ip admission {[cacke] [configuration] [eapoudp]}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example: Router> enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show ip admission configuration	Displays all the IP admission control rules configured for the device.
	Example: Router# show ip admission configuration	

Displaying the EAPoUDP Configuration

This task displays information about the current EAPoUDP configuration for the device, including any NAC—Auth Fail Open policies in effect.

SUMMARY STEPS

1. **enable**
2. **show eou {all | authentication {clientless | eap | static} | interface {interface-type} | ip {ip-address} | mac {mac-address} | posturetoken {name}} [{begin | exclude | include} expression]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example: Router> enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show eou ip 10.0.0.1	Displays information about the EAPoUDP configuration for the specified interface.
	Example: Router# show eou ip 10.0.0.1	

Enabling EOU Logging

A set of new system logs is included in Cisco IOS Release 12.4(11)T. These new logs track the status of the servers defined by the methodlist, and the NAC Auth Fail policy configuration. You should enable EOU logging to generate syslog messages that notify you when the AAA servers defined by the methodlist are unavailable, and display the configuration of the NAC—Auth Fail Open policy. The display shows whether a global or rule-specific policy is configured for the NAD or interface. If no policy is configured, the existing policy is retained.

This task enables EOU logging.

SUMMARY STEPS

1. **configure terminal**
2. **eou logging**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 2	eou logging Example: Router (config) # eou logging	Enables EOU logging.

Configuration Examples for NAC—Auth Fail Open

This section contains the following examples:

- [Sample NAC—Auth Fail Open Configuration: Example, page 12](#)
- [Sample RADIUS Server Configuration: Example, page 13](#)
- [show ip admission configuration Output: Example, page 13](#)
- [show eou Output: Example, page 13](#)
- [show aaa servers Output: Example, page 14](#)
- [EOU Logging Output: Example, page 14](#)

Sample NAC—Auth Fail Open Configuration: Example

The example below shows how to configure the NAC—Auth Fail Open feature:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip admission name AAA_DOWN eapoudp event timeout aaa policy identity
global_policy
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default local
Switch(config)# aaa authentication eou default group radius
Switch(config)# identity policy global_policy
Switch(config-identity-policy)# ac
Switch(config-identity-policy)# access-group global_acl
Switch(config)# ip access-list extended global_acl
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
```


Sample RADIUS Server Configuration: Example

The example below shows that the RADIUS server will be considered unreachable after 3 unsuccessful tries:

```
Switch(config)# radius-server host 10.0.0.4 test username administrator idle-time 1 key
sample
Switch(config)# radius-server dead-criteria tries 3
Switch(config)# radius-server deadtime 30
Switch(config)# radius-server vsa send authentication
Switch(config)# radius-server attribute 8 include-in-access-req
Switch(config)# int fastEthernet 2/13
Switch(config-if)# ip admission AAA_DOWN
Switch(config-if)# exit
```

show ip admission configuration Output: Example

The following example shows that a policy called “global policy” has been configured for use when the AAA server is unreachable:

```
Switch# show ip admission configuration
```

```
Authentication global cache time is 60 minutes Authentication global absolute time is 0
minutes Authentication global init state time is 2 minutes Authentication Proxy Watch-list
is disabled
```

```
Authentication Proxy Rule Configuration
```

```
Auth-proxy name AAA_DOWN
```

```
    eapoudp list not specified auth-cache-time 60 minutes
```

```
    Identity policy name global_policy for AAA fail policy
```

show eou Output: Example

The example below shows the configuration of the AAA servers defined for a NAC—Auth Fail policy configuration:

```
Router# show eou ip 10.0.0.1
```

```
Address : 10.0.0.1
MAC Address : 0001.027c.f364
Interface : Vlan333
! Authtype is show as AAA DOWN when in AAA is not reachable.
AuthType : AAA DOWN
! AAA Down policy name:
AAA Down policy : rule_policy
Audit Session ID : 00000000011C11830000000311000001
PostureToken : -----
Age(min) : 0
URL Redirect : NO URL REDIRECT
URL Redirect ACL : NO URL REDIRECT ACL
ACL Name : rule_acl
Tag Name : NO TAG NAME
User Name : UNKNOWN USER
```

```
Revalidation Period : 500 Seconds
Status Query Period : 300 Seconds
Current State : AAA DOWN
```

show aaa servers Output: Example

The example below shows sample status information for a configured AAA server:

```
Switch# show aaa servers

RADIUS: id 1, priority 1, host 10.0.0.4, auth-port 1645, acct-port 1646

    State: current UP, duration 5122s, previous duration 9s

    Dead: total time 79s, count 3

    Authen: request 158, timeouts 14

        Response: unexpected 1, server error 0, incorrect 0, time 180ms

        Transaction: success 144, failure 1

    Author: request 0, timeouts 0

        Response: unexpected 0, server error 0, incorrect 0, time 0ms

        Transaction: success 0, failure 0

    Account: request 0, timeouts 0

        Response: unexpected 0, server error 0, incorrect 0, time 0ms

        Transaction: success 0, failure 0

    Elapsed time since counters last cleared: 2h13mS
```

EOU Logging Output: Example

The example below shows the display when EOU logging is enabled:

```
Router (config)# eou logging
EOU-5-AAA_DOWN: AAA unreachable.
METHODLIST=Default| HOST=17.0.0.1| POLICY=Existing policy retained.
EOU-5-AAA_DOWN: AAA unreachable.
METHODLIST=Default| HOST=17.0.0.1| POLICY=aaa_unreachable_policy
```

Additional References

The following sections provide references related to the NAC—Auth Fail Open feature.

Related Documents

Related Topic	Document Title
Configuring NAC	Network Admission Control Software Configuration Guide
Security commands	Cisco IOS Security Command Reference , Release 12.4

Standards

Standard	Title
IEEE 802.1x	IEEE Standard 802.1X - 2004 Port-Based Network Access Control

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and technical documentation. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **ip admission**
- **ip admission name**
- **show eou**
- **show ip admission**
- **Feature Information for NAC—Auth Fail Open**

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Network Admission Control: Agentless Host Support

First Published: February 27, 2006

Last Updated: February 27, 2006

The Network Admission Control: Agentless Host Support feature allows for an exhaustive examination of agentless hosts (hosts that are not running the Cisco Trust Agent software). This examination allows customers to build a robust host or examination functionality by integrating any third-party audit mechanisms into the Network Admission Control architecture.

This feature also allows for Extensible Authentication Protocol over UDP (EAPoUDP) bypass, which speeds up the posture validation of hosts that are not using Cisco Trust Agent.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Network Admission Control: Agentless Host Support](#)” section on page 18.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Network Admission Control: Agentless Host Support, page 2](#)
- [Information About Network Admission Control: Agentless Host Support, page 2](#)
- [How to Configure Network Admission Control: Agentless Host Support, page 4](#)
- [Configuration Examples for Network Admission Control: Agentless Host Support, page 6](#)
- [Additional References, page 7](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Command Reference, page 8](#)
- [Feature Information for Network Admission Control: Agentless Host Support, page 18](#)

Prerequisites for Network Admission Control: Agentless Host Support

- You must be running Cisco IOS Release 12.4(6)T or a later release.
- You must be using a Cisco access control server (ACS) version 4.0 or a later version.
- You must have a Cisco or third-party audit server setup.

Information About Network Admission Control: Agentless Host Support

To configure the Network Admission Control: Agentless Host Support feature, you should understand the following concepts:

- [Network Admission Control, page 2](#)
- [Agentless Hosts, page 2](#)
- [EAPoUDP Bypass, page 3](#)
- [Vendor-Specific Attributes for This Feature, page 3](#)

Network Admission Control

The Cisco Network Admission Control functionality enables the credentials of the endpoint device to be checked for compliance with the security policy before the device is granted access to network resources. This checking requires a security application called Cisco Trust Agent (CTA) to be installed on end devices that gather security state information and communicate it to access servers where policy decisions are made and eventually enforced on Cisco network access devices (such as routers and switches).

Agentless Hosts

End devices that do not run CTA cannot provide credentials when challenged by network access devices (NADs). Such hosts are termed “agentless” or “nonresponsive.” In the Phase 1 release of Network Admission Control, agentless hosts were supported by either a static configuration using exception lists (an identity profile) or by using “clientless” username and password authentication on an ACS. These methods are restrictive and do not convey any specific information about the host while making policy decisions.

EAPoUDP Bypass

You can use the EAPoUDP Bypass feature to reduce latency of the validation of hosts that are not using CTA. If EAPoUDP bypass is enabled, the NAD does not contact the host to request the antivirus condition (the NAD does not try to establish an EAPoUDP association with the host if the EAPoUDP Bypass option is configured). Instead, the NAD sends a request to the Cisco Secure ACS that includes the IP address, MAC address, service type, and EAPoUDP session ID of the host. The Cisco Secure ACS makes the access control decision and sends the policy to the NAD.

If EAPoUDP bypass is enabled, the NAD sends an agentless host request to the Cisco Secure ACS and applies the access policy from the server to the host.

If EAPoUDP bypass is enabled and the host uses the Cisco Trust Agent, the NAD also sends a nonresponsive-host request to the Cisco Secure ACS and applies the access policy from the server to the host.

Vendor-Specific Attributes for This Feature

The following new attributes are supported for various RADIUS message exchanges:

- [audit-session-id](#), page 3
- [url-redirect-acl](#), page 3

audit-session-id

The audit-session-id vendor-specific attribute (VSA) is a 32-byte string that uniquely identifies a host session. This identifier is generated by a NAD when the host is detected, and it remains the same until the session is deleted. Session revalidation or reinitialization does not change this identifier. Every time a session is detected, a new identifier is generated. This attribute is included in access requests to the authentication, authorization, and accounting (AAA) server and in web requests to the audit server. The value of this attribute is displayed in **show eou** command output (using the **ip** keyword).

url-redirect-acl

The url-redirect-acl VSA string specifies the name of the access control list (ACL) for URL redirection. Any ingress HTTP from the host that matches the access list that is specified by this attribute is subjected to redirection to the URL address specified by the url-redirect VSA. The access list specified in this attribute has to be locally configured on the NAD as an “ip access-list extended” named ACL. This attribute is specified only in RADIUS access-accept messages. The value of the url-redirect-acl attribute is displayed using the **show eou** command (with the **ip** keyword).



Note

Phase 1 of the Network Admission Control feature introduced the url-redirect VSA that allowed the HTTP sessions of users to be redirected to the address specified by the url-redirect VSA. This redirection is useful if you want to remediate hosts that do not comply to network security policy. However, to determine to which users HTTP requests are to be redirected, Phase 1 of Network Admission Control assumed that any HTTP traffic that was intercepted and denied by the host policy ACL (the access control server ACL) was subjected to redirection. The url-redirect-acl VSA provides an option so that users can customize the redirect criteria. The url-redirect-acl VSA supports backward compatibility. If the url-redirect-acl is specified in the access-accept message for the host, any user HTTP sessions that

match the ACL are subjected to redirection. However, if the url-redirect-acl attribute is not received, the Phase 1 logic to perform redirection is used. The Phase 1 logic to perform redirection applies only to Cisco IOS routers. The url-redirect-acl attribute is mandatory for Cisco IOS switches.

How to Configure Network Admission Control: Agentless Host Support

This section includes the following required and optional tasks.

- [Configuring a NAD to Bypass EAPoUDP Communication, page 4](#) (required)
- [Verifying Agentless Host and EAPoUDP Bypass, page 5](#) (optional)

Configuring a NAD to Bypass EAPoUDP Communication

To configure a NAD to bypass EAPoUDP, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission name** *admission-name* **eapoudp bypass**
4. **eou allow clientless**
5. **interface type** *slot/port*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip admission name <i>admission-name</i> eapoudp bypass Example: Router (config)# ip admission name greentree eapoudp bypass	The IP network admission control rule bypasses EAPoUDP communication.
Step 4	eou allow clientless Example: Router (config)# eou allow clientless	Allows authentication of clientless hosts (systems that do not run Cisco Trust Agent).
Step 5	interface type <i>slot/port</i> Example: Router (config)# interface ethernet 2/4	Configures an interface type and enters interface configuration mode.
Step 6	end Example: Router (config-if)# end	Exits configuration modes.

Verifying Agentless Host and EAPoUDP Bypass

To verify your configuration for Agentless Host and EOUoUDP Bypass, perform the following steps. The **debug** and **show** commands can be used independently of each other.

SUMMARY STEPS

1. **enable**
2. **debug eou**
3. **show eou ip** *ip-address*
4. **show ip admission configuration**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	debug eou Example: Router# debug eou	Displays information about EAUoUDP.
Step 3	show eou ip ip-address Example: Router# show eou ip 10.0.0.0	Displays information about EAPoUDP global values or EAPoUDP session cache entries.
Step 4	show ip admission configuration Example: Router# show ip admission configuration	Displays information about the agentless and EAPoUDP Bypass configuration.

Configuration Examples for Network Admission Control: Agentless Host Support

This section provides the following configuration examples.

- [RADIUS Message Exchange url-redirect-acl VSA: Example, page 6](#)
- [Show Output Displaying the Value of a Newly Defined VSA, page 6](#)

RADIUS Message Exchange url-redirect-acl VSA: Example

ACS Configuration

```
url-redirect=http://audit-server.com/host_session_id=$host_session_id
url-redirect-acl=RedirectACL
```

NAD Configuration

```
Router(config)# ip access-list extended RedirectACL
Router (config-ext-nacl)# permit tcp any 10.0.0.0 0.0.0.255 eq www
Router (config-ext-nacl)# end
```

Show Output Displaying the Value of a Newly Defined VSA

The following **show eou** command output displays EAPoUDP session cache information for a given IP address. The value of the newly defined VSA is also shown.

```
Router# show eou ip 10.0.0.1
```

```
Address           : 10.0.0.1
MAC Address       : 0001.027c.f364
Interface         : FastEthernet1/0/3
AuthType          : EAP
Audit Session ID  : 000000001C8A6A330000001812000001
PostureToken      : Infected
Age(min)          : 444
URL Redirect      : http://wwwin.cisco.com
URL Redirect ACL  : RedirectACL
ACL Name          : #ACSACL#-IP-Infected-42835ff7
User Name         : NAC-DEV-PC-3:Administrator
Revalidation Period : 30000 Seconds
Status Query Period : 300 Seconds
Current State     : AUTHENTICATED
```

Additional References

The following sections provide references related to Network Admission Control: Agentless Host.

Related Documents

Related Topic	Document Title
Configuring AAA and RADIUS for EAPoUDP	“Configuring AAA for EAPoUDP” section of the <i>Network Admission Control feature guide</i> .
Security commands	<i>Cisco IOS Security Command Reference</i> , Release 12.4T
Network Admission Control	<i>Network Admission Control</i> feature guide

Standards

Standard	Title
No new or modified standards are supported by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this

module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **eou clientless**
- **ip admission name**
- **show eou**
- **Feature Information for Network Admission Control: Agentless Host Support**

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Authentication Proxy



Configuring Authentication Proxy

This chapter describes the Cisco IOS Firewall Authentication Proxy feature. Authentication proxy provides dynamic, per-user authentication and authorization, authenticating users against industry standard TACACS+ and RADIUS authentication protocols. Authenticating and authorizing connections by users provides more robust protection against network attacks.

For a complete description of the authentication proxy commands in this chapter, refer to the “Authentication Proxy Commands” chapter of the *Cisco IOS Security Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the “Identifying Supported Platforms” section in the chapter “Using Cisco IOS Software.”

In This Chapter

This chapter contains the following sections:

- [About Authentication Proxy](#)
- [Authentication Proxy Configuration Task List](#)
- [Monitoring and Maintaining the Authentication Proxy](#)
- [Authentication Proxy Configuration Examples](#)

About Authentication Proxy

The Cisco IOS Firewall authentication proxy feature allows network administrators to apply specific security policies on a per-user basis. Previously, user identity and related authorized access were associated with a user IP address, or a single security policy had to be applied to an entire user group or subnetwork. Now, users can be identified and authorized on the basis of their per-user policy. Tailoring of access privileges on an individual basis is possible, as opposed to applying a general policy across multiple users.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

With the authentication proxy feature, users can log in to the network or access the Internet via HTTP, and their specific access profiles are automatically retrieved and applied from a CiscoSecure ACS, or other RADIUS, or TACACS+ authentication server. The user profiles are active only when there is active traffic from the authenticated users.

The authentication proxy is compatible with other Cisco IOS security features such as Network Address Translation (NAT), Context-based Access Control (CBAC), IP Security (IPSec) encryption, and Cisco Secure VPN Client (VPN client) software.

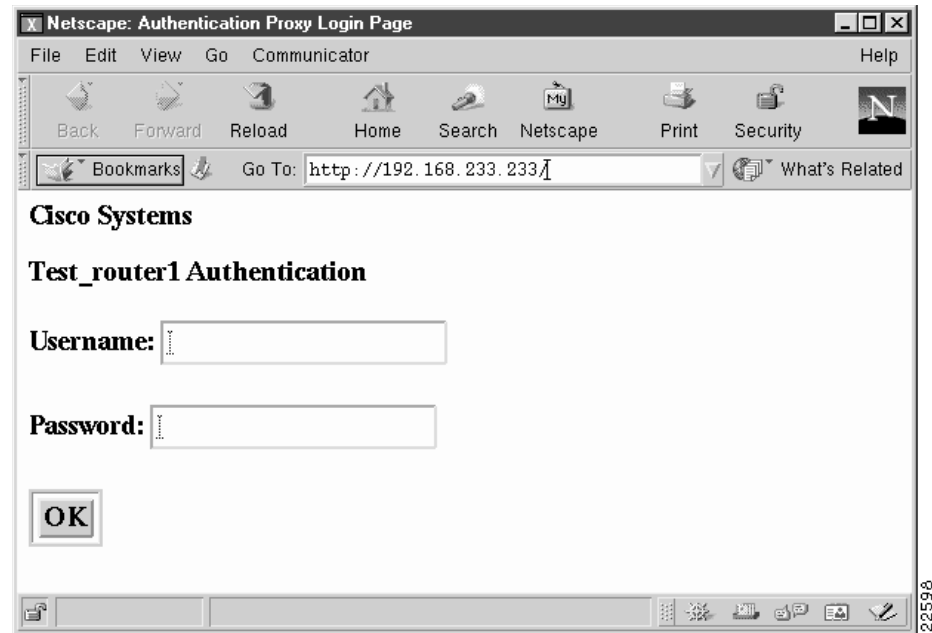
This section contains the following sections:

- [How the Authentication Proxy Works](#)
- [Secure Authentication](#)
- [Using the Authentication Proxy](#)
- [When to Use the Authentication Proxy](#)
- [Applying the Authentication Proxy](#)
- [Operation with One-Time Passwords](#)
- [Compatibility with Other Security Features](#)
- [Compatibility with AAA Accounting](#)
- [Protection Against Denial-of-Service Attacks](#)
- [Risk of Spoofing with Authentication Proxy](#)
- [Comparison with the Lock-and-Key Feature](#)
- [Restrictions](#)
- [Prerequisites to Configuring Authentication Proxy](#)

How the Authentication Proxy Works

When a user initiates an HTTP session through the firewall, the authentication proxy is triggered. The authentication proxy first checks to see if the user has been authenticated. If a valid authentication entry exists for the user, the connection is completed with no further intervention by the authentication proxy. If no entry exists, the authentication proxy responds to the HTTP connection request by prompting the user for a username and password.

[Figure 42](#) illustrates the authentication proxy HTML login page.

Figure 42 Authentication Proxy Login Page

Users must successfully authenticate themselves with the authentication server by entering a valid username and password.

If the authentication succeeds, the user's authorization profile is retrieved from the AAA server. The authentication proxy uses the information in this profile to create dynamic access control entries (ACEs) and add them to the inbound (input) access control list (ACL) of an input interface and to the outbound (output) ACL of an output interface, if an output ACL exists at the interface. This process enables the firewall to allow authenticated users access to the network as permitted by the authorization profile. For example, a user can initiate a Telnet connection through the firewall if Telnet is permitted in the user's profile.

If the authentication fails, the authentication proxy reports the failure to the user and prompts the user with multiple retries. If the user fails to authenticate after five attempts, the user must wait two minutes and initiate another HTTP session to trigger authentication proxy.

The login page is refreshed each time the user makes requests to access information from a web server.

The authentication proxy customizes each of the access list entries in the user profile by replacing the source IP addresses in the downloaded access list with the source IP address of the authenticated host.

At the same time that dynamic ACEs are added to the interface configuration, the authentication proxy sends a message to the user confirming that the login was successful. [Figure 43](#) illustrates the login status in the HTML page.

Figure 43 **Authentication Proxy Login Status Message**



The authentication proxy sets up an inactivity (idle) timer for each user profile. As long as there is activity through the firewall, new traffic initiated from the user's host does not trigger the authentication proxy, and authorized user traffic is permitted access through the firewall.

If the idle timer expires, the authentication proxy removes the user's profile information and dynamic access lists entries. When this happens, traffic from the client host is blocked. The user must initiate another HTTP connection to trigger the authentication proxy.

Secure Authentication

The authentication proxy uses JavaScript to help achieve secure authentication using the client browser. Secure authentication prevents a client from mistakenly submitting a username and password to a network web server other than the authentication proxy router.

This section contains the following sections:

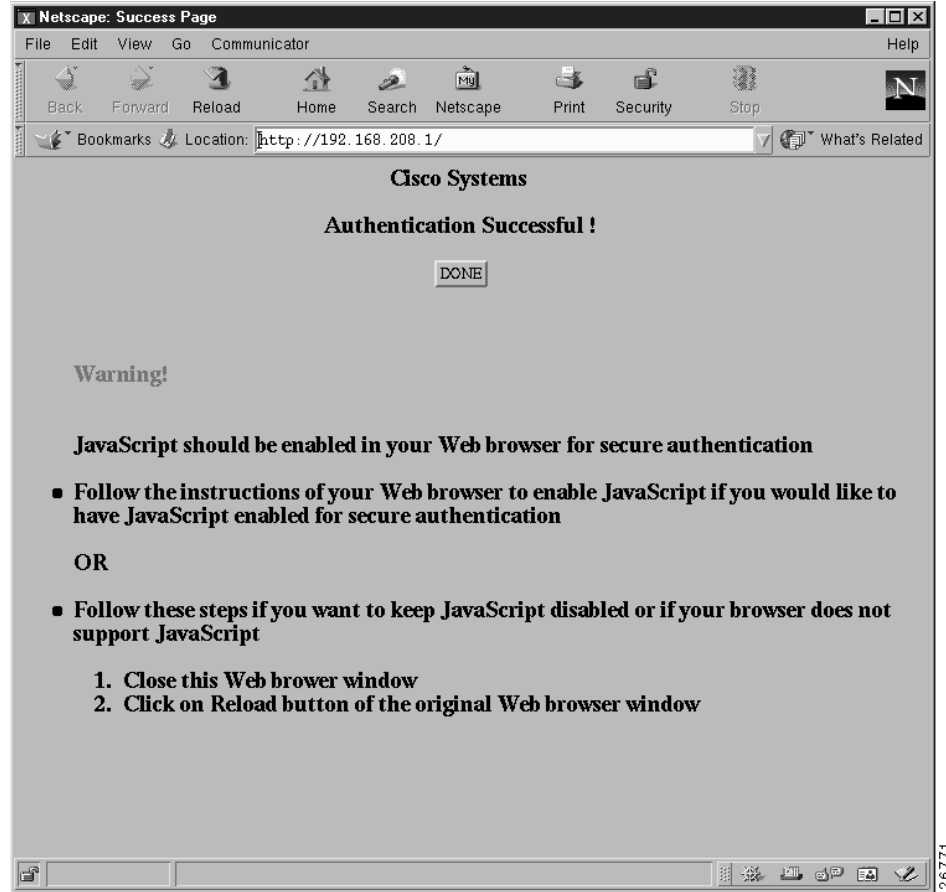
- [Operation with JavaScript](#)
- [Operation Without JavaScript](#)

Operation with JavaScript

Users should enable JavaScript on the browser prior to initiating an HTTP connection. With JavaScript enabled on the browser, secure authentication is done automatically, and the user sees the authentication message shown in [Figure 43](#). The HTTP connection is completed automatically for the user.

Operation Without JavaScript

If the client browser does not support JavaScript, or if site security policy prevents users from enabling JavaScript, any login attempt generates a popup window with instructions for manually completing the connection. [Figure 44](#) illustrates the authentication proxy login status message with JavaScript disabled on the browser.

Figure 44 Authentication Proxy Login Status Message with JavaScript Disabled

To close this window, click Close on the browser File menu.

After closing the popup window, the user should click Reload (Refresh for Internet Explorer) in the browser window in which the authentication login page is displayed. If the user's last authentication attempt succeeds, clicking Reload brings up the web page the user is trying to retrieve. If the user's last attempt fails, clicking Reload causes the authentication proxy to intercept the client HTTP traffic again, prompting the user with another login page that solicits the username and password.

If JavaScript is not enabled, it is strongly recommended that site administrators advise users of the correct procedure for closing the popup window as described in the section "[Establishing User Connections Without JavaScript](#)."

Using the Authentication Proxy

Unlike some Cisco IOS Firewall features that operate transparently to the user, the authentication proxy feature requires some user interaction on the client host. [Table 40](#) describes the interaction of the authentication proxy with the client host.

Table 40 **Authentication Proxy Interaction with the Client Host**

Authentication Proxy Action with Client	Description
Triggering on HTTP connections	If a user is not currently authenticated at the firewall router, any HTTP connection initiated by the user triggers the authentication proxy. If the user is already authenticated, the authentication proxy is transparent to the user.
Logging in using the login page	Triggering the authentication proxy generates an HTML-based login page. The user must enter a username and password to be authenticated with the AAA server. Figure 42 illustrates the authentication proxy login page.
Authenticating the user at the client	<p>Following the login attempt, the authentication proxy action can vary depending on whether JavaScript is enabled in the browser. If JavaScript is enabled, and authentication is successful, the authentication proxy displays a message indicating the status of the authentication as shown in Figure 43. After the authentication status is displayed, the proxy automatically completes the HTTP connection.</p> <p>If JavaScript is disabled, and authentication is successful, the authentication proxy generates a popup window with additional instructions for completing the connection. See Figure 44.</p> <p>If authentication is unsuccessful in any case, the user must log in again from the login page.</p>

When to Use the Authentication Proxy

Here are examples of situations in which you might use the authentication proxy:

- You want to manage access privileges on an individual (per-user) basis using the services provided by the authentication servers instead of configuring access control based on host IP address or global access policies. Authenticating and authorizing users from any host IP address also allows network administrators to configure host IP addresses using DHCP.
- You want to authenticate and authorize local users before permitting access to intranet or Internet services or hosts through the firewall.
- You want to authenticate and authorize remote users before permitting access to local services or hosts through the firewall.
- You want to control access for specific extranet users. For example, you might want to authenticate and authorize the financial officer of a corporate partner with one set of access privileges while authorizing the technology officer for that same partner to use another set of access privileges.
- You want to use the authentication proxy in conjunction with VPN client software to validate users and to assign specific access privileges.
- You want to use the authentication proxy in conjunction with AAA accounting to generate “start” and “stop” accounting records that can be used for billing, security, or resource allocation purposes, thereby allowing users to track traffic from the authenticated hosts.

Applying the Authentication Proxy

Apply the authentication proxy in the inbound direction at any interface on the router where you want per-user authentication and authorization. Applying the authentication proxy inbound at an interface causes it to intercept a user's initial connection request before that request is subjected to any other processing by the firewall. If the user fails to gain authentication with the AAA server, the connection request is dropped.

How you apply the authentication proxy depends on your security policy. For example, you can block all traffic through an interface and enable the authentication proxy feature to require authentication and authorization for all user initiated HTTP connections. Users are authorized for services only after successful authentication with the AAA server.

The authentication proxy feature also allows you to use standard access lists to specify a host or group of hosts whose initial HTTP traffic triggers the proxy.

Figure 45 shows the authentication proxy applied at the LAN interface with all network users required to be authenticated upon the initial connection (all traffic is blocked at each interface).

Figure 45 **Applying the Authentication Proxy at the Local Interface**

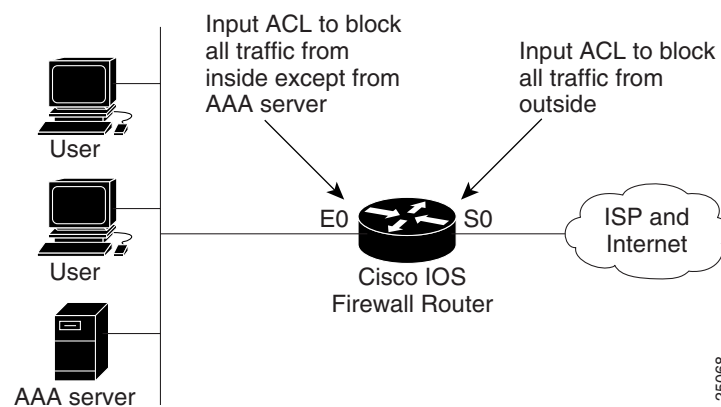
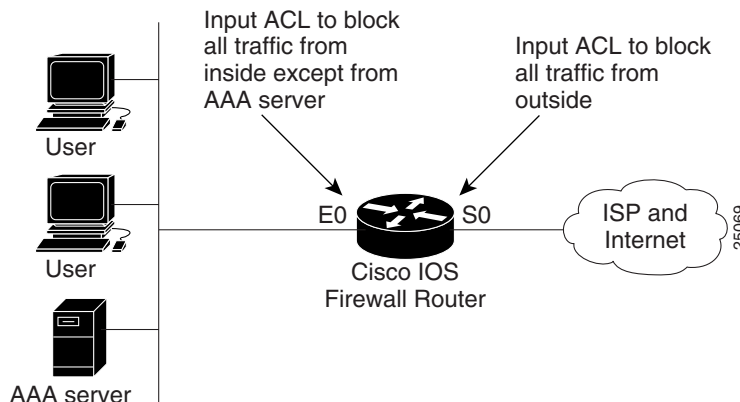


Figure 46 shows the authentication proxy applied at the dial-in interface with all network traffic blocked at each interface.

Figure 46 *Applying the Authentication Proxy at an Outside Interface*



Operation with One-Time Passwords

Given a one-time password, the user enters the username and one-time password in the HTML login page as usual.

The user must enter the correct token password within the first three attempts. After three incorrect entries, the user must enter two valid token passwords in succession before authentication is granted by the AAA server.

Compatibility with Other Security Features

The authentication proxy is compatible with Cisco IOS software and with Cisco IOS security features:

- Cisco IOS Firewall Intrusion Detection System (IDS)
- NAT
- CBAC
- IPSec encryption
- VPN client software

The authentication proxy works transparently with the Cisco IOS Firewall IDS and IPSec encryption features. The following sections describe the relationship of the NAT, CBAC, and VPN client software features with the authentication proxy:

- [NAT Compatibility](#)
- [CBAC Compatibility](#)
- [VPN Client Compatibility](#)

NAT Compatibility

The authentication proxy feature is compatible with NAT only if the ACL and authentication are completed prior to the NAT translation. Although NAT is compatible with the authentication proxy feature, NAT is not a requirement of the feature.

CBAC Compatibility

Although authentication proxy is compatible with CBAC security functions, CBAC is not required to use the authentication proxy feature.

Authentication proxy's authorization returns Access Control Entries (ACEs) that are dynamically prepended into a manually created ACL. Thereafter, apply the ACL to the "protected side" inbound interface, allowing or disallowing an authorized user's source IP address access to the remote networks.

VPN Client Compatibility

Using the authentication proxy, network administrators can apply an extra layer of security and access control for VPN client traffic. If a VPN client initiates an HTTP connection, the authentication proxy first checks for prior client authentication. If the client is authenticated, authorized traffic is permitted. If the client is not authenticated, the HTTP request triggers the authentication proxy, and the user is prompted for a username and password.

If the user authentication is successful, the authentication proxy retrieves the user profile from the AAA server. The source address in the user profile entries is replaced with the IP address of the authenticated VPN client from the decrypted packet.

Compatibility with AAA Accounting

Using the authentication proxy, you can generate "start" and "stop" accounting records with enough information to be used for billing and security auditing purposes. Thus, you can monitor the actions of authenticated hosts that use the authentication proxy service.

When an authentication proxy cache and associated dynamic access control lists are created, the authentication proxy will start to track the traffic from the authenticated host. Accounting saves data about this event in a data structure stored with the data of other users. If the accounting start option is enabled, you can generate an accounting record (a "start" record) at this time. Subsequent traffic from the authenticated host will be recorded when the dynamic ACL created by the authentication proxy receives the packets.

When an authentication proxy cache expires and is deleted, additional data, such as elapsed time, is added to the accounting information and a "stop" record is sent to the server. At this point, the information is deleted from the data structure.

The accounting records for the authentication proxy user session are related to the cache and the dynamic ACL usage.

**Note**

The accounting records must include RADIUS attributes 42, 46, and 47 for both RADIUS and TACACS+.

For more information on RADIUS attributes, refer to the appendix "RADIUS Attributes."

Protection Against Denial-of-Service Attacks

The authentication proxy monitors the level of incoming HTTP requests. For each request, the authentication proxy prompts the user's for login credentials. A high number of open requests could indicate that the router is the subject of a denial-of-service (DoS) attack. The authentication proxy limits the level of open requests and drops additional requests until the number of open requests has fallen below 40.

If the firewall is experiencing a high level of connection requests requiring authentication, legitimate network users may experience delays when making connections, or the connection may be rejected and the user must try the connection again.

Risk of Spoofing with Authentication Proxy

When the authentication proxy is triggered, it creates a dynamic opening in the firewall by temporarily reconfiguring an interface with user access privileges. While this opening exists, another host might spoof the authenticated users address to gain access behind the firewall. The authentication proxy does not cause the address spoofing problem; the problem is only identified here as a matter of concern to the user. Spoofing is a problem inherent to all access lists, and the authentication proxy does not specifically address this problem.

Comparison with the Lock-and-Key Feature

Lock-and-key is another Cisco IOS Firewall feature that uses authentication and dynamic access list to provide user access through the firewall. [Table 41](#) compares the authentication proxy and lock-and-key features.

Table 41 Comparison of the Authentication Proxy and Lock-and-Key Features

Lock-and-Key	Authentication Proxy
Triggers on Telnet connection requests.	Triggers on HTTP connection requests.
TACACS+, RADIUS, or local authentication.	TACACS+ or RADIUS authentication and authorization.
Access lists are configured on the router only.	Access lists are retrieved from the AAA server only.
Access privileges are granted on the basis of the user's host IP address.	Access privileges are granted on a per-user and host IP address basis.
Access lists are limited to one entry for each host IP address.	Access lists can have multiple entries as defined by the user profiles on the AAA server.
Associates a fixed IP addresses with a specific user. Users must log in from the host with that IP address.	Allows DHCP-based host IP addresses, meaning that users can log in from any host location and obtain authentication and authorization.

Use the authentication proxy in any network environment that provides a per-user security policy. Use lock-and-key in network environments that might benefit from local authentication and a limited number of router-based access control policies based on host addresses. Use lock-and-key in environments not using the Cisco Secure Integrated Software.

Restrictions

- The authentication proxy triggers only on HTTP connections.
- HTTP services must be running on the standard (well-known) port, which is port 80 for HTTP.
- Client browsers must enable JavaScript for secure authentication.
- The authentication proxy access lists apply to traffic passing through the router. Traffic destined to the router is authenticated by the existing authentication methods provided by Cisco IOS software.
- The authentication proxy does not support concurrent usage; that is, if two users try to log in from the same host at the same time, authentication and authorization applies only to the user who first submits a valid username and password.
- Load balancing using multiple or different AAA servers is not supported.

Prerequisites to Configuring Authentication Proxy

Prior to configuring authentication proxy, review the following:

- For the authentication proxy to work properly, the client host must be running the following browser software:
 - Microsoft Internet Explorer 3.0 or later
 - Netscape Navigator 3.0 or later
- The authentication proxy has an option to use standard access lists. You must have a solid understanding of how access lists are used to filter traffic before you attempt to configure the authentication proxy. For an overview of how to use access lists with the Cisco IOS Firewall, refer to the chapter “Access Control Lists: Overview and Guidelines.”
- The authentication proxy employs user authentication and authorization as implemented in the Cisco authentication, authorization, and accounting (AAA) paradigm. You must understand how to configure AAA user authentication, authorization, and accounting before you configure the authentication proxy. User authentication, authorization, and accounting are explained in the chapter “Authentication, Authorization, and Accounting (AAA).”
- To run the authentication proxy successfully with Cisco IOS Firewall, configure CBAC on the firewall. For complete information on the CBAC feature, refer to the chapter “Configuring Context-Based Access Control.”

Authentication Proxy Configuration Task List

To configure the authentication proxy feature, perform the following tasks:

- [Configuring AAA](#) (Required)
- [Configuring the HTTP Server](#) (Required)
- [Configuring the Authentication Proxy](#) (Required)
- [Verifying the Authentication Proxy](#) (Optional)

For authentication proxy configuration examples using the commands in this chapter, refer to the section “[Authentication Proxy Configuration Examples](#)” at the end of this chapter.

Configuring AAA

You must configure the authentication proxy for AAA services. Use the following commands in global configuration mode to enable authorization and to define the authorization methods:

	Command	Purpose
Step 1	<code>router(config)# aaa new-model</code>	Enables the AAA functionality on the router.
Step 2	<code>router(config)# aaa authentication login default TACACS+ RADIUS</code>	Defines the list of authentication methods at login.
Step 3	<code>router(config)# aaa authorization auth-proxy default [method1 [method2...]]</code>	Uses the auth-proxy keyword to enable authentication proxy for AAA methods.
Step 4	<code>router(config)# aaa accounting auth-proxy default start-stop group tacacs+</code>	Uses the auth-proxy keyword to set up the authorization policy as dynamic ACLs that can be downloaded. This command activates authentication proxy accounting.
Step 5	<code>router(config)# tacacs-server host hostname</code>	Specifies an AAA server. For RADIUS servers, use the radius server host command.
Step 6	<code>router(config)# tacacs-server key key</code>	Sets the authentication and encryption key for communications between the router and the AAA server. For RADIUS servers use the radius server key command.
Step 7	<code>router(config)# access-list access-list-number permit tcp host source eq tacacs host destination</code>	Creates an ACL entry to allow the AAA server to return traffic to the firewall. The source address is the IP address of the AAA server, and the destination is the IP address of the router interface where the AAA server resides.

In addition to configuring AAA on the firewall router, the authentication proxy requires a per-user access profile configuration on the AAA server. To support the authentication proxy, configure the AAA authorization service **auth-proxy** on the AAA server as outlined here:

- Define a separate section of authorization for the **auth-proxy** keyword to specify the downloadable user profiles. This keyword does not interfere with other type of services, such as EXEC. The following example shows a user profile on a TACACS server:

```
default authorization = permit
key = cisco
user = newuser1 {
  login = cleartext cisco
  service = auth-proxy
  {
    priv-lvl=15
    proxyacl#1="permit tcp any any eq 26"
    proxyacl#2="permit icmp any host 60.0.0.2"
    proxyacl#3="permit tcp any any eq ftp"
    proxyacl#4="permit tcp any any eq ftp-data"
    proxyacl#5="permit tcp any any eq smtp"
    proxyacl#6="permit tcp any any eq telnet"
  }
}
```

- The only supported attribute in the AAA server user configuration is proxyacl#n. Use the proxyacl#n attribute when configuring the access lists in the profile. The attribute proxyacl#n is for both RADIUS and TACACS+ attribute-value (AV) pairs.
- The privilege level must be set to 15 for all users.

- The access lists in the user profile on the AAA server must have access commands that contain only the **permit** keyword.
- Set the source address to the **any** keyword in each of the user profile access list entries. The source address in the access lists is replaced with the source address of the host making the authentication proxy request when the user profile is downloaded to the firewall.
- The supported AAA servers are:
 - CiscoSecure ACS 2.1.x for Windows NT
 - CiscoSecure ACS 2.3 for Windows NT
 - CiscoSecure ACS 2.2.4 for UNIX
 - CiscoSecure ACS 2.3 for UNIX
 - TACACS+ server (vF4.02.alpha)
 - Ascend RADIUS server radius-980618 (required attribute-value pair patch)
 - Livingston RADIUS server (v1.16)

Refer to the section [“AAA Server User Profile Example”](#) for sample AAA server configurations.

Configuring the HTTP Server

To use authentication proxy, you must also enable the HTTP server on the firewall and set the HTTP server authentication method to use AAA. Enter the following commands in global configuration mode:

	Command	Purpose
Step 1	<code>router(config)# ip http server</code>	Enables the HTTP server on the router. The authentication proxy uses the HTTP server to communicate with the client for user authentication.
Step 2	<code>router(config)# ip http access-class access-list-number</code>	Specifies the access list for the HTTP server. Use the standard access list number configured in the section “Interface Configuration Example.”

Configuring the Authentication Proxy



Note

Set the **auth-cache-time** option for any authentication proxy rule to a higher value than the idle timeout value for any CBAC inspection rule. When the authentication proxy removes an authentication cache along with its associated dynamic user ACL, there may be some idle connections monitored by CBAC, and removal of user-specific ACLs could cause those idle connections to hang. If CBAC has a shorter idle timeout, CBAC resets these connections when the idle timeout expires; that is, before the authentication proxy removes the user profile.

To configure the authentication proxy, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	<code>router(config)# ip auth-proxy auth-cache-time min</code>	Sets the global authentication proxy idle timeout value in minutes. If the timeout expires, user authentication entries are removed, along with any associated dynamic access lists. The default value is 60 minutes.
Step 2	<code>router(config)# ip auth-proxy auth-proxy-banner</code>	(Optional) Displays the name of the firewall router in the authentication proxy login page. The banner is disabled by default.
Step 3	<code>router(config)# ip auth-proxy name auth-proxy-name http [auth-cache-time min] [list {acl acl-name}]</code>	<p>Creates authentication proxy rules. The rules define how you apply authentication proxy. This command associates connections initiating HTTP protocol traffic with an authentication proxy name. You can associate the named rule with an access control list (ACL), providing control over which hosts use the authentication proxy feature. If no standard access list is defined, the named authentication proxy rule intercepts HTTP traffic from all hosts whose connection initiating packets are received at the configured interface.</p> <p>(Optional) The auth-cache-time option overrides the global authentication proxy cache timer. This option provides more control over timeout values for a specific authentication proxy rule. If no value is specified, the proxy rule assumes the value set with the ip auth-proxy auth-cache-time command.</p> <p>(Optional) The list option allows you to apply a standard, extended (1-199), or named access list to a named authentication proxy rule. HTTP connections initiated by hosts in the access list are intercepted by the authentication proxy.</p>
Step 4	<code>router(config)# interface type</code>	Enters interface configuration mode by specifying the interface type on which to apply the authentication proxy.
Step 5	<code>router(config-if)# ip auth-proxy auth-proxy-name</code>	In interface configuration mode, applies the named authentication proxy rule at the interface. This command enables the authentication proxy rule with that name.

Verifying the Authentication Proxy

Verifying the authentication proxy configuration can have several components:

- [Checking the Authentication Proxy Configuration](#) (Optional)
- [Establishing User Connections with JavaScript](#) (Optional)
- [Establishing User Connections Without JavaScript](#) (Optional)

Checking the Authentication Proxy Configuration

To check the current authentication proxy configuration, use the **show ip auth-proxy configuration** command in privileged EXEC mode:

Command	Purpose
router# show ip auth-proxy configuration	Displays the authentication proxy configuration.

In the following example, the global authentication proxy idle timeout value is set to 60 minutes, the named authentication proxy rule is “pxy”, and the idle timeout value for this named rule is one minute. The display shows that no host list is specified, meaning that all connections initiating HTTP traffic at the interface are subject to the authentication proxy rule.

```
router# show ip auth-proxy configuration
Authentication cache time is 60 minutes
Authentication Proxy Rule Configuration
Auth-proxy name pxy
http list not specified auth-cache-time 1 minutes
```

To verify that the authentication proxy is successfully configured on the router, ask a user to initiate an HTTP connection through the router. The user must have authentication and authorization configured at the AAA server. If the user authentication is successful, the firewall completes the HTTP connection for the user. If the authentication is unsuccessful, check the access list and the AAA server configurations.

Display the user authentication entries using the **show ip auth-proxy cache** command in privileged EXEC mode:

Command	Purpose
router# show ip auth-proxy cache	Displays the list of user authentication entries.

The authentication proxy cache lists the host IP address, the source port number, the timeout value for the authentication proxy, and the state of the connection. If the authentication proxy state is HTTP_ESTAB, the user authentication was successful.

```
router# show ip auth-proxy cache
Authentication Proxy Cache
Client IP 192.168.25.215 Port 57882, timeout 1, state HTTP_ESTAB
```

Wait for one minute, which is the timeout value for this named rule, and ask the user to try the connection again. After one minute, the user connection is denied because the authentication proxy has removed the user's authentication entry and any associated dynamic ACLs. The user is presented with a new authentication login page and must log in again to gain access through the firewall.

Establishing User Connections with JavaScript

To verify client connections using the authentication proxy with JavaScript enabled on the client browser, follow this procedure:

- Step 1** From a client host, initiate an HTTP connection through the firewall. This generates the authentication proxy login page.
- Step 2** At the authentication proxy login page, enter a username and password.

Step 3 Click **OK** to submit the username and password to the AAA server.

A popup window appears indicating whether the login attempt succeeded or failed. If the authentication is successful, the connection is completed automatically. If the authentication fails, the authentication proxy reports the failure to the user and prompts the user with multiple retries.

**Note**

If the authentication attempt is unsuccessful after five attempts, the user must wait two minutes and initiate another HTTP session to trigger authentication proxy.

Establishing User Connections Without JavaScript

To ensure secure authentication, the authentication proxy design requires JavaScript. You can use the authentication proxy without enabling JavaScript on the browser, but this poses a potential security risk if users do not properly establish network connections. The following procedure provides the steps to properly establish a connection with JavaScript disabled. Network administrators are strongly advised to instruct users on how to properly establish connections using the procedure in this section.

**Note**

Failure to follow this procedure can cause user credentials to be passed to a network web server other than the authentication proxy or can cause the authentication proxy to reject the login attempt.

To verify client connections using the authentication proxy when JavaScript is not enabled on the client browser, follow this procedure:

Step 1 Initiate an HTTP connection through the firewall.

This generates the authentication proxy login page.

Step 2 From the authentication proxy login page at the client, enter the username and password.

Step 3 Click **OK** to submit the username and password to the AAA server.

A popup window appears indicating whether the login attempt succeeded or failed. If the popup window indicates successful authentication, go to [Step 7](#).

Step 4 If the popup window displays a failed authentication message, click **Close** on the browser **File** menu.

**Note**

Do not click **Reload** (**Refresh** for Internet Explorer) to close the popup window.

Step 5 From the original authentication login page, click **Reload** (**Refresh** for Internet Explorer) on the browser toolbar. The user login credentials are cleared from the form.

**Note**

Do not click **OK**. You must click **Reload** or **Refresh** to clear the username and password and to reload the form before attempting to log in again.

Step 6 Enter the username and password again.

If the authentication is successful, a window appears displaying a successful authentication message. If the window displays a failed authentication message, go to [Step 4](#).

Step 7 Click **Close** on the browser **File** menu.

Step 8 From the original authentication proxy login page, click **Reload** (**Refresh** for Internet Explorer) on the browser toolbar.

The authentication proxy completes the authenticated connection with the web server.

Monitoring and Maintaining the Authentication Proxy

This section describes how to view dynamic access list entries and how to manually remove authentication entries. This section contains the following sections:

- [Displaying Dynamic ACL Entries](#)
- [Deleting Authentication Proxy Cache Entries](#)

Displaying Dynamic ACL Entries

You can display dynamic access list entries when they are in use. After an authentication proxy entry is cleared by you or by the idle timeout parameter, you can no longer display it. The number of matches displayed indicates the number of times the access list entry was hit.

To view dynamic access lists and any temporary access list entries that are currently established by the authentication proxy, use the **show ip access-lists** command in privileged EXEC mode:

Command	Purpose
router# show ip access-lists	Displays the standard and extended access lists configured on the firewall, including dynamic ACL entries.

Consider the following example where ACL 105 is applied inbound at the input interface where you configure authentication proxy. The initial display shows the contents of the ACLs prior to authentication. The second display shows the same displays after user authentication with the AAA server.



Note

If NAT is configured, the **show ip access list** command might display the translated host IP address for the dynamic ACL entry or the IP address of the host initiating the connection. If the ACL is applied on the NAT outside interface, the translated address is displayed. If the ACL is applied on the NAT inside interface, the IP address of the host initiating the connection is displayed. The **show ip auth-proxy cache** command always displays the IP address of the host initiating the connection.

For example, the following is a list of ACL entries prior to the authentication proxy:

```
Router# show ip access-lists
.
.
.
Extended IP access list 105
deny tcp any any eq telnet
deny udp any any
permit tcp any any (28 matches)
permit ip any any
```

The following sample output shows a list of ACL entries following user authentication:

```
Router# show ip access-lists
.
.
.
Extended IP access list 105
! The ACL entries following user authentication are shown below.
permit tcp host 192.168.25.215 any eq 26
permit icmp host 192.168.25.215 host 60.0.0.2
permit tcp host 192.168.25.215 any eq telnet
permit tcp host 192.168.25.215 any eq ftp
permit tcp host 192.168.25.215 any eq ftp-data
permit tcp host 192.168.25.215 any eq smtp
deny tcp any any eq telnet
deny udp any any
permit tcp any any (76 matches)
permit ip any any
```

Deleting Authentication Proxy Cache Entries

When the authentication proxy is in use, dynamic access lists dynamically grow and shrink as authentication entries are added and deleted. To display the list of authentication entries, use the **show ip auth-proxy cache** command. To manually delete an authentication entry, use the **clear ip auth-proxy cache** command in privileged EXEC mode:

Command	Purpose
router# clear ip auth-proxy cache { * host ip address }	Deletes authentication proxy entries from the firewall before they time out. Use an asterisk to delete all authentication cache entries. Enter a specific IP address to delete an entry for a single host.

Authentication Proxy Configuration Examples

Configuring the authentication proxy feature requires configuration changes on both the router and the AAA server. The following sections provide authentication proxy configuration examples:

- [Authentication Proxy Configuration Example](#)
- [Authentication Proxy, IPSec, and CBAC Configuration Example](#)
- [Authentication Proxy, IPSec, NAT, and CBAC Configuration Example](#)
- [AAA Server User Profile Example](#)

Throughout these examples, the exclamation point (!) indicates a comment line. Comment lines precede the configuration entries being described.

Authentication Proxy Configuration Example

The following examples highlight the specific authentication proxy configuration entries. These examples do not represent a complete router configuration. Complete router configurations using the authentication proxy are included later in this chapter.

This section contains the following examples:

- [AAA Configuration Example](#)
- [HTTP Server Configuration Example](#)
- [Authentication Proxy Configuration Example](#)
- [Interface Configuration Example](#)

AAA Configuration Example

```
aaa new-model
aaa authentication login default group tacacs group radius
! Set up the aaa new model to use the authentication proxy.
aaa authorization auth-proxy default group tacacs group radius
! Define the AAA servers used by the router.
aaa accounting auth-proxy default start-stop group tacacs+
! Set up authentication proxy with accounting.
tacacs-server host 172.31.54.143
tacacs-server key cisco
radius-server host 172.31.54.143
radius-server key cisco
```

HTTP Server Configuration Example

```
! Enable the HTTP server on the router.
ip http server
! Set the HTTP server authentication method to AAA.
ip http authentication aaa
! Define standard access list 61 to deny any host.
access-list 61 deny any
! Use ACL 61 to deny connections from any host to the HTTP server.
ip http access-class 61
```

Authentication Proxy Configuration Example

```
! Set the global authentication proxy timeout value.
ip auth-proxy auth-cache-time 60
! Apply a name to the authentication proxy configuration rule.
ip auth-proxy name HQ_users http
```

Interface Configuration Example

```
! Apply the authentication proxy rule at an interface.
interface e0
 ip address 10.1.1.210 255.255.255.0
 ip auth-proxy HQ_users
```

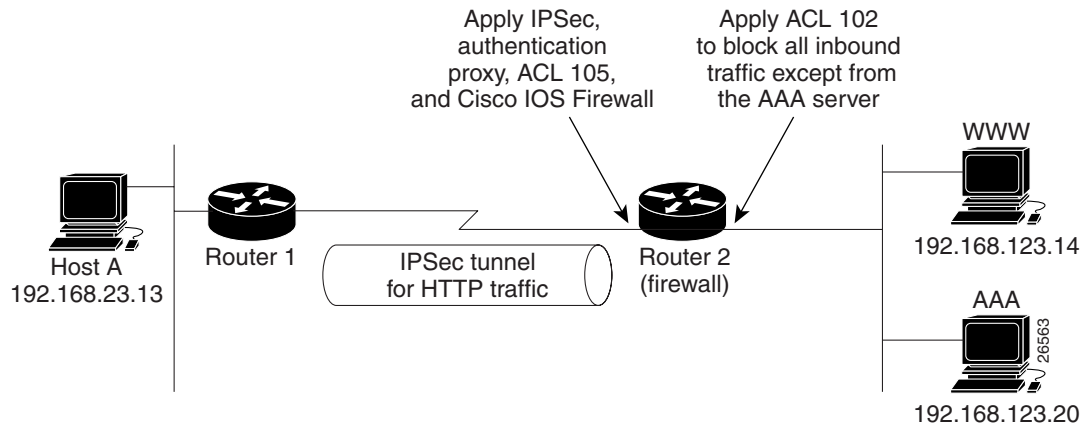
Authentication Proxy, IPSec, and CBAC Configuration Example

The following example shows a router configuration with the authentication proxy, IPSec, and CBAC features. [Figure 47](#) illustrates the configuration.

**Note**

If you are using this feature with Cisco IOS software release 12.3(8)T or later, see the document [Crypto Access Check on Clear-Text Packets](#) (feature module, release 12.3(8)T).

Figure 47 Authentication Proxy, IPSec, and CBAC Configuration Example



In this example, Host A initiates an HTTP connection with the web server (WWW). The HTTP traffic between Router 1 and Router 2 is encrypted using IPSec. The authentication proxy, IPSec, and CBAC are configured at interface Serial0 on Router 2, which is acting as the firewall. ACL 105 blocks all traffic at interface Serial0. ACL 102 is applied at interface Ethernet0 on Router 2 to block all traffic on that interface except traffic from the AAA server.

When Host A initiates an HTTP connection with the web server, the authentication proxy prompts the user at Host A for a username and password. These credentials are verified with the AAA server for authentication and authorization. If authentication is successful, the per-user ACLs are downloaded to the firewall to permit services.

The following examples provide both the Router 1 and Router 2 configurations for completeness:

- [Router 1 Configuration Example](#)
- [Router 2 Configuration Example](#)

Router 1 Configuration Example

```

! Configure Router 1 for IPSec.
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router1
!
logging buffered 4096 debugging
no logging console
enable secret 5 $1$E00B$AQF1vFZM3fLr3LQA0sudL/
enable password junk
!
username Router2 password 0 welcome
crypto isakmp policy 1
authentication pre-share
  
```

```

crypto isakmp key cisco1234 address 10.0.0.2
!
crypto ipsec transform-set rule_1 ah-sha-hmac esp-des esp-sha-hmac
!
!
crypto map testtag 10 ipsec-isakmp
set peer 10.0.0.2
set transform-set rule_1
match address 155
!
interface Ethernet0/0
ip address 192.168.23.2 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface Serial3/1
ip address 10.0.0.1 255.0.0.0
no ip directed-broadcast
encapsulation PPP
ip route-cache
no ip mroute-cache
no keepalive
no fair-queue
clockrate 56000
crypto map testtag
!
!
ip classless
ip route 192.168.123.0 255.255.255.0 10.0.0.2
! Identify the IPSec specific traffic.
access-list 155 permit tcp host 192.168.23.13 host 192.168.123.14 eq www
access-list 155 permit tcp host 192.168.23.13 eq www host 192.168.123.14

```

Router 2 Configuration Example

```

! Configure Router 2 as the firewall, using the authentication proxy, IPSec, and CBAC.
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router2
!
logging buffered 4096 debugging
aaa new-model
aaa authentication login default group tacacs
aaa authentication login console_line none
aaa authentication login special none
aaa authentication ppp default group tacacs
aaa authorization exec default group tacacs
! Configure AAA for the authentication proxy.
aaa authorization auth-proxy default group tacacs+
enable password junk
!
! Create the CBAC inspection rule HTTP_TEST.
ip inspect name rule22 http
ip inspect name rule22 tcp
ip inspect name rule22 ftp
ip inspect name rule22 smtp
!
! Create the authentication proxy rule PXY.

```

```

ip auth-proxy name pxy http
! Turn on display of the router name in the authentication proxy login page.
ip auth-proxy auth-proxy-banner
ip audit notify log
ip audit po max-events 100
!
! Configure IPsec.
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco1234 address 10.0.0.1
!
crypto ipsec transform-set rule_1 ah-sha-hmac esp-des esp-sha-hmac
!
crypto map testtag 10 ipsec-isakmp
 set peer 10.0.0.1
 set transform-set rule_1
 match address 155
!
! Apply the CBAC inspection rule and the authentication proxy rule at interface
! Serial0/0.
interface Serial0/0
 ip address 10.0.0.2 255.0.0.0
 ip access-group 105 in
 no ip directed-broadcast
 ip inspect rule22 in
 ip auth-proxy pxy
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 no keepalive
 no fair-queue
 crypto map testtag
!
interface Ethernet0/1
 ip address 192.168.123.2 255.255.255.0
 ip access-group 102 in
 no ip directed-broadcast
 ip route-cache
 no ip mroute-cache
!
no ip classless
ip route 192.168.23.0 255.255.255.0 10.0.0.1
ip route 192.168.50.0 255.255.255.0 16.0.0.1
! Configure the HTTP server.
ip http server
ip http access-class 15
ip http authentication aaa
!
! Create ACL 15 to block all traffic for the http server.
access-list 15 deny any
! Create ACL 102 to block all traffic inbound on interface Ethernet0/1 except for
! traffic from the AAA server.
access-list 102 permit tcp host 192.168.123.20 eq tacacs host 192.168.123.2
access-list 102 deny tcp any any
access-list 102 deny udp any any
access-list 102 permit ip any any
! Create ACL 105 to block all traffic inbound on interface Serial0/0. Permit only IP
! protocol traffic.
access-list 105 deny tcp any any
access-list 105 deny udp any any
access-list 105 permit ip any any
! Identify the IPsec specific traffic.
access-list 155 permit tcp host 192.168.123.14 host 192.168.23.13 eq www
access-list 155 permit tcp host 192.168.123.14 eq www host 192.168.23.13

```

```

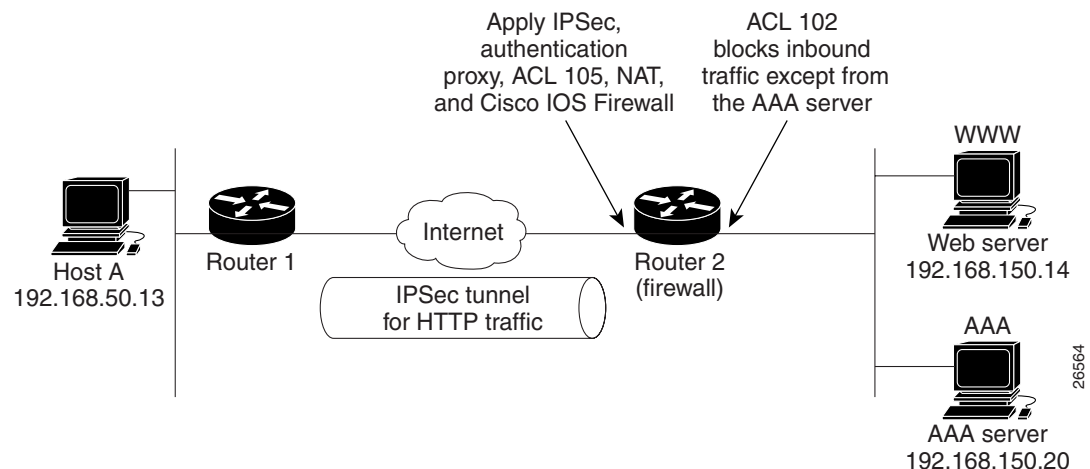
!
! Define the AAA server host and encryption key.
tacacs-server host 192.168.123.14
tacacs-server key cisco
!
line con 0
  exec-timeout 0 0
  login authentication special
  transport input none
line aux 0
  transport input all
  speed 38400
  flowcontrol hardware
line vty 0 4
  password lab

```

Authentication Proxy, IPSec, NAT, and CBAC Configuration Example

The following example provides a router configuration with the authentication proxy, IPSec, NAT, and CBAC features. [Figure 48](#) illustrates the configuration.

Figure 48 Authentication Proxy, IPSec, and CBAC Configuration Example



In this example, Host A initiates an HTTP connection with the web server (WWW). The HTTP traffic between router 1 (interface BRI0) and router 2 (interface Serial2) is encrypted using IPSec. The authentication proxy is configured on router 2, which is acting as the firewall. The authentication proxy, NAT, and CBAC are configured at interface Serial2, which is acting as the firewall. ACL 105 blocks all traffic at interface Serial2. ACL 102 is applied at interface Ethernet0 on router 2 to block all traffic on that interface except traffic from the AAA server. In this example, the authentication proxy uses standard ACL 10 to specify the hosts using the authentication proxy feature.

When any host in ACL 10 initiates an HTTP connection with the web server, the authentication proxy prompts the user at that host for a username and password. These credentials are verified with AAA server for authentication and authorization. If authentication is successful, the per-user ACLs are downloaded to the firewall to permit services.

The following examples provide both the router 1 and router 2 configurations for completeness:

- [Router 1 Configuration Example](#)

- [Router 2 Configuration Example](#)

Router 1 Configuration Example

```
! Configure router 1 for IPSec.
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router1
!
logging buffered 4096 debugging
no logging console
!
isdn switch-type basic-5ess
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco1234 address 16.0.0.2
crypto ipsec transform-set rule_1 ah-sha-hmac esp-des esp-sha-hmac
!
!
crypto map testtag 10 ipsec-isakmp
set peer 16.0.0.2
set transform-set rule_1
match address 155
!
!
process-max-time 200
!
interface BRI0
ip address 16.0.0.1 255.0.0.0
no ip directed-broadcast
encapsulation ppp
dialer idle-timeout 5000
dialer map ip 16.0.0.2 name router2 broadcast 50006
dialer-group 1
isdn switch-type basic-5ess
crypto map testtag
!
interface FastEthernet0
ip address 192.168.50.2 255.255.255.0
no ip directed-broadcast
!
ip classless
ip route 192.168.150.0 255.255.255.0 16.0.0.2
no ip http server
! Identify the IPSec specific traffic.
access-list 155 permit tcp host 192.168.50.13 host 192.168.150.100 eq www
access-list 155 permit tcp host 192.168.50.13 eq www host 192.168.150.100
dialer-list 1 protocol ip permit
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
password lab
login
```


Router 2 Configuration Example

```
! Configure router 2 as the firewall, using the authentication proxy, IPSec, NAT, and
! CBAC.
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router2
!
logging buffered 4096 debugging
aaa new-model
aaa authentication login default group tacacs+
aaa authentication login console_line none
aaa authorization exec default group tacacs+
! Configure AAA for the authentication proxy.
aaa authorization auth-proxy default group tacacs+
!
! Create the CBAC inspection rule "rule44."
ip inspect name rule44 http java-list 5
ip inspect name rule44 tcp
ip inspect name rule44 ftp
ip inspect name rule44 smtp
!
! Create the authentication proxy rule "pxy." Set the timeout value for rule
! pxy to three minutes. Standard ACL 10 is applied to the rule.
ip auth-proxy name pxy http list 10 auth-cache-time 3
isdn switch-type primary-5ess
!
! Configure IPSec.
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco1234 address 16.0.0.1
!
!
crypto ipsec transform-set rule_1 ah-sha-hmac esp-des esp-sha-hmac
!
!
crypto map testtag 10 ipsec-isakmp
 set peer 16.0.0.1
 set transform-set rule_1
 match address 155
!
controller T1 2/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
! Apply ACL 102 inbound at interface Ethernet0/1 and configure NAT.
interface Ethernet0/1
 ip address 192.168.150.2 255.255.255.0
 ip access-group 102 in
 no ip directed-broadcast
 ip nat inside
 no ip mroute-cache
!
! Apply the authentication proxy rule PXY, CBAC inspection rule HTTP_TEST, NAT, and
! and ACL 105 at interface Serial2/0:23.
interface Serial2/0:23
 ip address 16.0.0.2 255.0.0.0
 ip access-group 105 in
 no ip directed-broadcast
```

```

ip nat outside
ip inspect rule44 in
ip auth-proxy pxy
encapsulation ppp
ip mroute-cache
dialer idle-timeout 5000
dialer map ip 16.0.0.1 name router1 broadcast 71011
dialer-group 1
isdn switch-type primary-5ess
fair-queue 64 256 0
crypto map testtag
!
! Use NAT to translate the Web server address.
ip nat inside source static 192.168.150.14 192.168.150.100
ip classless
ip route 192.168.50.0 255.255.255.0 16.0.0.1
! Configure the HTTP server.
ip http server
ip http access-class 15
ip http authentication aaa
!
! Create standard ACL 5 to specify the list of hosts from which to accept java applets.
! ACL 5 is used to block Java applets in the CBAC inspection rule named "rule44," which
! is applied at interface Serial2/0:23.
access-list 5 permit any
! Create standard ACL 10 to specify the hosts using the authentication proxy. This ACL
! used in the authentication proxy rule named "PXY", which is applied at interface
! Serial2/0:23.
access-list 10 permit any
! Create ACL 15 to block all traffic for the http server.
access-list 15 deny any
! Create extended ACL 102 to block all traffic inbound on interface Ethernet0/1
! except for traffic from the AAA server.
access-list 102 permit tcp host 192.168.150.20 eq tacacs 192.168.150.2
access-list 102 deny tcp any any
access-list 102 deny udp any any
access-list 102 permit ip any any
! Create extended ACL 105 to block all TCP and UDP traffic inbound on interface
! Serial2/0:23.
access-list 105 deny tcp any any
access-list 105 deny udp any any
access-list 105 permit ip any any
! Identify the IPSec specific traffic.
access-list 155 permit tcp host 192.168.150.100 host 192.168.50.13 eq www
access-list 155 permit tcp host 192.168.150.100 eq www host 192.168.50.13
dialer-list 1 protocol ip permit
! Define the AAA server host and encryption key.
tacacs-server host 192.168.126.14
tacacs-server key cisco
!
line con 0
exec-timeout 0 0
! Define the AAA server host and encryption key.
login authentication console_line
transport input none
line aux 0
line vty 0 4
password lab
!
!
end

```

AAA Server User Profile Example

This section includes examples of the authentication proxy user profile entries on the AAA servers. The “proxyacl” entries define the user access privileges. After the user has successfully used the authentication proxy to log in, these entries are transferred to the firewall router. Each entry in the profile must specify “permit” access for the service or application. The source address in each entry is set to “any”, which is replaced with the IP address of the authenticating host when the profile is downloaded to the firewall. The privilege level must be set to 15 for all AAA users.

This section contains the following sections:

- [CiscoSecure ACS 2.3 for Windows NT](#)
- [CiscoSecure ACS 2.3 for UNIX](#)
- [TACACS+ Server](#)
- [Livingston Radius Server](#)
- [Ascend Radius Server](#)

CiscoSecure ACS 2.3 for Windows NT

This section describes how to configure authentication proxy on CiscoSecure ACS 2.3 for Windows NT. For detailed information about CiscoSecure ACS, refer to the documentation for that product.

The following sample configuration is for the TACACS+ service of CiscoSecure ACS for Windows NT.

-
- Step 1** Click the Interface Configuration icon and click **TACACS+ (Cisco)**.
- a. Scroll down to New Services.
 - b. Add a new service, “auth-proxy”, in the Service field. Leave the Protocol field empty.
 - c. Select both the User and Group check boxes for the new service.
 - d. Scroll down to Advance Configuration Options and check the Per-user Advance TACACS+ features.
 - e. Click **Submit**.
- Step 2** Click the Network Configuration icon.
- a. Click the Add Entry icon for Network Access Servers and fill in the Network Access Server Hostname, IP address, and key (the key configured on the router) fields.
 - b. Select TACACS+ (Cisco) for the Authenticate Using option.
 - c. Click the Submit + Restart icon.
- Step 3** Click the Group Setup icon.
- a. Select a user group from the drop-down menu.
 - b. Select the Users in Group check box.
 - c. Select a user from the user list.
 - d. In the User Setup list, scroll down to TACACS+ Settings and select the “auth-proxy” check box.
 - e. Select the Custom Attributes check box.
 - f. Add the profile entries (do not use single or double quotes around the entries) and set the privilege level to 15.

```
priv-lvl=15
proxyacl#1=permit tcp any any eq 26
```

```

proxyacl#2=permit icmp any host 60.0.0.2
proxyacl#3=permit tcp any any eq ftp
proxyacl#4=permit tcp any any eq ftp-data
proxyacl#5=permit tcp any any eq smtp
proxyacl#6=permit tcp any any eq telnet

```

g. Click **Submit**.

Step 4 Click the User Setup icon.

a. Click **List All Users**.

b. Add a username.

c. Scroll down to User Setup Password Authentication.

d. Select SDI SecurID Token Card from the Password Authentication drop-down menu.

e. Select the previous configured user group 1.

f. Click **Submit**.

Step 5 Click Group Setup icon again.

a. Select the user group 1.

b. Click **Users in Group**.

c. Click **Edit Settings**.

d. Click the Submit + Restart icon to make sure the latest configuration is updated and sent to the AAA server.

CiscoSecure ACS 2.3 for UNIX

This section describes how to configure authentication proxy on CiscoSecure ACS 2.3 for UNIX. For detailed information regarding CiscoSecure ACS, refer to the documentation for that product.

To manage the CiscoSecure ACS using the Administrator program, you need a web browser that supports Java and JavaScript. You must enable Java in the browser application. You can start the Java-based CiscoSecure Administrator advanced configuration program from any of the CiscoSecure ACS Administrator web pages.

The following sample configuration procedure is for the TACACS+ service of CiscoSecure ACS 2.3 for UNIX.

Step 1 On the CiscoSecure ACS web menu bar of the CiscoSecure ACS web interface, click **Advanced** and then click **Advanced** again.

The Java-based CiscoSecure Administrator advanced configuration program appears. It might require a few minutes to load.

Step 2 In the CiscoSecure Administrator advanced configuration program, locate and deselect Browse in the Navigator pane of the tabbed Members page.

This displays the Create New Profile icon.

Step 3 In the Navigator pane, do one of the following:

- Locate and click the group to which the user will belong.
- If you do not want the user to belong to a group, click the [Root] folder icon.

- Step 4** Click **Create Profile** to display the New Profile dialog box.
- Step 5** Make sure the Group check box is cleared.
- Step 6** Enter the name of the user you want to create and click **OK**. The new user appears in the tree.
- Step 7** Click the icon for the group or user profile in the tree that is displayed in the Navigator pane of the tabbed Members page.
- Step 8** If necessary, in the Profile pane, click the Profile icon to expand it.
A list or dialog box that contains attributes applicable to the selected profile or service appears in the window at the bottom right of the screen. The information in this window changes depending on what you have selected in the Profile pane.
- Step 9** Click **Service-String**.
- Step 10** Click **string**, enter **auth-proxy** in the text field, and click **Apply**.
- Step 11** Select the **Option** menu.
- Step 12** On the **Option** menu, click **Default Attributes**.
- Step 13** Change the attribute from Deny to **Permit**.
- Step 14** Click **Apply**.
- Step 15** On the **Option** menu, click **Attribute** and enter the privilege level in the text field:
`priv-lvl=15`
- Step 16** On the **Option** menu, click **Attribute** and enter the **proxyacl** entries in the text field:
`proxyacl#1="permit tcp any any eq 26"`

Repeat this step for each additional service or protocol to add:
`proxyacl#2="permit icmp any host 60.0.0.2"`
`proxyacl#3="permit tcp any any eq ftp"`
`proxyacl#4="permit tcp any any eq ftp-data"`
`proxyacl#5="permit tcp any any eq smtp"`
`proxyacl#6="permit tcp any any eq telnet"`
- Step 17** When you have finished making all your changes, click **Submit**.

TACACS+ Server

```
default authorization = permit
key = cisco
user = Brian {
login = cleartext cisco
service = auth-proxy
{
priv-lvl=15
proxyacl#1="permit tcp any any eq 26"
proxyacl#2="permit icmp any host 60.0.0.2"
proxyacl#3="permit tcp any any eq ftp"
proxyacl#4="permit tcp any any eq ftp-data"
proxyacl#5="permit tcp any any eq smtp"
proxyacl#6="permit tcp any any eq telnet"
}
}
```

Livingston Radius Server

```
Bob Password = "cisco" User-Service-Type=Outbound-User
cisco-avpair = "auth-proxy:priv-lvl=15",
cisco-avpair = "auth-proxy:proxyacl#1=permit tcp any any eq 26",
cisco-avpair = "auth-proxy:proxyacl#2=permit icmp any host 60.0.0.2",
cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq ftp",
cisco-avpair = "auth-proxy:proxyacl#4=permit tcp any any eq ftp-data",
cisco-avpair = "auth-proxy:proxyacl#5=permit tcp any any eq smtp",
cisco-avpair = "auth-proxy:proxyacl#6=permit tcp any any eq telnet"
```

Ascend Radius Server

```
Alice Password = "cisco" User-Service = Dialout-Framed-User
cisco-avpair = "auth-proxy:priv-lvl=15",
cisco-avpair = "auth-proxy:proxyacl#1=permit tcp any any eq 26",
cisco-avpair = "auth-proxy:proxyacl#2=permit icmp any host 60.0.0.2",
cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq ftp",
cisco-avpair = "auth-proxy:proxyacl#4=permit tcp any any eq ftp-data",
cisco-avpair = "auth-proxy:proxyacl#5=permit tcp any any eq smtp",
cisco-avpair = "auth-proxy:proxyacl#6=permit tcp any any eq telnet"
```

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Consent Feature for Cisco IOS Routers

First Published: July 19, 2007

Last Updated: July 19, 2007

The Consent Feature for Cisco IOS Routers enables organizations to provide temporary Internet and corporate access to end users through their wired and wireless networks by presenting a consent webpage. This webpage lists the terms and conditions in which the organization is willing to grant requested access to an end user. Users can connect to the network only after they accept the terms of use on the consent webpage.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Authentication Proxy with Consent Support](#)” section on page 32.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Consent Feature for Cisco IOS Routers, page 2](#)
- [Information About Consent Feature for Cisco IOS Routers, page 2](#)
- [How to Configure Authentication Proxy Consent, page 3](#)
- [Configuration Examples for Authentication Proxy Consent, page 8](#)
- [Additional References, page 10](#)
- [Command Reference, page 11](#)
- [Feature Information for Authentication Proxy with Consent Support, page 32](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for Consent Feature for Cisco IOS Routers

To enable a consent webpage, you must be running an Advanced Enterprise image.

Information About Consent Feature for Cisco IOS Routers

Before enabling the consent feature for Cisco IOS routers, you should understand the following concepts:

- [Authentication Proxy Overview, page 2](#)
- [An Integrated Consent–Authentication Proxy Webpage, page 2](#)

Authentication Proxy Overview

Authentication proxy is an ingress authentication feature that grants access to an end user (out an interface) only if the user submits valid username and password credentials for an ingress traffic that is destined for HTTP, Telnet, or FTP protocols. After the submitted authentication credentials have been checked against the credentials that are configured on an Authentication, Authorization, Accounting (AAA) server, access is granted to the requester (source IP address).

When an end user posts an HTTP(S), FTP, or Telnet request on a router's authentication-proxy-enabled ingress interface, the Network Authenticating Device (NAD) verifies whether or not the same host has already been authenticated. If a session is already present, the ingress request is not authenticated again, and it is subjected to the dynamic (Auth-Proxy) ACEs and the ingress interface ACEs. If an entry is not present, the authentication proxy responds to the ingress connection request by prompting the user for a valid username and password. When authenticated, the Network Access Profiles (NAPs) that are to be applied are either downloaded from the AAA server or taken from the locally configured profiles.

An Integrated Consent–Authentication Proxy Webpage

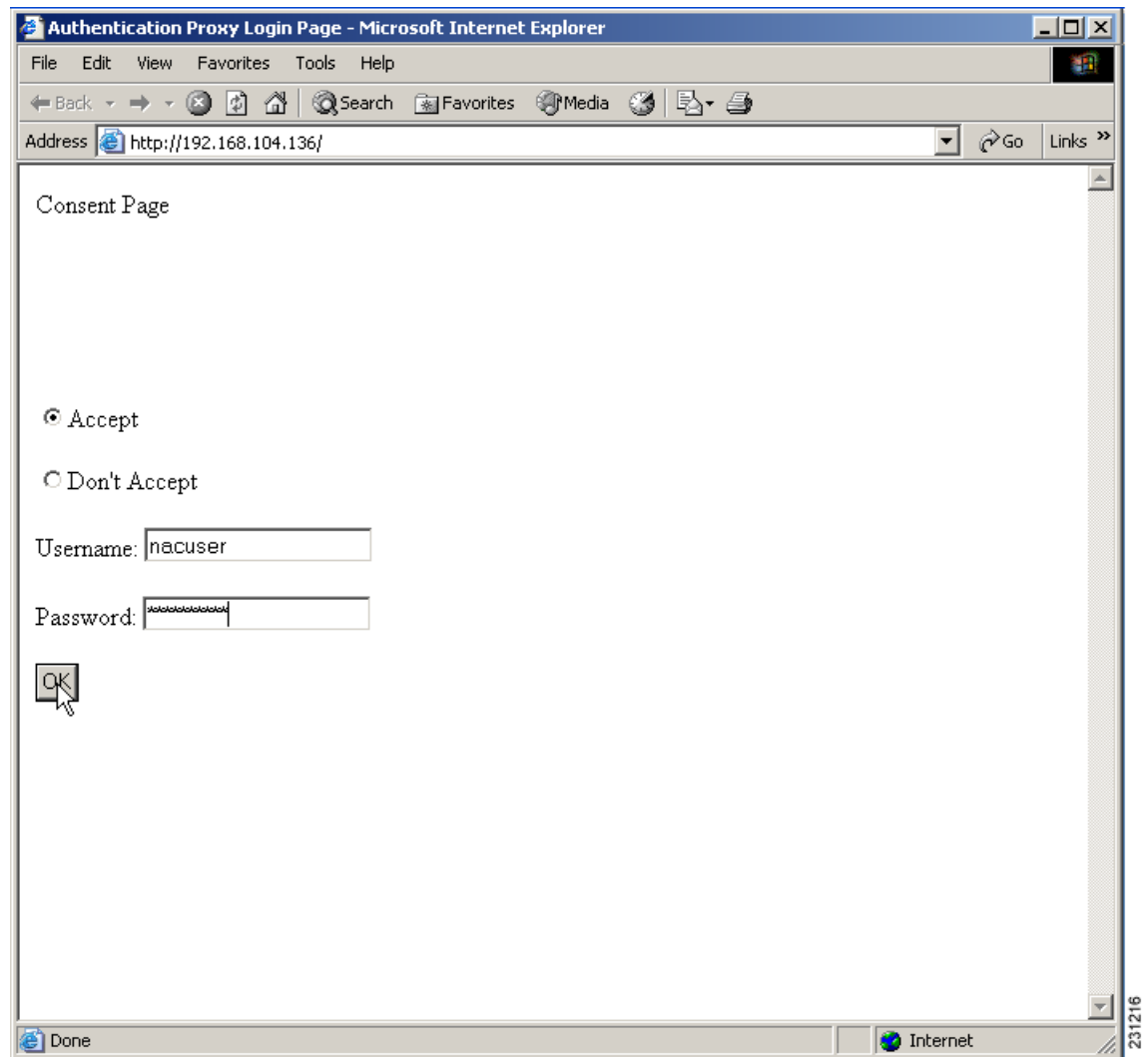
The HTTP authentication proxy webpage has been extended to support radio buttons—"Accept" and "Don't Accept"—for the consent webpage feature. The consent webpage radio buttons are followed by the authentication proxy input fields for a username and a password. (See [Figure 1](#).)

The following consent scenarios are possible:

- If consent is declined (that is, the "Don't Accept" radio button is selected), the authentication proxy radio buttons are disabled. The ingress client session's access will be governed by the default ingress interface ACL.
- If consent is accepted (that is, the "Accept" radio button is selected), the authentication proxy radio buttons are enabled. If the wrong username and password credentials are entered, HTTP-Auth-Proxy authentication will fail. The ingress client session's access will again be governed only by the default ingress interface ACL.
- If consent is accepted (that is, the "Accept" radio button is selected) and valid username and password credentials are entered, HTTP-Auth-Proxy authentication is successful. Thus, one of the following possibilities can occur:
 - If the ingress client session's access request is HTTP_GET, the destination webpage will open and the ingress client session's access will be governed by the default ingress interface ACL and the dynamic (Auth-Proxy) ACEs.

- If the ingress client session's access request is HTTPS_GET, a "Security Dialogue Box" will be displayed on the client's browser. If the user selects YES on the Security Dialogue Box window, the destination webpage will open and the ingress client session's access will be governed by the default ingress interface ACL and the dynamic (Auth-Proxy) ACEs. If the user selects NO on the Security Dialogue Box window, the destination page will not open and the user will see the message "Page cannot be displayed." However the ingress client session's access will still be governed by the default ingress interface ACL and the dynamic (Auth-Proxy) ACEs.

Figure 1 **Consent WebPage: Example**



How to Configure Authentication Proxy Consent

Use the following tasks to configure a consent webpage and enable a consent webpage that is to be displayed to end users:

- [Configuring an IP Admission Rule for Authentication Proxy Consent, page 4](#)
- [Defining a Parameter Map for Authentication Proxy Consent, page 6](#)

Configuring an IP Admission Rule for Authentication Proxy Consent

Use this task to define the IP admission rule for authentication proxy consent and to associate the rule with an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission name** *admission-name* **consent** [[**absolute-timer** *minutes*] [**event**] [**inactivity-time** *minutes*] [**list** {*acl* | *acl-name*}] [**parameter-map** *consent-parameter-map-name*]]
4. **ip admission consent banner** [**file** *file-name* | **text** *banner-text*]
5. **interface** *type number*
6. **ip admission** *admission-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip admission name <i>admission-name</i> consent [[absolute-timer <i>minutes</i>] [event] [inactivity-time <i>minutes</i>] [list { <i>acl</i> <i>acl-name</i> }] [parameter-map <i>consent-parameter-map-name</i>] Example: Router(config)# ip admission name consent_rule consent absolute-timer 304 list 103 inactivity-time 204 parameter-map consent_parameter_map	Defines the IP admission rule for authentication proxy consent.
Step 4	ip admission consent banner [file <i>file-name</i> text <i>banner-text</i>] Example: Router(config)# ip admission consent banner file flash:consent_page.html	(Optional) Displays a banner in the authentication proxy consent webpage.
Step 5	interface <i>type number</i> Example: Router(config)# interface FastEthernet 0/0	Specifies the interface in which the consent IP admission rule will be applied and enters interface configuration mode.
Step 6	ip admission <i>admission-name</i> Example: Router(config-if)# ip admission consent_rule	Applies the IP admission rule created in Step 3 to an interface.

Troubleshooting Tips

To display authentication proxy consent page information on the router, you can use the **debug ip admission consent** command.

```
Router# debug ip admission consent errors
IP Admission Consent Errors debugging is on
```

```
Router# debug ip admission consent events
IP Admission Consent Events debugging is on
```

```
Router# debug ip admission consent messages
IP Admission Consent Messages debugging is on
Router#
Router# show debugging
```

```
IP Admission Consent:  
IP Admission Consent Errors debugging is on  
IP Admission Consent Events debugging is on  
IP Admission Consent Messages debugging is on
```

Defining a Parameter Map for Authentication Proxy Consent

Use this task to define a parameter map that is to be used for authentication proxy consent.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type consent** *parameter-map-name*
4. **copy** *src-file-name* *dst-file-name*
5. **file** *file-name*
6. **authorize accept identity** *identity-policy-name*
7. **timeout file download** *minutes*
8. **logging enabled**
9. **exit**
10. **show parameter-map type consent** [*parameter-map-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	parameter-map type consent <i>parameter-map-name</i> Example: Router(config)# parameter-map type consent consent_parameter_map	Defines an authentication proxy consent-specific parameter map and enters parameter-map type consent configuration mode. To use a default policy-map, enter default for the parameter-map-name.
Step 4	copy <i>src-file-name</i> <i>dst-file-name</i> Example: Router(config-profile)# copy tftp://192.168.104.136/consent_page.html flash:consent_page.html	Transfers a file (consent webpage) from an external server to a local file system on your device.
Step 5	file <i>file-name</i> Example: Router(config-profile)# file flash:consent_page.html	(Optional) Specifies a local filename that is to be used as the consent webpage.
Step 6	authorize accept identity <i>identity-policy-name</i> Example: Router(config-profile)# authorize accept identity consent_identity_policy	(Optional) Configures an accept policy. Note Currently, only an accept policy can be configured.
Step 7	timeout file download <i>minutes</i> Example: Router(config-profile)# timeout file download 35791	(Optional) Specifies how often the consent page file should be downloaded from the external TFTP server.
Step 8	logging enabled Example: Router(config-profile)# logging enabled	(Optional) Enables syslog messages.

	Command or Action	Purpose
Step 9	exit Example: Router(config-profile) # exit Router(config) # exit	Returns to global configuration and privileged EXEC modes.
Step 10	show parameter-map type consent [parameter-map-name] Example: Router# show parameter-map type consent	(Optional) Displays all or a specified configured consent profiles.

Configuration Examples for Authentication Proxy Consent

This section contains the following configuration examples:

- [Ingress Interface ACL and Intercept ACL Configuration: Example, page 8](#)
- [Consent Page Policy Configuration: Example, page 9](#)
- [Parameter Map Configuration: Example, page 9](#)
- [IP Admission Consent Rule Configuration: Example, page 9](#)

Ingress Interface ACL and Intercept ACL Configuration: Example

The following example shows how to define the ingress interface ACL (via the **ip access-list extended 102** command) to which the consent page policy ACEs will be dynamically appended. This example also shows how to define an intercept ACL (via the **ip access-list extended 103** command) to intercept the ingress interesting traffic by the IP admission consent rule.

```
ip access-list extended 102
 permit ip any 192.168.100.0 0.0.0.255
 permit ip any host 192.168.104.136
 permit udp any any eq bootps
 permit udp any any eq domain
 permit tcp any any eq www
 permit tcp any any eq 443
 permit udp any any eq 443
 exit
!
ip access-list extended 103
 permit ip any host 192.168.104.136
 permit udp any host 192.168.104.132 eq domain
 permit tcp any host 192.168.104.136 eq www
 permit udp any host 192.168.104.136 eq 443
 permit tcp any host 192.168.104.136 eq 443
 exit
!
```

Consent Page Policy Configuration: Example

The following example shows how to configure the consent page policy ACL, the consent page identity policy, and the URL redirect ACL:

```
ip access-list extended consent-pg-ip-acc-group
 permit ip any host 192.168.104.128
 permit ip any host 192.168.104.136
 exit
!
identity policy consent_identity_policy
 description ### Consent Page Identity Policy ###
 access-group consent-pg-ip-acc-group
 exit
!
ip access-list extended url-redirect-acl
 permit tcp any host 192.168.104.136 eq www
 permit tcp any host 192.168.104.136 eq 443
 exit
```

Parameter Map Configuration: Example

The following example shows how to define the consent-specific parameter map “consent_parameter_map” and a default consent parameter map:

```
parameter-map type consent consent_parameter_map
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity consent_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
parameter-map type consent default
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity test_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
```

IP Admission Consent Rule Configuration: Example

The following example shows how to configure an IP admission consent rule, which includes the consent page parameter map as defined the in the [“Parameter Map Configuration: Example”](#) section:

```
ip admission name consent-rule consent inactivity-time 204 absolute-timer 304 param-map
 consent_parameter_map list 103
ip admission consent-banner file flash:consent_page.html
ip admission consent-banner text ^C Consen-Page-Banner-Text ^C
ip admission max-login-attempts 5
ip admission init-state-timer 15
ip admission auth-proxy-audit
ip admission inactivity-timer 205
ip admission absolute-timer 305
ip admission ratelimit 100
ip http server
ip http secure-server
```

```
!  
interface FastEthernet 0/0  
  description ### CLIENT-N/W ###  
  ip address 192.168.100.170 255.255.255.0  
  ip access-group 102 in  
  ip admission consent-rule  
  no shut  
  exit  
!  
interface FastEthernet 0/1  
  description ### AAA-DHCP-AUDIT-SERVER-N/W ###  
  ip address 192.168.104.170 255.255.255.0  
  no shut  
  exit  
!  
line con 0  
  exec-timeout 0 0  
  login authentication noAAA  
  exit  
!  
line vty 0 15  
  exec-timeout 0 0  
  login authentication noAAA  
  exit  
!
```

Additional References

The following sections provide references related to the Consent Feature for Cisco IOS Routers feature.

Related Documents

Related Topic	Document Title
Additional authentication proxy configuration tasks	The chapter “ Configuring Authentication Proxy ” in the <i>Cisco IOS Security Configuration Guide</i>

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **authorize accept identity**
- **copy (consent-parameter-map)**
- **debug ip admission consent**
- **file (consent-parameter-map)**
- **ip admission consent banner**
- **ip admission name**
- **logging enabled**
- **parameter-map type**
- **show ip admission**
- **timeout file download**
- **Feature Information for Authentication Proxy with Consent Support**

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Firewall Support of HTTPS Authentication Proxy

The Firewall Support of HTTPS Authentication Proxy feature allows a user to encrypt the change of the username and password between the HTTP client and the Cisco IOS router via Secure Socket Layer (SSL) when authentication proxy is enabled on the Cisco IOS firewall, thereby ensuring confidentiality of the data passing between the HTTP client and the Cisco IOS router.

Feature Specifications for the Firewall Support of HTTPS Authentication Proxy feature

Feature History

Release	Modification
12.2(11)YU	This feature was introduced.
12.2(15)T	This feature was integrated into Cisco IOS Release 12.2(15)T.

Supported Platforms

For platforms supported in Cisco IOS Releases 12.2(11)YU and 12.2(15)T, consult Cisco Feature Navigator.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Firewall Support of HTTPS Authentication Proxy, page 2](#)
- [Restrictions for Firewall Support of HTTPS Authentication Proxy, page 2](#)
- [Information About Firewall Support of HTTPS Authentication Proxy, page 2](#)
- [How to Use HTTPS Authentication Proxy, page 4](#)
- [Monitoring Firewall Support of HTTPS Authentication Proxy, page 6](#)
- [Additional References, page 12](#)
- [Command Reference, page 14](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Glossary, page 15](#)

Prerequisites for Firewall Support of HTTPS Authentication Proxy

Before enabling this feature, ensure that your router is running a crypto image with k8 and k9 designations and that your Cisco IOS image supports SSL.

Restrictions for Firewall Support of HTTPS Authentication Proxy

- Although Port to Application Mapping (PAM) configuration is allowed in Cisco IOS Firewall processing, authentication proxy is limited to the server ports that are configured by the HTTP subsystem of the router.
- To conform to a proper TCP connection handshake, the authentication proxy login page will be returned from the same port and address as the original request. Only the postrequest, which contains the username and password of the HTTP client, will be forced to use HTTP over SSL (HTTPS).

Information About Firewall Support of HTTPS Authentication Proxy

To configure the Firewall Support of HTTPS Authentication Proxy feature, you must understand the following concepts:

- [Authentication Proxy, page 2](#)
- [Feature Design for HTTPS Authentication Proxy, page 3](#)

Authentication Proxy

Authentication proxy grants Internet access to an authorized user through the Cisco Secure Integrated Software (also known as a Cisco IOS firewall). Access is granted on a per-user basis after the proper identification process is completed and the user policies are retrieved from a configured authentication, authorization, and accounting (AAA) server.

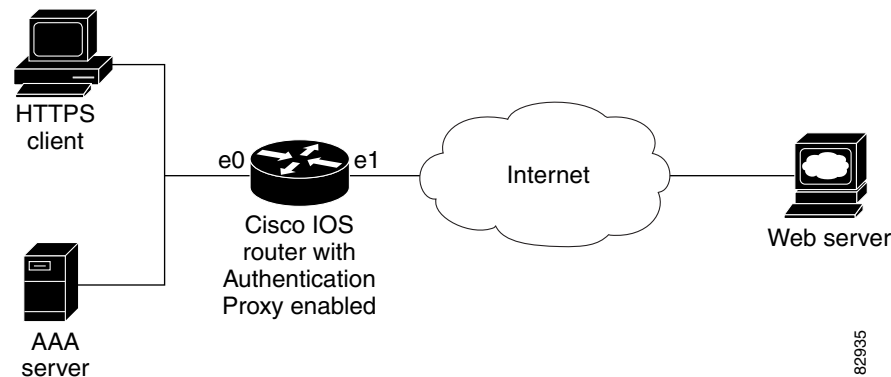
When authentication proxy is enabled on a Cisco router, users can log into the network or access the Internet via HTTP(S). When a user initiates an HTTP(S) session through the firewall, the authentication proxy is triggered. Authentication proxy first checks to see if the user has been authenticated. If a valid authentication entry exists for the user, the connection is completed with no further intervention by authentication proxy. If no entry exists, the authentication proxy responds to the HTTP(S) connection request by prompting the user for a username and password. When authenticated, the specific access profiles are automatically retrieved and applied from a CiscoSecure Access Control Server (ACS), or other RADIUS or TACACS+ authentication server. The user profiles are active only when there is active traffic from the authenticated users.

Feature Design for HTTPS Authentication Proxy

Authentication proxy support using HTTPS provides encryption between the HTTPS client and the Cisco IOS router during the username and password exchange, ensuring secure communication between trusted entities.

Figure 49 and the corresponding steps explain how the data flows from the time the client issues a HTTP request to the time the client receives a response from the Cisco IOS router.

Figure 49 *HTTPS Authentication Proxy Data Flow*



1. The HTTP or HTTPS client requests a web page.
2. The HTTP or HTTPS request is intercepted by the Cisco IOS router with authentication proxy.
3. The router marks the TCP/IP connection and forwards the request (with the client address) to the web server, if authentication is required.
4. The web server builds the authentication request form and sends it to the HTTP or HTTPS client via the original request protocol—HTTP or HTTPS.
5. The HTTP or HTTPS client receives the authentication request form.
6. The user enters his or her username and password in the HTTPS POST form and returns the form to the router. At this point, the authentication username and password form is sent via HTTPS. The web server will negotiate a new SSL connection with the HTTPS client.



Note Your Cisco IOS image must support HTTPS, and HTTPS must be configured; otherwise, an HTTP request form will be generated.

7. The router receives the HTTPS POST form from the HTTPS client and retrieves the username and password.
8. The router sends the username and password to the AAA server for client authentication.
9. If the AAA server validates the username and password, it sends the configured user profile to the router. (If it cannot validate the username and password, an error is generated and sent to the router.)
10. If the router receives a user profile from the AAA server, it updates the access list with the user profile and returns a successful web page to the HTTPS client. (If the router receives an error from the AAA server, it returns an error web page to the HTTPS client.)

11. After the HTTPS client receives the successful web page, it retries the original request. Thereafter, HTTPS traffic will depend on HTTPS client requests; no router intervention will occur.

How to Use HTTPS Authentication Proxy

To enable HTTPS authentication proxy, you must enable AAA service, configure the HTTPS server, and enable authentication proxy. This section contains the following procedures:

- [Configuring the HTTPS Server, page 4](#)
- [Verifying HTTPS Authentication Proxy, page 5](#)

Configuring the HTTPS Server

To use HTTPS authentication proxy, you must enable the HTTPS server on the firewall and set the HTTPS server authentication method to use AAA.

Prerequisites

Before configuring the HTTPS server, you must perform the following procedures:

- Configure the authentication proxy for AAA services by enabling AAA and configuring a RADIUS or TACACS+ server. For information on completing these tasks, refer to the section “Configuring AAA” in the chapter “Configuring Authentication Proxy” of the *Cisco IOS Security Configuration Guide*, Release 12.2.
- Obtain a certification authority (CA) certificate. For information on completing this task, refer to the section “Configuring a Trustpoint CA” in the *Trustpoint CLI*, Cisco IOS Release 12.2(8)T feature module.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **ip http authentication aaa**
5. **ip http secure-server**
6. **ip http secure-trustpoint *name***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip http server Example: Router (config)# ip http server	Enables the HTTP server on the router. <ul style="list-style-type: none"> The authentication proxy uses the HTTP server to communicate with the client for user authentication.
Step 4	ip http authentication aaa Router (config)# ip http authentication aaa	Sets the HTTP server authentication method to AAA.
Step 5	ip http secure-server Example: Router (config)# ip http secure-server	Enables HTTPS.
Step 6	ip http secure-trustpoint name Example: Router (config)# ip http secure-trustpoint netCA	Enables HTTP secure server certificate trustpoint.

What to Do Next

After you have finished configuring the HTTPS server, you must configure the authentication proxy (globally and per interface). For information on completing this task, refer to the section “Configuring the Authentication Proxy” in the chapter “Configuring Authentication Proxy” of the *Cisco IOS Security Configuration Guide*, Release 12.2.

Verifying HTTPS Authentication Proxy

To verify your HTTPS authentication proxy configuration, perform the following optional steps:

SUMMARY STEPS

1. enable
2. show ip auth-proxy configuration
3. show ip auth-proxy cache
4. show ip http server secure status

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show ip auth-proxy configuration Example: Router# show ip auth-proxy configuration	Displays the current authentication proxy configuration.
Step 3	show ip auth-proxy cache Example: Router# show ip auth-proxy cache	Displays the list of user authentication entries. The authentication proxy cache lists the host IP address, the source port number, the timeout value for the authentication proxy, and the state of the connection. If the authentication proxy state is HTTP_ESTAB, the user authentication was successful.
Step 4	show ip http server secure status Example: Router# show ip http server secure status	Displays HTTPS status.

Monitoring Firewall Support of HTTPS Authentication Proxy

Perform the following task to troubleshoot your HTTPS authentication proxy configuration:

SUMMARY STEPS

1. enable
2. debug ip auth-proxy detailed

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	Example: debug ip auth-proxy detailed Example: Router# debug ip auth-proxy detailed	Displays the authentication proxy configuration information on the router.

Configuration Examples for HTTPS Authentication Proxy

This section provides the following comprehensive configuration examples:

- [HTTPS Authentication Proxy Support Example, page 7](#)
- [RADIUS User Profile Example, page 10](#)
- [TACACS User Profile Example, page 10](#)
- [HTTPS Authentication Proxy Debug Example, page 11](#)

HTTPS Authentication Proxy Support Example

The following example is output from the **show running-config** command. This example shows how to enable HTTPS authentication proxy on a Cisco IOS router.

```
Router# show running-config

Building configuration...

Current configuration : 6128 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 7200a
!
boot system disk0:c7200-ik9o3s-mz.emweb
aaa new-model
!
!
aaa authentication login default group tacacs+ group radius
aaa authorization auth-proxy default group tacacs+ group radius
aaa session-id common
!
ip subnet-zero
ip cef
!
!
ip domain name cisco.com
!
ip auth-proxy auth-proxy-banner
ip auth-proxy auth-cache-time 3
ip auth-proxy name authname http
ip audit notify log
ip audit po max-events 100
!
! Obtain a CA certificate.
crypto ca trustpoint netCA
  enrollment mode ra
  enrollment url http://10.3.10.228:80/certsrv/mscep/mscep.dll
  subject-name CN=7200a.cisco.com
  crl optional
crypto ca certificate chain netCA
certificate ca 0702EFC30EC4B18D471CD4531FF77E29
  308202C5 3082026F A0030201 02021007 02EFC30E C4B18D47 1CD4531F F77E2930
  0D06092A 864886F7 0D010105 0500306D 310B3009 06035504 06130255 53310B30
  09060355 04081302 434F3110 300E0603 55040713 07426F75 6C646572 31163014
  06035504 0A130D43 6973636F 20537973 74656D73 310C300A 06035504 0B130349
```

Configuration Examples for HTTPS Authentication Proxy

```

54443119 30170603 55040313 10495444 20426F75 6C646572 202D2043 41301E17
0D303230 31323532 33343434 375A170D 31323031 32353233 35343333 5A306D31
0B300906 03550406 13025553 310B3009 06035504 08130243 4F311030 0E060355
04071307 426F756C 64657231 16301406 0355040A 130D4369 73636F20 53797374
656D7331 0C300A06 0355040B 13034954 44311930 17060355 04031310 49544420
426F756C 64657220 2D204341 305C300D 06092A86 4886F70D 01010105 00034B00
30480241 00B896F0 7CE9DCBD 59812309 1793C610 CEC83704 D56C29CA 3E8FAC7A
A113520C E15E3DEF 64909FB9 88CD43BD C7DFBAD6 6D523804 3D958A97 9733EE71
114D8F3F 8B020301 0001A381 EA3081E7 300B0603 551D0F04 04030201 C6300F06
03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 14479FE0 968DAD8A
46774122 2276C19B 6800FA3C 79308195 0603551D 1F04818D 30818A30 42A040A0
3E863C68 7474703A 2F2F6369 73636F2D 736A7477 77383779 792F4365 7274456E
726F6C6C 2F495444 25323042 6F756C64 65722532 302D2532 3043412E 63726C30
44A042A0 40863E66 696C653A 2F2F5C5C 63697363 6F2D736A 74777738 3779795C
43657274 456E726F 6C6C5C49 54442532 30426F75 6C646572 2532302D 25323043
412E6372 6C301006 092B0601 04018237 15010403 02010030 0D06092A 864886F7
0D010105 05000341 0044DE07 3964E080 09050906 512D40C0 D4D86A0A 6B33E752
6E602D96 3F68BB8E 463E3EF6 D29BE400 615E7226 87DE1DE3 96AE23EF E076EE60
BF789728 5ED0D5FC 2C
quit
certificate 55A47951000000000000
308203FC 308203A6 A0030201 02020A55 A4795100 00000000 0D300D06 092A8648
86F70D01 01050500 306D310B 30090603 55040613 02555331 0B300906 03550408
1302434F 3110300E 06035504 07130742 6F756C64 65723116 30140603 55040A13
0D436973 636F2053 79737465 6D73310C 300A0603 55040B13 03495444 31193017
06035504 03131049 54442042 6F756C64 6572202D 20434130 1E170D30 32303631
38323030 3035325A 170D3033 30363138 32303130 35325A30 3A311E30 1C06092A
864886F7 0D010902 130F3732 3030612E 63697363 6F2E636F 6D311830 16060355
0403130F 37323030 612E6369 73636F2E 636F6D30 5C300D06 092A8648 86F70D01
01010500 034B0030 48024100 F61D6551 77F9CABD BC3ACAAC D564AE53 541A40AE
B89B6215 6A6D8D88 831F672E 66678331 177AF07A F476CD59 E535DAD2 C145E41D
BF33BEB5 83DF2A39 887A05BF 02030100 01A38202 59308202 55300B06 03551D0F
04040302 05A0301D 0603551D 0E041604 147056C6 ECE3A7A4 E4F9AFF9 20F23970
3F8A7BED 323081A6 0603551D 2304819E 30819B80 14479FE0 968DAD8A 46774122
2276C19B 6800FA3C 79A171A4 6F306D31 0B300906 03550406 13025553 310B3009
06035504 08130243 4F311030 0E060355 04071307 426F756C 64657231 16301406
0355040A 130D4369 73636F20 53797374 656D7331 0C300A06 0355040B 13034954
44311930 17060355 04031310 49544420 426F756C 64657220 2D204341 82100702
EFC30EC4 B18D471C D4531FF7 7E29301D 0603551D 110101FF 04133011 820F3732
3030612E 63697363 6F2E636F 6D308195 0603551D 1F04818D 30818A30 42A040A0
3E863C68 7474703A 2F2F6369 73636F2D 736A7477 77383779 792F4365 7274456E
726F6C6C 2F495444 25323042 6F756C64 65722532 302D2532 3043412E 63726C30
44A042A0 40863E66 696C653A 2F2F5C5C 63697363 6F2D736A 74777738 3779795C
43657274 456E726F 6C6C5C49 54442532 30426F75 6C646572 2532302D 25323043
412E6372 6C3081C6 06082B06 01050507 01010481 B93081B6 30580608 2B060105
05073002 864C6874 74703A2F 2F636973 636F2D73 6A747777 38377979 2F436572
74456E72 6F6C6C2F 63697363 6F2D736A 74777738 3779795F 49544425 3230426F
756C6465 72253230 2D253230 43412E63 7274305A 06082B06 01050507 3002864E
66696C65 3A2F2F5C 5C636973 636F2D73 6A747777 38377979 5C436572 74456E72
6F6C6C5C 63697363 6F2D736A 74777738 3779795F 49544425 3230426F 756C6465
72253230 2D253230 43412E63 7274300D 06092A86 4886F70D 01010505 00034100
9BAE173E 337CAD74 E95D5382 A5DF7D3C 91F69832 761E374C 0E1E4FD6 EBDE59F6
5B8D0745 32C3233F 25CF45FE DEEB73E 8E5AD908 BF7008F8 BB957163 D63D31AF
quit
!!
!
voice call carrier capacity active
!
!
interface FastEthernet0/0
ip address 192.168.126.33 255.255.255.0
duplex half
no cdp enable
!

```

```
interface ATM1/0
 no ip address
 shutdown
 no atm ilmi-keepalive
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex half
 no cdp enable
!
interface FastEthernet3/0
 ip address 192.168.26.33 255.255.255.0
! Configure auth-proxy interface.
 ip auth-proxy authname
 duplex half
 no cdp enable
!
interface FastEthernet4/0
 ip address 10.3.10.46 255.255.0.0
 duplex half
 no cdp enable
!
interface FastEthernet4/0.1
!
ip nat inside source static 192.168.26.2 192.168.26.25
ip classless
! Configure the HTTPS server.
ip http server
ip http authentication aaa
ip http secure-trustpoint netCA
ip http secure-server
ip pim bidir-enable
!
!
access-list 101 deny tcp any any
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
! Configure AAA and RADIUS server.
tacacs-server host 192.168.126.3
tacacs-server key letmein
!
radius-server host 192.168.126.2 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key letmein
radius-server authorization permit missing Service-Type
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!!
!
gatekeeper
 shutdown
!
!
line con 0
line aux 0
line vty 0 4
 password letmein
!
```

```
!
end
```

RADIUS User Profile Example

The following example is a sample RADIUS user profile for Livingston RADIUS:

```
#----- Proxy user -----

http          Password = "test" User-Service-Type=Outbound-User
              cisco-avpair = "auth-proxy:priv-lvl=15",
              cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq 23"

http_1        Password = "test"
              User-Service-Type = Shell-User,
              User-Service-Type=Dialout-Framed-User,
              cisco-avpair = "shell:priv-lvl=15",
              cisco-avpair = "shell:inacl#4=permit tcp any host 192.168.134.216
eq 23          cisco-avpair = "auth-proxy:priv-lvl=15",
              cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq 23"

http_fail     Password = "test" User-Service-Type=Outbound-User
              cisco-avpair = "auth-proxy:priv-lvl=14",
              cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq 23"

proxy        Password = "cisco" User-Service-Type=Outbound-User      cisco-avpair =
"auth-proxy:proxyacl#4=permit tcp any any eq 20"
```

TACACS User Profile Example

The following examples are sample TACACS user profiles:

```
default authorization = permit
key = cisco
user = http_1 {
    default service = permit
    login = cleartext test
    service = exec
    {
        priv-lvl = 15
        inacl#4="permit tcp any host 192.168.134.216 eq 23"
        inacl#5="permit tcp any host 192.168.134.216 eq 20"
        inacl#6="permit tcp any host 192.168.134.216 eq 21"
        inacl#3="deny -1"
    }
    service = auth-proxy
    {
        priv-lvl=15
        proxyacl#4="permit tcp any host 192.168.105.216 eq 23"
        proxyacl#5="permit tcp any host 192.168.105.216 eq 20"
        proxyacl#6="permit tcp any host 192.168.105.216 eq 21"
        proxyacl#7="permit tcp any host 192.168.105.216 eq 25"
    }
}
user = http {
    login = cleartext test
```

```

        service = auth-proxy
        {
            priv-lvl=15
            proxyacl#4="permit tcp any host 192.168.105.216 eq 23"
            proxyacl#5="permit tcp any host 192.168.105.216 eq 20"
            proxyacl#6="permit tcp any host 192.168.105.216 eq 21"
        }
    }
    user = proxy_1 {
        login = cleartext test
        service = auth-proxy
        {
            priv-lvl=14
        }
    }

    user = proxy_3 {
        login = cleartext test
        service = auth-proxy
        {
            priv-lvl=15
        }
    }

```

HTTPS Authentication Proxy Debug Example

The following is a sample of **debug ip auth-proxy** detailed command output:

```

*Mar  1 21:18:18.534: AUTH-PROXY:proto_flag=7, dstport_index=4
*Mar  1 21:18:18.534:  SYN SEQ 462612879 LEN 0
*Mar  1 21:18:18.534: dst_addr 172.16.171.219 src_addr 171.69.89.25 dst_port 80
src_port 3061
*Mar  1 21:18:18.538: AUTH-PROXY:auth_proxy_half_open_count++ 1
*Mar  1 21:18:18.542: AUTH-PROXY:proto_flag=7, dstport_index=4
*Mar  1 21:18:18.542:  ACK 3715697587 SEQ 462612880 LEN 0
*Mar  1 21:18:18.542: dst_addr 172.16.171.219 src_addr 171.69.89.25 dst_port 80
src_port 3061
*Mar  1 21:18:18.542: clientport 3061 state 0
*Mar  1 21:18:18.542: AUTH-PROXY:proto_flag=7, dstport_index=4
*Mar  1 21:18:18.542:  PSH ACK 3715697587 SEQ 462612880 LEN 250
*Mar  1 21:18:18.542: dst_addr 172.16.171.219 src_addr 171.69.89.25 dst_port 80
src_port 3061
*Mar  1 21:18:18.542: clientport 3061 state 0
*Mar  1 21:18:18.554: AUTH-PROXY:proto_flag=7, dstport_index=4
*Mar  1 21:18:18.554:  ACK 3715698659 SEQ 462613130 LEN 0
*Mar  1 21:18:18.554: dst_addr 172.16.171.219 src_addr 171.69.89.25 dst_port 80
src_port 3061
*Mar  1 21:18:18.554: clientport 3061 state 0
*Mar  1 21:18:18.610: AUTH-PROXY:proto_flag=7, dstport_index=4
*Mar  1 21:18:18.610:  ACK 3715698746 SEQ 462613130 LEN 0
*Mar  1 21:18:18.610: dst_addr 172.16.171.219 src_addr 171.69.89.25 dst_port 80
src_port 3061
*Mar  1 21:18:18.610: clientport 3061 state 0
*Mar  1 21:18:18.766: AUTH-PROXY:proto_flag=7, dstport_index=4
*Mar  1 21:18:18.766:  FIN ACK 3715698746 SEQ 462613130 LEN 0
*Mar  1 21:18:18.766: dst_addr 172.16.171.219 src_addr 171.69.89.25 dst_port 80
src_port 3061
*Mar  1 21:18:18.766: clientport 3061 state 0
*Mar  1 21:18:33.070: AUTH-PROXY:proto_flag=7, dstport_index=4
*Mar  1 21:18:33.070:  SYN SEQ 466414843 LEN 0
*Mar  1 21:18:33.070: dst_addr 172.16.171.219 src_addr 171.69.89.25 dst_port 80
src_port 3064
*Mar  1 21:18:33.070: clientport 3061 state 0
*Mar  1 21:18:33.074: AUTH-PROXY:proto_flag=7, dstport_index=4

```

```

*Mar 1 21:18:33.074: ACK 1606420512 SEQ 466414844 LEN 0
*Mar 1 21:18:33.074: dst_addr 172.16.171.219 src_addr 171.69.89.25 dst_port 80
src_port 3064
*Mar 1 21:18:33.074: clientport 3064 state 0
*Mar 1 21:18:33.078: AUTH-PROXY:proto_flag=7, dstport_index=4
*Mar 1 21:18:33.078: PSH ACK 1606420512 SEQ 466414844 LEN 431
*Mar 1 21:18:33.078: dst_addr 172.16.171.219 src_addr 171.69.89.25 dst_port 80
src_port 3064
*Mar 1 21:18:33.078: clientport 3064 state 0
*Mar 1 21:18:33.090: AUTH-PROXY:proto_flag=7, dstport_index=0
*Mar 1 21:18:33.090: AUTH-PROXY:Protocol not configured on if_input
*Mar 1 21:18:33.226: AUTH-PROXY:proto_flag=7, dstport_index=0
*Mar 1 21:18:33.226: AUTH-PROXY:Protocol not configured on if_input
*Mar 1 21:18:33.546: AUTH-PROXY:proto_flag=7, dstport_index=0
*Mar 1 21:18:33.546: AUTH-PROXY:Protocol not configured on if_input
*Mar 1 21:18:33.550: AUTH-PROXY:proto_flag=7, dstport_index=0
*Mar 1 21:18:33.550: AUTH-PROXY:Protocol not configured on if_input
*Mar 1 21:18:33.594: AUTH-PROXY:proto_flag=7, dstport_index=0
*Mar 1 21:18:33.594: AUTH-PROXY:Protocol not configured on if_input
*Mar 1 21:18:33.594: AUTH-PROXY:proto_flag=7, dstport_index=0
*Mar 1 21:18:33.594: AUTH-PROXY:Protocol not configured on if_input
*Mar 1 21:18:33.598: AUTH-PROXY:proto_flag=7, dstport_index=0
*Mar 1 21:18:33.598: AUTH-PROXY:Protocol not configured on if_input
*Mar 1 21:18:33.706: AUTH-PROXY:proto_flag=7, dstport_index=0
*Mar 1 21:18:33.706: AUTH-PROXY:Protocol not configured on if_input
*Mar 1 21:18:33.810: AUTH-PROXY:proto_flag=7, dstport_index=0
*Mar 1 21:18:33.810: AUTH-PROXY:Protocol not configured on if_input
*Mar 1 21:18:33.810: AUTH-PROXY:proto_flag=7, dstport_index=0
*Mar 1 21:18:33.810: AUTH-PROXY:Protocol not configured on if_input
*Mar 1 21:18:33.810: AUTH-PROXY:proto_flag=7, dstport_index=4
*Mar 1 21:18:33.810: ACK 1606421496 SEQ 466415275 LEN 0
*Mar 1 21:18:33.810: dst_addr 172.16.171.219 src_addr 171.69.89.25 dst_port 80
src_port 3064
*Mar 1 21:18:33.814: clientport 3064 state 6
*Mar 1 21:18:33.814: AUTH-PROXY:Packet in FIN_WAIT state
*Mar 1 21:18:33.838: AUTH-PROXY:proto_flag=7, dstport_index=4
*Mar 1 21:18:33.838: FIN ACK 1606421496 SEQ 466415275 LEN 0
*Mar 1 21:18:33.838: dst_addr 172.16.171.219 src_addr 171.69.89.25 dst_port 80
src_port 3064
*Mar 1 21:18:33.838: clientport 3064 state 6
*Mar 1 21:18:33.838: AUTH-PROXY:Packet in FIN_WAIT state

```

Additional References

For additional information related to the Firewall Support of HTTPS Authentication Proxy feature, refer to the following references:

- [Related Documents, page 13](#)
- [Standards, page 13](#)
- [MIBs, page 13](#)
- [RFCs, page 14](#)
- [Technical Assistance, page 14](#)

Related Documents

Related Topic	Document Title
Authentication proxy configuration tasks	<i>The chapter “Configuring Authentication Proxy” in the Cisco IOS Security Configuration Guide, Release 12.2</i>
Authentication proxy commands	<i>The chapter “Authentication Proxy Commands” in the Cisco IOS Security Command Reference, Release 12.2</i>
Information on adding HTTPS support to the Cisco IOS web server	<i>Secure HTTP (HTTPS), Cisco IOS Release 12.1(11b)E feature module</i>
Information on configuring and obtaining a CA certificate.	<i>Trustpoint CLI, Cisco IOS Release 12.2(8)T feature module</i>

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

RFCs ¹	Title
RFC 1945	<i>Hypertext Transfer Protocol — HTTP/ 1.0</i>
RFC 2616	<i>Hypertext Transfer Protocol — HTTP/ 1.1</i>

1. Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This feature uses no new or modified commands. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*..

Glossary

ACL—access control list. An ACL is a list kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).

Cisco IOS Firewall—The Cisco IOS Firewall is a protocol that provides advanced traffic filtering functionality and can be used as an integral part of your network's firewall.

The Cisco IOS Firewall creates temporary openings in access lists at firewall interfaces. These openings are created when specified traffic exits your internal network through the firewall. The openings allow returning traffic (that would normally be blocked) and additional data channels to enter your internal network back through the firewall. The traffic is allowed back through the firewall only if it is part of the same session as the original traffic that triggered the Cisco IOS Firewall when exiting through the firewall.

firewall—A firewall is a networking device that controls access to the network assets of your organization. Firewalls are positioned at the entrance points into your network. If your network has multiple entrance points, you must position a firewall at each point to provide effective network access control.

The most basic function of a firewall is to monitor and filter traffic. Firewalls can be simple or elaborate, depending on your network requirements. Simple firewalls are usually easier to configure and manage. However, you might require the flexibility of a more elaborate firewall.

HTTPS—HTTP over SSL. HTTPS is client communication with a server by first negotiating an SSL connection and then transmitting the HTTP protocol data over the SSL application data channel.

SSL—Secure Socket Layer. SSL is encryption technology for the web used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.

**Note**

Refer to the [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Firewall Authentication Proxy for FTP and Telnet Sessions

Before the introduction of the Firewall Authentication Proxy for FTP and Telnet Sessions feature, users could enable only HTTP when configuring authentication proxy. This feature introduces support for FTP and Telnet, providing users with three protocol options when configuring authentication proxy.

Feature Specifications for the Firewall Authentication Proxy for FTP and Telnet Sessions Feature

Feature History

Release	Modification
12.3(1)	This feature was introduced.

Supported Platforms

For platforms supported in Cisco IOS Release 12.3(1), consult Cisco Feature Navigator.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions for Firewall Authentication Proxy for FTP and Telnet Sessions, page 2](#)
- [Information About Firewall Authentication Proxy for FTP and Telnet Sessions, page 2](#)
- [How to Configure FTP or Telnet Authentication Proxy, page 7](#)
- [Configuration Examples for FTP and Telnet Authentication Proxy, page 12](#)
- [Additional References, page 15](#)
- [Command Reference, page 17](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Restrictions for Firewall Authentication Proxy for FTP and Telnet Sessions

- Authentication proxy is an IP-only feature; thus, it comes with only -o3 images.
- “proxyacl#<n>” is the only supported attribute in the authentication, authorization, and accounting (AAA) server’s user configuration.
- Authentication proxy is subjected only to the traffic that passes through the router; traffic that is destined for the router continues to be authenticated by the existing authentication methods that are provided by Cisco IOS.

Information About Firewall Authentication Proxy for FTP and Telnet Sessions

To configure the Authentication Proxy for FTP and Telnet Sessions feature, you must understand the following concepts:

- [Feature Design for FTP and Telnet Authentication Proxy, page 2](#)
- [Absolute Timeout, page 7](#)

Feature Design for FTP and Telnet Authentication Proxy

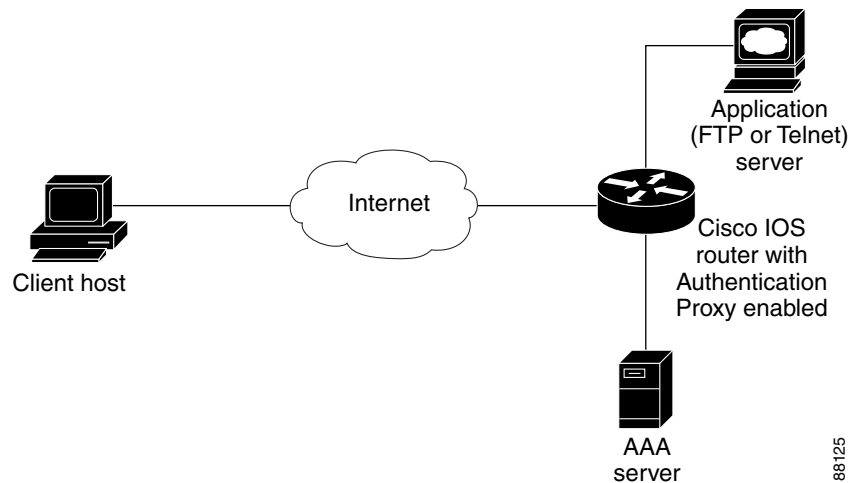
Authentication proxy for FTP and Telnet Sessions functions like authentication proxy for HTTP; that is, FTP and Telnet are independent components in the Cisco IOS software and can be enabled or disabled on the interface of an unauthenticated host.

Many of the authentication proxy for FTP or Telnet functions are similar to those used with HTTP, such as the interaction between the authentication proxy router and the AAA server during authentication. However, because of protocol differences, FTP and Telnet login methods are different from HTTP.

FTP and Telnet Login Methods

[Figure 1](#) displays a typical authentication proxy topology.

Figure 1 *Typical Authentication Proxy Topology*

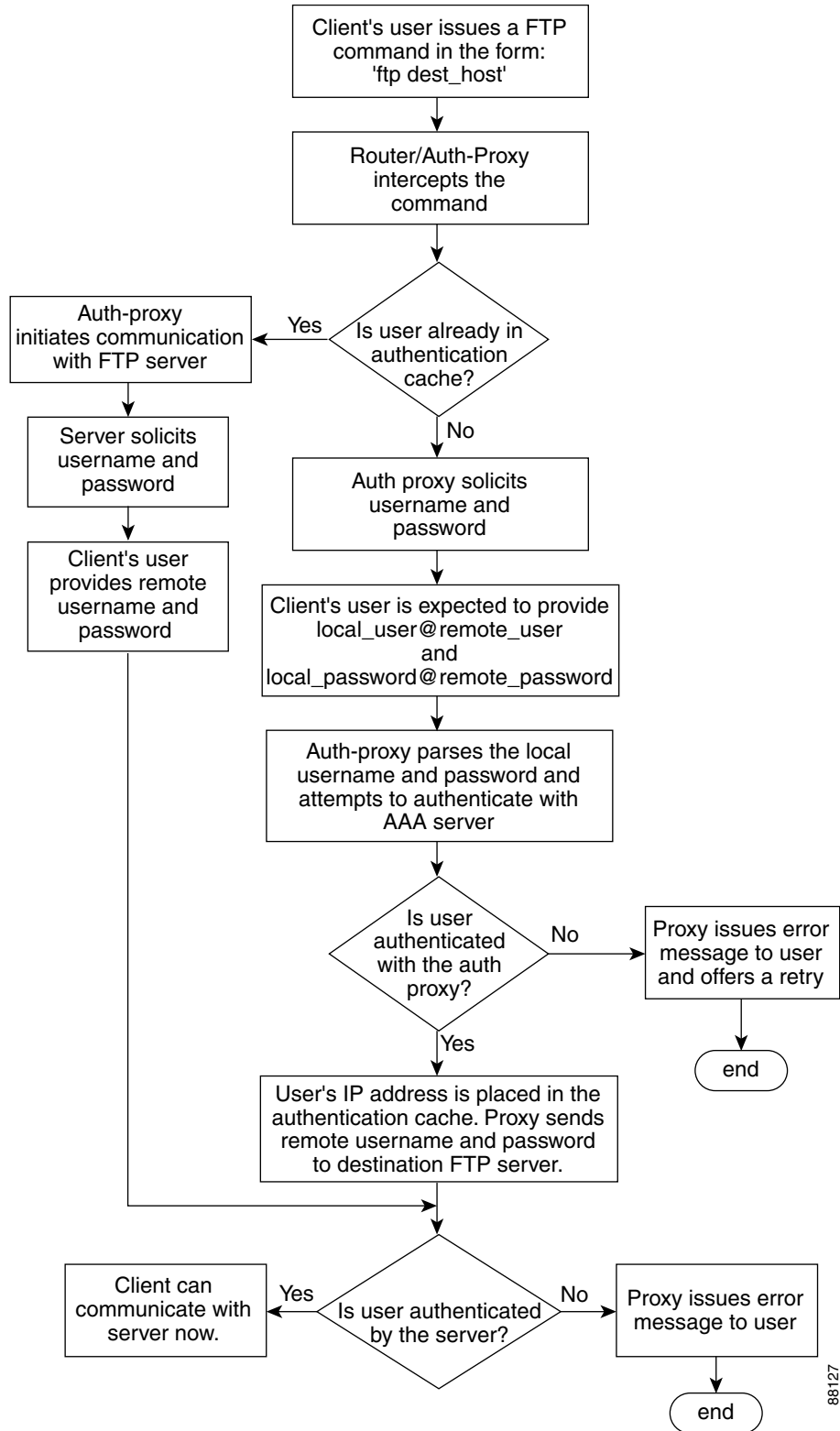


Just as with HTTP, the authentication proxy router intercepts traffic that is sent from the client host. Upon receiving a FTP or Telnet packet, the router will look into its authentication cache to check whether the client host has already been authenticated. If it has been authenticated, the router will forward the client host's traffic to the FTP or Telnet server for additional authentication. If the IP address of the client host is not in the cache of the router, the router will try to authenticate the client host with the AAA server using the username and password of the router.

FTP Login

For FTP login, the client host will be prompted (by the authentication proxy router) for the username and password of the router; the client must respond with the username and password in the following format: "login: proxy_username@ftp_username" and "password: proxy_passwd@ftp_passwd:". The authentication proxy will use the proxy username and password to verify the client's profile against the AAA server's user database. After the client is successfully authenticated with the AAA server, the authentication proxy will pass the FTP (remote) username and password to the FTP server (destination server) for the application server authentication.

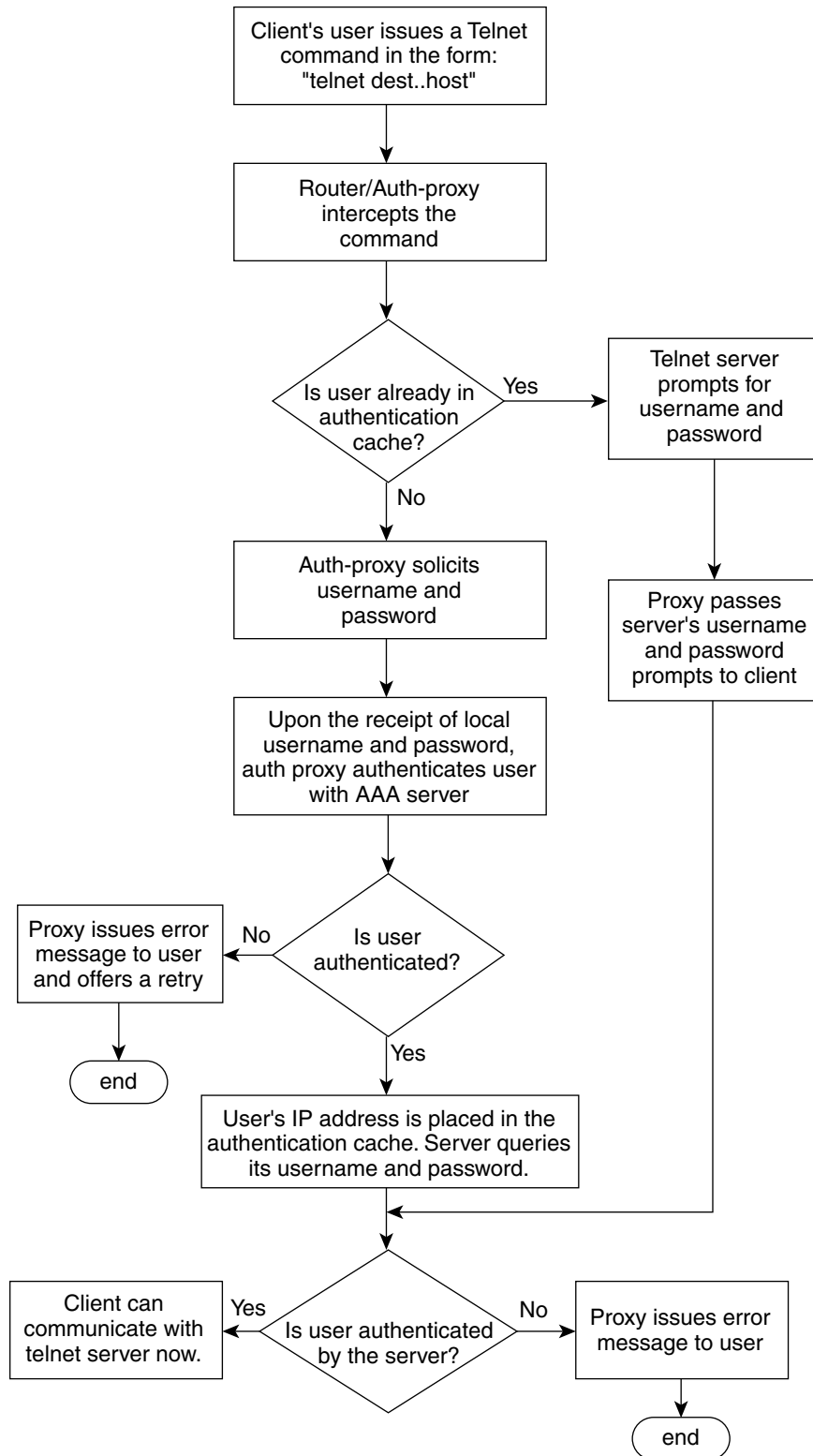
A flow chart that depicts an overview of the FTP authentication proxy process is shown in [Figure 2](#).

Figure 2 *FTP Authentication Proxy Overview*

Telnet Login

For Telnet login, the client host will be prompted (by the authentication proxy router) for the username, followed by the password; the client must respond with the username and password in the following format: “login: proxy_username:” and “password: proxy_passwd:”. The username and password will be verified against the AAA server’s user database. After the client is successfully authenticated with the AAA server, the Telnet server (destination server) will prompt the client for the username and password of the Telnet server.

A flow chart that depicts an overview of the Telnet authentication proxy process is shown in [Figure 3](#).

Figure 3 *Telnet Authentication Proxy Overview*

88126

If authentication with the AAA server fails, the proxy will inform the client accordingly. With Telnet, the proxy does not have any interest in the Telnet server's username and password. If the client is authenticated with the AAA server but fails with the Telnet server, the client will not have to authenticate with the AAA server the next time he or she logs into the network; the client's IP address will be stored in the authentication cache. The client will have to authenticate only with the Telnet server.

**Note**

With FTP, the client must always reenter the local and remote username and password combination every time he or she tries to log into the network—regardless of a successful AAA server authentication.

Absolute Timeout

An absolute timeout value has been added to allow users to configure a window during which the authentication proxy on the enabled interface is active. After the absolute timer expires, the authentication proxy will be disabled regardless of any activity. The absolute timeout value can be configured per protocol (via the **ip auth-proxy name** command) or globally (via the **ip auth-proxy** command). The default value of the absolute timeout is zero; that is, the absolute timer is turned off by default, and the authentication proxy is enabled indefinitely and is subject only to the timeout specified by the **inactivity-timer** keyword.

**Note**

The **inactivity-timer** keyword deprecates the **auth-cache-time** keyword in the **ip auth-proxy name** and the **ip auth-proxy** commands.

How to Configure FTP or Telnet Authentication Proxy

To enable FTP or Telnet authentication proxy, you must enable AAA services, configure the FTP or Telnet server, and enable authentication proxy. This section contains the following procedures:

- [Configuring AAA, page 7](#)
- [Configuring the Authentication Proxy, page 9](#)
- [Verifying FTP or Telnet Authentication Proxy, page 11](#)
- [Monitoring and Maintaining FTP or Telnet Authentication Proxy Sessions, page 11](#)

Configuring AAA

To use authentication proxy, you must configure a AAA server for authentication. The authentication proxy service of the AAA server must also be configured for authorization. To configure these tasks, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login default group tacacs+ group radius**

5. **aaa authorization auth-proxy default** [[group tacacs+] [group radius]]
6. **aaa authorization exec default** [group tacacs+] [group radius]
7. **aaa accounting auth-proxy default stop-only** [group tacacs+] [group radius]
8. **access-list** *access-list-number* {permit | deny} {tcp | ip | icmp} host *source* eq *tacacs* host *destination*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa new-model Example: Router (config)# aaa new-model	Enables the AAA functionality on the router.
Step 4	aaa authentication login default group tacacs+ group radius Example: Router (config)# aaa authentication login default group tacacs+ group radius	Defines the list of authentication methods at login.
Step 5	aaa authorization auth-proxy default [[group tacacs+] [group radius]] Example: Router (config)# aaa authorization auth-proxy default group tacacs+ group radius	Uses the auth-proxy keyword to enable authorization proxy for AAA methods.
Step 6	aaa authorization exec default [group tacacs+] [group radius] Example: Router (config)# aaa authorization exec default group tacacs+ group radius	Enables authorization for TACACS+ and RADIUS.

	Command or Action	Purpose
Step 7	<pre>aaa accounting auth-proxy default stop-only [group tacacs+] [group radius]</pre> <p>Example:</p> <pre>Router (config)# aaa accounting auth-proxy default stop-only group tacacs+ group radius</pre>	Activates authentication proxy accounting and uses the auth-proxy keyword to set up the authorization policy as dynamic access control lists (ACLs) that can be downloaded.
Step 8	<pre>access-list access-list-number {permit deny} {tcp ip icmp} host source eq tacacs host destination</pre> <p>Example:</p> <pre>Router (config)# access-list 111 permit tcp host 209.165.200.225 eq tacacs host 209.165.200.254</pre> <p>or</p> <pre>Router (config)# access-list 111 deny ip any any</pre> <p>or</p> <pre>Router (config)# access-list 111 permit icmp any any</pre>	<p>Creates an ACL entry to allow the AAA server to return traffic to the firewall.</p> <p>The source address is the IP address of the AAA server, and the destination is the IP address of the router interface where the AAA server resides.</p>

What to Do Next

Ensure that your FTP or Telnet server is enabled and that the user credentials of the client (the username and password) are stored in the server's database.

Configuring the Authentication Proxy

To configure the authentication proxy, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip auth-proxy {inactivity-timer *min* | absolute-timer *min*}**
4. **ip auth-proxy auth-proxy-banner {ftp | http | telnet} [*banner-text*]**
5. **ip auth-proxy name *auth-proxy-name* {ftp | http | telnet} [*inactivity-timer min* | *absolute-timer min*] [*list {acl | acl-name}*]**
6. **interface *type***
7. **ip auth-proxy *auth-proxy-name***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip auth-proxy {inactivity-timer min absolute-timer min} Example: Router (config)# ip auth-proxy inactivity-timer 30	Sets the global authentication proxy idle timeout values in minutes. <ul style="list-style-type: none"> inactivity-timer min—Specifies the length of time in minutes that an authentication cache entry is managed after a period of inactivity. Enter a value in the range 1 to 2,147,483,647. The default value is 60 minutes. absolute-timer min—Specifies a window in which the authentication proxy on the enabled interface is active. Enter a value in the range 1 to 65,535 minutes (45 and a half days). The default value is 0 minutes.
Step 4	ip auth-proxy auth-proxy-banner {ftp http telnet} [banner-text] Example: Router (config)# ip auth-proxy auth-proxy-banner ftp hello	Optional) Displays the name of the firewall router in the authentication proxy login page. Disabled by default. <ul style="list-style-type: none"> ftp—Specifies the FTP protocol. http—Specifies the HTTP protocol. telnet—Specifies the Telnet protocol. banner-text—(Optional) A text string that replaces the default banner.
Step 5	ip auth-proxy name auth-proxy-name {ftp http telnet} [inactivity-timer min] [absolute-timer min] [list {acl acl-name}] Example: Router (config)# ip auth-proxy name ftp_list1 ftp absolute-timer 60 ftp list 102	Configures authentication proxy on an interface. <ul style="list-style-type: none"> ftp—Specifies FTP to trigger that authentication proxy. http—Specifies HTTP to trigger that authentication proxy. telnet—Specifies Telnet to trigger that authentication proxy. inactivity-timer min—Overrides global authentication proxy cache timer for a specific authentication proxy name. absolute-timer min— Overrides the global value specified via the ip auth-proxy command. list {acl acl-name}—Specifies a standard (1–99), extended (1–199), or named access list to use with the authentication proxy.

	Command or Action	Purpose
Step 6	interface <i>type</i> Example: Router (config)# interface e0	Enters interface configuration mode by specifying the interface type on which to apply the authentication proxy.
Step 7	ip auth-proxy <i>auth-proxy-name</i> Example: Router(config-if)# ip auth-proxy authproxyrule	In interface configuration mode, applies the named authentication proxy rule at the interface. This command enables the authentication proxy rule with that name.

Verifying FTP or Telnet Authentication Proxy

To verify your FTP or Telnet authentication proxy configuration, perform the following optional steps:

SUMMARY STEPS

1. **enable**
2. **show ip auth-proxy configuration**
3. **show ip auth-proxy cache**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	show ip auth-proxy configuration Example: Router# show ip auth-proxy configuration	Displays the current authentication proxy configuration.
Step 3	show ip auth-proxy cache Example: Router# show ip auth-proxy cache	Displays the list of user authentication entries. The authentication proxy cache lists the host IP address, the source port number, the timeout value for the authentication proxy, and the state of the connection. If the authentication proxy state is ESTAB or INTERCEPT, the user authentication was successful.

Monitoring and Maintaining FTP or Telnet Authentication Proxy Sessions

To monitor FTP or Telnet authentication proxy sessions, perform the following optional steps:

SUMMARY STEPS

1. **enable**
2. **debug ip auth-proxy {detailed | ftp | function-trace | object-creation | object-deletion | telnet | timers}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	debug ip auth-proxy {detailed ftp function-trace object-creation object-deletion telnet timers} Example: Router# debug ip auth-proxy ftp	Displays the authentication proxy configuration information on the router.

Configuration Examples for FTP and Telnet Authentication Proxy

This section provides the following configuration examples:

- [Authentication Proxy Configuration Example, page 12](#)
- [AAA Server User Profile Examples, page 13](#)

Authentication Proxy Configuration Example

The following example shows how to configure your router for authentication proxy:

```

aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
aaa authorization auth-proxy default group tacacs+
enable password lab
!
ip inspect name pxy_test ftp
ip auth-proxy name pxy auth-cache-time 1
!
interface Ethernet0/0
 ip address 209.165.200.225 255.255.255.224
 ip access-group 105 in
 no ip directed-broadcast
 ip inspect pxy_test in
 ip auth-proxy pxy
 no shut
!
interface Ethernet0/1
 ip address 209.165.200.225 255.255.255.224
 ip access-group 102 in
 no ip directed-broadcast

```

```

no shut
!
ip http authentication aaa
!
access-list 102 permit any
access-list 102 permit tcp host 209.165.200.234 eq tacacs any
access-list 102 deny tcp any any
access-list 102 deny udp any any
access-list 102 permit ip any any
access-list 105 permit tcp any any eq www
access-list 105 permit ip any any
access-list 105 deny tcp any any
access-list 105 deny udp any any
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
tacacs-server host 209.165.200.234
tacacs-server key cisco
!
line con 0
  transport input none
  login authentication special
line aux 0
line vty 0 4
  password lab

```

AAA Server User Profile Examples

This section includes examples of the authentication proxy user profile entries on the AAA servers. The “proxyacl” entries define the user access privileges. After the user has successfully used the authentication proxy to log in, these entries are transferred to the firewall router. Each entry in the profile must specify “permit” access for the service or application. The source address in each entry is set to “any”, which is replaced with the IP address of the authenticating host when the profile is downloaded to the firewall. The privilege level must be set to 15 for all AAA users.

This section contains the following examples:

- [TACACS+ User Profiles Example](#)
- [Livingston RADIUS User Profiles Example](#)
- [Ascend RADIUS User Profiles Example](#)

TACACS+ User Profiles Example

The following example are sample TACACS+ user profiles:

```

default authorization = permit
key = cisco
user = http_1 {
  default service = permit
  login = cleartext test
  service = exec
  {
    priv-lvl = 15
    inacl#4="permit tcp any host 209.165.200.234 eq 23"
    inacl#5="permit tcp any host 209.165.200.234 eq 20"
    inacl#6="permit tcp any host 209.165.200.234 eq 21"
    inacl#3="deny -1"
  }
}

```

```

service = auth-proxy
{
    priv-lvl=15
    proxyacl#4="permit tcp any host 209.165.201.1 eq 23"
    proxyacl#5="permit tcp any host 209.165.201.1 eq 20"
    proxyacl#6="permit tcp any host 209.165.201.1 eq 21"
    proxyacl#7="permit tcp any host 209.165.201.1 eq 25"
}

}

user = http {
    login = cleartext test
    service = auth-proxy
    {
        priv-lvl=15
        proxyacl#4="permit tcp any host 209.165.201.1 eq 23"
        proxyacl#5="permit tcp any host 209.165.201.1 eq 20"
        proxyacl#6="permit tcp any host 209.165.201.1 eq 21"
    }
}

user = proxy_1 {
    login = cleartext test
    service = auth-proxy
    {
        priv-lvl=14
    }
}

user = proxy_3 {
    login = cleartext test
    service = auth-proxy
    {
        priv-lvl=15
    }
}

```

Livingston RADIUS User Profiles Example

The following examples are sample user profiles for the Livingston RADIUS server:

```

#----- Proxy user -----

http          Password = "test" User-Service-Type=Outbound-User
cisco-avpair = "auth-proxy:priv-lvl=15",
cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq 23"

http_1        Password = "test"
User-Service-Type = Shell-User,
User-Service-Type=Dialout-Framed-User,
cisco-avpair = "shell:priv-lvl=15",
cisco-avpair = "shell:inacl#4=permit tcp any host 209.165.200.234
eq 23
cisco-avpair = "auth-proxy:priv-lvl=15",
cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq 23"

http_fail     Password = "test" User-Service-Type=Outbound-User
cisco-avpair = "auth-proxy:priv-lvl=14",
cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq 23"

proxy Password = "cisco" User-Service-Type=Outbound-User      cisco-avpair =
"auth-proxy:proxyacl#4=permit tcp any any eq 20"

```


Ascend RADIUS User Profiles Example

The following examples are sample user profiles for the Ascend RADIUS server:

```
#----- Proxy user -----

http          Password = "test" User-Service=Dialout-Framed-User
cisco-avpair = "auth-proxy:priv-lvl=15",
cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq 23"

http_2        Password = "test"
User-Service=Dialout-Framed-User
cisco-avpair = "auth-proxy:priv-lvl=15",
cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq 23",
cisco-avpair = "shell:inacl#4=permit tcp any host 209.165.200.234 eq 25"

http_1        Password = "test"
User-Service=Dialout-Framed-User,
cisco-avpair = "shell:inacl#4=permit tcp any host 209.165.200.234 eq 23",
cisco-avpair = "auth-proxy:priv-lvl=15",
cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq 23"

http_fail     Password = "test" User-Service=Dialout-Framed-User
cisco-avpair = "auth-proxy:priv-lvl=14",
cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq 23"

cisco-avpair = "auth-proxy:proxyacl#1=permit tcp any any eq 23",
cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq ftp",
cisco-avpair = "auth-proxy:proxyacl#4=permit tcp any any eq 20"

#-----

proxy Password = "cisco" User-Service = Dialout-Framed-User

cisco-avpair = "auth-proxy:priv-lvl=15",

cisco-avpair = "auth-proxy:priv-lvl=15",
cisco-avpair = "auth-proxy:proxyacl#1=permit tcp any any eq 26",
cisco-avpair = "auth-proxy:proxyacl#3=permit tcp any any eq ftp",
```

Additional References

The following sections provide additional references related to the Firewall Authentication Proxy for FTP and Telnet Sessions feature:

- [Related Documents, page 16](#)
- [Standards, page 16](#)
- [MIBs, page 16](#)
- [RFCs, page 16](#)
- [Technical Assistance, page 16](#)

Related Documents

Related Topic	Document Title
Additional authentication proxy configuration tasks	<i>The chapter “Configuring Authentication Proxy” in the Cisco IOS Security Configuration Guide, Release 12.3</i>
Additional authentication proxy commands	<i>Cisco IOS Security Command Reference, Release 12.3</i>
RADIUS and TACACS+ configuration information	The section “Security Server Protocols” in the <i>Cisco IOS Security Configuration Guide, Release 12.3</i>
RADIUS and TACACS+ attribute information	The chapters “RADIUS Attributes” and “TACACS+ Attribute-Value Pairs” in the <i>Cisco IOS Security Configuration Guide, Release 12.3</i>
Additional authentication proxy information	<i>Firewall Support of HTTPS Authentication Proxy, Cisco IOS Release 12.2(15)T feature module</i>

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug ip auth-proxy**
- **ip auth-proxy**
- **ip auth-proxy auth-proxy-banner**
- **ip auth-proxy name**

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Transparent Bridging Support for Authentication Proxy

First Published: June 29, 2007

Last Updated: June 29, 2007

The Transparent Bridging Support for Authentication Proxy feature allows network administrators to deploy authentication proxy on existing networks without changing the statically defined IP addresses of their network-connected devices. Thus, administrators can configure a security solution that dynamically authenticates and authorizes security policies on a per user basis.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Transparent Authentication Proxy](#)” section on page 10.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Restrictions for Transparent Bridging Support for Authentication Proxy, page 2](#)
- [Information About Transparent Bridging Support for Authentication Proxy, page 2](#)
- [How to Configure Transparent Authentication Proxy, page 3](#)
- [Configuration Examples for Transparent Authentication Proxy, page 3](#)
- [Additional References, page 7](#)
- [Command Reference, page 8](#)
- [Feature Information for Transparent Authentication Proxy, page 10](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Restrictions for Transparent Bridging Support for Authentication Proxy

Authentication Proxy is not supported on vLAN trunk interfaces that are configured in a bridge group.

Information About Transparent Bridging Support for Authentication Proxy

To use transparent authentication proxy in your network, you should understand the following concepts:

- [Benefits of Transparent Authentication Proxy, page 2](#)
- [Transparent Authentication Proxy Overview, page 2](#)

Benefits of Transparent Authentication Proxy

Added Security with Minimum Configuration

Users can simply configure transparent authentication proxy into an existing network without having to reconfigure their statically defined devices. Thus, the tedious and costly overhead that was required to renumber devices on the trusted network is eliminated.

Authentication Proxy on Bridged and Routed Interfaces

Authentication proxy rules on bridged interfaces can coexist with router interfaces on the same device, whenever applicable. Thus, users can deploy different authentication proxy rules on bridged and routed domains.

Transparent Authentication Proxy Overview

Authentication proxy provides dynamic, per-user authentication and authorization of network access connections. It allows network administrators to enforce security policies on per-user basis. Typically, authentication proxy is a Layer 3 functionality that is configured on routed interfaces with different networks and IP subnets on each interface.

Integrating authentication proxy with transparent bridging enables network administrators to deploy authentication proxy on an existing network without impacting the existing network configuration and IP address assignments of the hosts on the network.

Transparent Bridging Overview

If configured for bridging, a Cisco IOS device can bridge any number of interfaces. The device can complete basic bridging tasks such as learning MAC addresses on ports to restrict collision domains and running Spanning Tree Protocol (STP) to prevent looping in the topology.

Within bridging, a user can configure Integrated Routed Bridging (IRB), which allows a device to bridge on some interfaces while a Layer 3 Bridged Virtual Interface (BVI) is presented for routing. The bridge can determine whether the packet is to be bridged or routed on the basis of the destination of the Layer 2 or Layer 3 IP address in the packet. Configured with an IP address, the BVI can manage the device even if no interface is configured for routing.

How to Configure Transparent Authentication Proxy

To configure authentication proxy on bridged interfaces, you must configure the interface in a bridge group and apply an authentication proxy rule on the interface. You must also set up and configure the authentication, authorization, and accounting (AAA) server (Cisco ACS) for authentication proxy. For examples on how to configure authentication proxy on a bridged interface, see the section, [“Configuration Examples for Transparent Authentication Proxy”](#) section on page 3.

Configuration Examples for Transparent Authentication Proxy

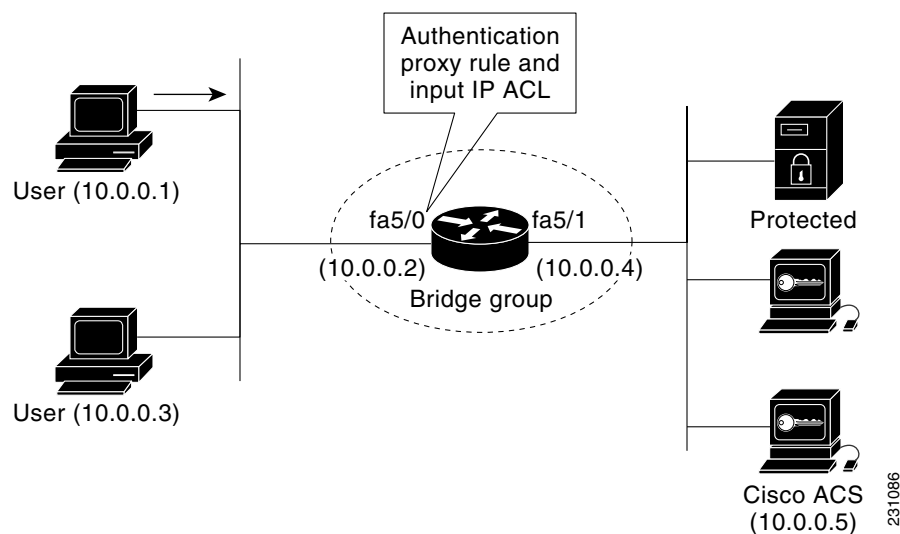
This section contains the following configuration examples, which show how to configure authentication proxy on a bridged interface:

- [Authentication Proxy in Transparent Bridge Mode: Example, page 3](#)
- [Authentication Proxy in Concurrent Route Bridge Mode: Example, page 4](#)
- [Authentication Proxy in Integrated Route Bridge Mode: Example, page 6](#)

Authentication Proxy in Transparent Bridge Mode: Example

The following example (see [Figure 1](#)) shows how to configure authentication proxy in a transparent bridged environment in which network users (that is, hosts on the bridged interface FastEthernet 5/0) are challenged for user credentials before being given access to protected resources.

Figure 1 Authentication Proxy in Transparent Bridging Mode: Sample Topology



```

aaa new-model
!
aaa authentication login default group radius
aaa authorization auth-proxy default group radius
aaa accounting auth-proxy default start-stop group radius
!
no ip routing
!
!
no ip cef
!
ip auth-proxy name AuthRule http inactivity-time 60
!
interface FastEthernet5/0
 ip address 10.0.0.2 255.255.255.0
 ip auth-proxy AuthRule
 ip access-group 100 in
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
!
interface FastEthernet5/1
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
!
ip http server
ip http secure-server
!
radius-server host 10.0.0.5 auth-port 1645 acct-port 1646
radius-server key cisco
!
bridge 1 protocol ieee
!
Router# show ip auth-proxy cache

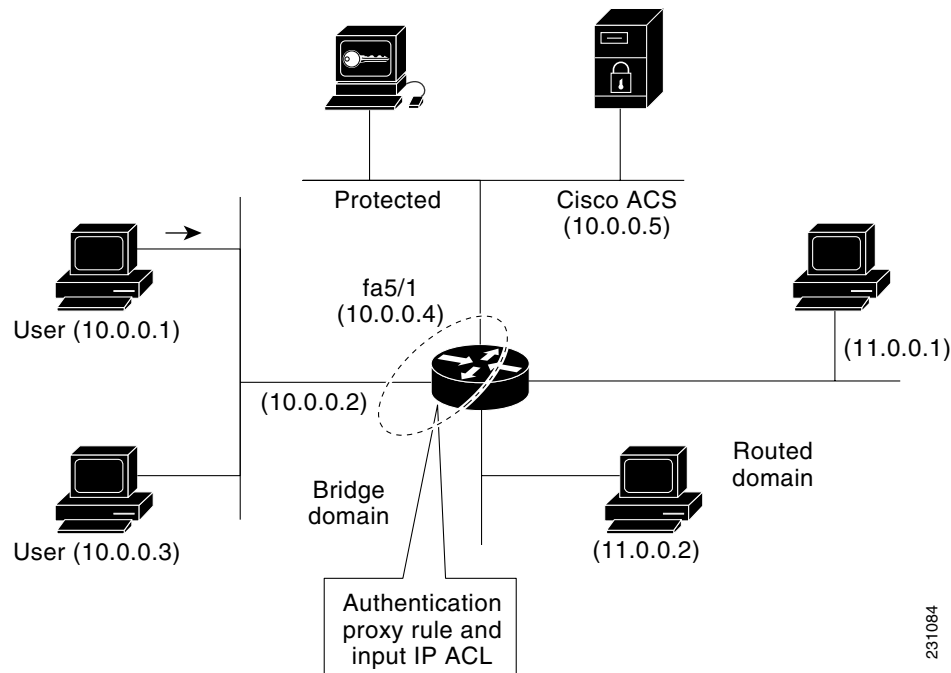
Authentication Proxy Cache
Client Name AuthRule, Client IP 10.0.0.1, Port 1100,
        timeout 60, Time Remaining 60, state ESTAB

```

Authentication Proxy in Concurrent Route Bridge Mode: Example

Concurrent routing and bridging configuration mode allows routing and bridging to occur in the same router; however, the given protocol is not switched between the two domains. Instead, routed traffic is confined to the routed interfaces and bridged traffic is confined to the bridged interfaces.

The following example (see [Figure 2](#)) shows how to configure authentication proxy in a concurrent routing and bridging environment in which network users (that is, hosts on the bridged interface FastEthernet 5/0) are challenged for user credentials before being given access to protected resources.

Figure 2 Authentication Proxy in Concurrent Route Bridge Mode: Sample Topology

```

aaa new-model
!
aaa authentication login default group radius
aaa authorization auth-proxy default group radius
aaa accounting auth-proxy default start-stop group radiusb
!
ip cef
!
bridge crb
!
ip auth-proxy name AuthRule http inactivity-time 60
!
interface FastEthernet5/0
 ip address 10.0.0.2 255.255.255.0
 ip auth-proxy AuthRule
 ip access-group 100 in
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
!
interface FastEthernet5/1
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
!
ip http server
ip http secure-server
!
radius-server host 10.0.0.5 auth-port 1645 acct-port 1646
radius-server key cisco
!

```

```

bridge 1 protocol ieee
!
Router# show ip auth-proxy cache

Authentication Proxy Cache
Client Name AuthRule, Client IP 10.0.0.1, Port 1145,
        timeout 60, Time Remaining 60, state ESTAB

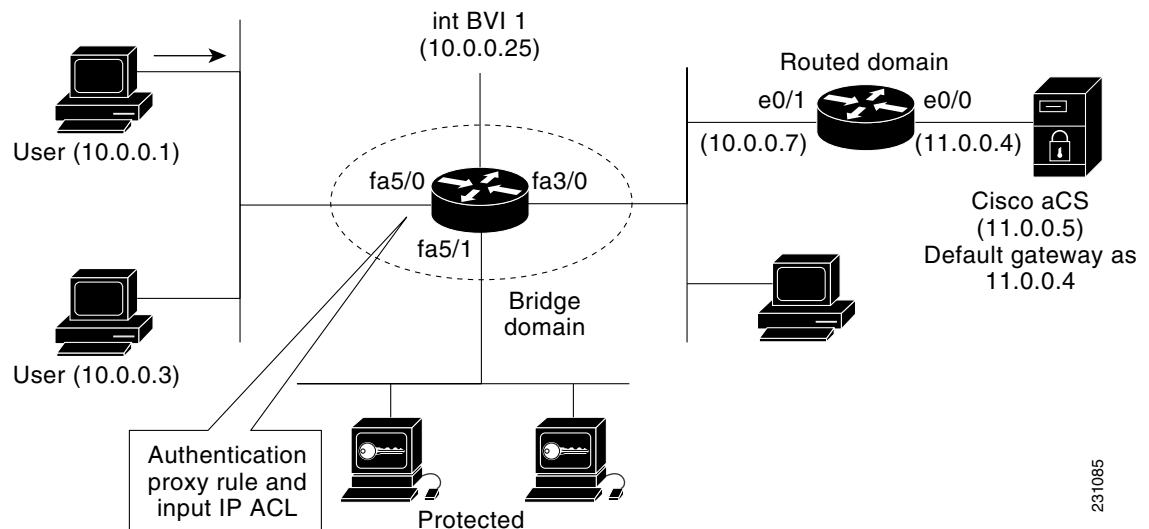
```

Authentication Proxy in Integrated Route Bridge Mode: Example

In an integrated routing and bridging environment, a bridged network is interconnected with a router network. Both routing and bridging can occur in the same router with connectivity between routed and bridged domains.

The following example (see [Figure 3](#)) shows how to configure authentication proxy in an integrated routing and bridging environment in which network users (that is, hosts on the bridged interface FastEthernet 5/0) are challenged for user credentials before being given access to protected resources.

Figure 3 Authentication Proxy in Integrated Route Bridge Mode: Sample Topology



```

!
aaa new-model
!
aaa authentication login default group radius
aaa authorization auth-proxy default group radius
aaa accounting auth-proxy default start-stop group radius
!
ip cef
!
ip auth-proxy name AuthRule http inactivity-time 60
!
bridge irb
!
interface FastEthernet3/0
no ip address
duplex half
bridge-group 1
!

```

```
interface FastEthernet5/0
  no ip address
  ip auth-proxy AuthRule
  ip access-group 100 in
  duplex auto
  speed auto
  bridge-group 1
!
interface FastEthernet5/1
  no ip address
  duplex auto
  speed auto
  bridge-group 1
!
interface BVI1
  ip address 10.0.0.25 255.255.255.0
!
!
ip route 11.0.0.0 255.255.255.0 10.0.0.7
!
ip http server
ip http secure-server
!
radius-server host 11.0.0.5 auth-port 1645 acct-port 1646
radius-server key cisco
!
bridge 1 protocol ieee
bridge 1 route ip
!
Router# show ip auth-proxy cache

Authentication Proxy Cache
Client Name AuthRule, Client IP 10.0.0.1, Port 1100,
      timeout 60, Time Remaining 60, state ESTAB
```

Additional References

The following sections provide references related to the Transparent Bridging Support for Authentication Proxy feature.

Related Documents

Related Topic	Document Title
Authentication proxy commands	Cisco IOS Security Command Reference , Release 12.4T
Bridging commands	Cisco IOS Bridging Command Reference , Release 12.4T

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

This feature uses no new or modified commands.

Feature Information for Transparent Authentication Proxy

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Transparent Authentication Proxy

Feature Name	Releases	Feature Information
Transparent Bridging Support for Authentication Proxy	12.4(15)T	This feature allows network administrators to deploy authentication proxy on existing networks without changing the statically defined IP addresses of their network-connected devices.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Configuring Port to Application Mapping

This chapter describes the Cisco IOS Firewall Port to Application Mapping (PAM) feature. PAM enables CBAC-supported applications to be run on nonstandard ports. Using PAM, network administrators can customize access control for specific applications and services to meet the distinct needs of their networks.

For a complete description of the PAM commands in this chapter, refer to the chapter “Port to Application Mapping Commands” of the *Cisco IOS Security Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the “Identifying Supported Platforms” section in the chapter “Using Cisco IOS Software.”

In This Chapter

This chapter contains the following sections:

- [About Port to Application Mapping](#)
- [PAM Configuration Task List](#)
- [Monitoring and Maintaining PAM](#)
- [PAM Configuration Examples](#)

About Port to Application Mapping

Port to Application Mapping (PAM) is a feature of the Cisco IOS Firewall feature set. PAM allows you to customize TCP or UDP port numbers for network services or applications. PAM uses this information to support network environments that run services using ports that are different from the registered or well-known ports associated with an application.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Using the port information, PAM establishes a table of default port-to-application mapping information at the firewall. The information in the PAM table enables Context-based Access Control (CBAC) supported services to run on nonstandard ports. Previously, CBAC was limited to inspecting traffic using only the well-known or registered ports associated with an application. Now, PAM allows network administrators to customize network access control for specific applications and services.

PAM also supports host or subnet specific port mapping, which allows you to apply PAM to a single host or subnet using standard access control lists (ACLs). Host or subnet specific port mapping is done using standard ACLs.

This section contains the following sections:

- [How PAM Works](#)
- [System-Defined Port Mapping](#)
- [PAM and CBAC](#)
- [When to Use PAM](#)

How PAM Works

PAM generates a table of information that identifies specific applications with specific TCP or UDP port information. When the firewall router first starts up, the PAM table is populated with system-defined mapping information. As you customize the mapping information, the PAM table is modified with the new information. The information in the PAM table serves as the default port mapping for traffic passing through the firewall.

PAM works with CBAC to identify the applications associated with various port numbers, including services running on non-standard ports, as it inspect traffic passing through the firewall. Previously, CBAC was limited to inspecting traffic using only the well-known or registered ports associated with an application.

Entries in the PAM table provide three types of mapping information:

- [System-Defined Port Mapping](#)
- [User-Defined Port Mapping](#)
- [Host-Specific Port Mapping](#)

System-Defined Port Mapping

PAM creates a table, or database, of system-defined mapping entries using the well-known or registered port mapping information set up during the system start-up. The system-defined entries comprise all the services supported by CBAC, which requires the system-defined mapping information to function properly. The system-defined mapping information cannot be deleted or changed; that is, you cannot map HTTP services to port 21 (FTP) or FTP services to port 80 (HTTP).



Note

You can override the system-defined entries for specific hosts using the PAM host-specific option. Refer to the section [“Host-Specific Port Mapping”](#) in this chapter.

[Table 42](#) lists the default system-defined services and applications in the PAM table.

Table 42 **System-Defined Port Mapping**

Application Name	Well-Known or Registered Port Number	Protocol Description
cuseeme	7648	CU-SeeMe Protocol
exec	512	Remote Process Execution
ftp	21	File Transfer Protocol (control port)
http	80	Hypertext Transfer Protocol
h323	1720	H.323 Protocol (for example, MS NetMeeting, Intel Video Phone)
login	513	Remote login
mgcp	2427	Media Gateway Control Protocol
msrpc	135	Microsoft Remote Procedure Call
netshow	1755	Microsoft NetShow
real-audio-video	7070	RealAudio and RealVideo
rtsp	8559	Real Time Streaming Protocol
shell	514	Remote command
sip	5060	Session Initiation Protocol
smtp	25	Simple Mail Transfer Protocol
sqlnet	1521	SQL-NET
streamworks	1558	StreamWorks Protocol
sunrpc	111	SUN Remote Procedure Call
telnet	23	Telnet
tftp	69	Trivial File Transfer Protocol
vdolive	7000	VDOLive Protocol

This section has the following sections:

- [User-Defined Port Mapping](#)
- [Host-Specific Port Mapping](#)

User-Defined Port Mapping

Network services or applications that use non-standard ports require user-defined entries in the PAM table. For example, your network might run HTTP services on the non-standard port 8000 instead of on the system-defined default port (port 80). In this case, you can use PAM to map port 8000 with HTTP services. If HTTP services run on other ports, use PAM to create additional port mapping entries. After you define a port mapping, you can overwrite that entry at a later time by simply mapping that specific port with a different application.



Note

If you try to map an application to a system-defined port, a message appears that warns you of a mapping conflict.

User-defined port mapping information can also specify a range of ports for an application by establishing a separate entry in the PAM table for each port number in the range.

User-defined entries are saved with the default mapping information when you save the router configuration.

Host-Specific Port Mapping

User-defined entries in the mapping table can include host-specific mapping information, which establishes port mapping information for specific hosts or subnets. In some environments, it might be necessary to override the default port mapping information for a specific host or subnet.

With host-specific port mapping, you can use the same port number for different services on different hosts. This means that you can map port 8000 with HTTP services for one host, while mapping port 8000 with Telnet services for another host.

Host-specific port mapping also allows you to apply PAM to a specific subnet when that subnet runs a service that uses a port number that is different from the port number defined in the default mapping information. For example, hosts on subnet 192.168.21.0 might run HTTP services on non-standard port 8000, while other traffic through the firewall uses the default port for HTTP services, which is port 80.

Host-specific port mapping allows you to override a system-defined entry in the PAM table. For example, if CBAC finds an entry in the PAM table that maps port 25 (the system-defined port for SMTP) with HTTP for a specific host, CBAC identifies port 25 as HTTP protocol traffic on that host.



Note

If the host-specific port mapping information is the same as an existing system-defined or user-defined default entries, host-specific port changes have no effect.

PAM and CBAC

CBAC uses the information in the PAM table to identify a service or application from traffic flowing through the firewall. With PAM, CBAC can associate non-standard port numbers with specific protocols. For example, if you use PAM to map port 8000 with HTTP services, CBAC can determine that traffic using port 8000 is an HTTP application.

When to Use PAM

Here are a few examples of when you might want to use PAM:

- Use PAM to apply a non-standard port numbers for a service or application.
- Use PAM when a specific host or subnet uses a port number for an application that is different than the default port number established in the PAM table.
- Use PAM when different hosts use the same port number for different applications.

PAM Configuration Task List

See the following sections for PAM configuration tasks. Each task in the list indicates if it is optional or required:

- [Configuring Standard ACLs](#) (Optional)
- [Configuring PAM](#) (Required)
- [Verifying PAM](#) (Optional)

Configuring Standard ACLs

If you require PAM for a specific host or subnet, use the **access-list** (standard) command in global configuration mode to define an ACL:

Command	Purpose
Router(config)# access-list <i>access-list-number</i> permit <i>source</i> [<i>source-wildcard</i>]	(Optional) Creates a standard ACL that defines the specific host or subnet for host-specific PAM. For complete information on access-list command, refer to the <i>Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services</i> .

Configuring PAM

To configure PAM, use the **ip port-map** command in global configuration mode:

Command	Purpose
Router(config)# ip port-map <i>appl_name</i> port <i>port_num</i> [list <i>acl_num</i>]	Establishes a port mapping entry using the TCP or UDP port number and the application name. (Optional) Use the list option to associate this port mapping to the specific hosts in the ACL. (PAM uses standard access lists only.) If an access list is included, the hosts defined in that ACL have the application <i>appl_name</i> running on port <i>port_num</i> .

Verifying PAM

To verify the port mapping information, enter the **show ip port-map** command in privileged EXEC mode and review the entries:

```
Router# show ip port-map
```

This command displays all entries in the PAM table, including the system-defined entries.

For PAM configuration examples using the commands in this chapter, refer to the “[PAM Configuration Examples](#)” section at the end of this chapter.

Monitoring and Maintaining PAM

The following commands can be used to monitor and maintain PAM:

Command	Purpose
Router# show ip port-map [<i>appl_name</i> port <i>port_num</i>]	Displays the port mapping information, including the system-defined entries. Include the application name to display a list of entries by application. Include the port number to display the entries by port.
Router(config)# no ip port-map <i>appl_name</i> port <i>port_num</i> [list <i>acl_num</i>]	Deletes user-defined port mapping information. This command has no effect on the system-defined port mapping information.

PAM Configuration Examples

The following sections provide PAM configuration examples:

- [Mapping an Application to a Non-Standard Port Example](#)
- [Mapping an Application with a Port Range Example](#)
- [Invalid Port Mapping Entry Example](#)
- [Mapping an Application to a Port for a Specific Host Example](#)
- [Mapping an Application to a Port for a Subnet Example](#)
- [Overriding a System-Defined Port Mapping Example](#)
- [Mapping Different Applications to the Same Port Example](#)

Mapping an Application to a Non-Standard Port Example

In this example, non-standard port 8000 is established as the user-defined default port mapping for HTTP services:

```
ip port-map http port 8000
```

Mapping an Application with a Port Range Example

The following PAM entries establish a range of non-standard ports for HTTP services:

```
ip port-map http 8001
ip port-map http 8002
ip port-map http 8003
ip port-map http 8004
```

Invalid Port Mapping Entry Example

This example is not valid because it tries to establish port 21, which is the system-defined default port for FTP, as the user-defined port for HTTP services:

```
ip port-map http port 21
```

Mapping an Application to a Port for a Specific Host Example

In this example, a specific host uses port 8000 for FTP services. ACL 10 identifies the server address (192.168.32.43), while port 8000 is mapped with FTP services.

```
access-list 10 permit 192.168.32.43
ip port-map ftp port 8000 list 10
```

Mapping an Application to a Port for a Subnet Example

In this example, a specific subnet runs HTTP services on port 8080. ACL 50 identifies the subnet, while port 8080 is mapped with HTTP services.

```
access-list 50 permit 192.168.92.0 0.0.0.255
ip port-map http 8080 list 50
```

Overriding a System-Defined Port Mapping Example

In this example, a specific host runs HTTP services on port 25, which is the system-defined port number for SMTP services. This requires a host-specific PAM entry that overrides the system-defined default port mapping for HTTP, which is port 80. ACL 15 identifies the host address (192.168.33.33), while port 25 is mapped with HTTP services.

```
access-list 15 permit 192.168.33.33
ip port-map http port 25 list 15
```

Mapping Different Applications to the Same Port Example

In this example, the same port number is required by different services running on different hosts. Port 8000 is required for HTTP services for host 192.168.3.4, while port 8000 is also required for FTP services for host 192.168.5.6. ACL 10 and ACL 20 identify the specific hosts, while the PAM entries map the ports with the services for each ACL.

```
access-list 10 permit 192.168.3.4
access-list 20 permit 192.168.5.6
ip port-map http port 8000 list 10
ip port-map http ftp 8000 list 20
```

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and

coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



IPSec and IKE



Internet Key Exchange for IPSec VPNs



Configuring Internet Key Exchange for IPSec VPNs

This module describes how to configure the Internet Key Exchange (IKE) protocol for basic IP Security (IPSec) virtual private networks (VPNs). IKE is a key management protocol standard that is used in conjunction with the IPSec standard. IPSec is an IP security feature that provides robust authentication and encryption of IP packets.

IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard.

IKE is a hybrid protocol, which implements the Oakley key exchange and Skeme key exchange inside the Internet Security Association Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.)

Module History

This module was first published on May 2, 2005, and last updated on May 2, 2005.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all features. To find information about feature support and configuration, use the [“Feature Information for Configuring IKE for IPSec VPNs”](#) section on page 24.

Contents

- [Prerequisites for IKE Configuration, page 2](#)
- [Restrictions for IKE Configuration, page 2](#)
- [Information About Configuring IKE for IPSec VPNs, page 2](#)
- [How to Configure IKE for IPSec VPNs, page 4](#)
- [Configuration Examples for an IKE Configuration, page 19](#)
- [Where to Go Next, page 22](#)
- [Additional References, page 22](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for IKE Configuration

- You should be familiar with the concepts and tasks explained in the module “Configuring Security for VPNs with IPSec.”
- Ensure that your access control lists (ACLs) are compatible with IKE. Because IKE negotiation uses User Datagram Protocol (UDP) on port 500, your ACLs must be configured so that UDP port 500 traffic is not blocked at interfaces used by IKE and IPSec. In some cases you might need to add a statement to your ACLs to explicitly permit UDP port 500 traffic.

Restrictions for IKE Configuration

The following restrictions are applicable when configuring IKE negotiation:

- The initiating router *must not* have a certificate associated with the remote peer.
- The preshared key *must* be by fully qualified domain name (FQDN) on both peers. (To configure the preshared key, enter the **crypto isakmp key** command.)
- The communicating routers *must* have a FQDN host entry for each other in their configurations.
- The communicating routers *must* be configured to authenticate by hostname, *not* by IP address; thus, you should use the **crypto isakmp identity hostname** command.

Information About Configuring IKE for IPSec VPNs

To configure IKE for IPSec VPNs, you should understand the following concepts:

- [Supported Standards for Use with IKE, page 2](#)
- [IKE Benefits, page 4](#)
- [IKE Main Mode and Aggressive Mode, page 4](#)

Supported Standards for Use with IKE

Cisco implements the following standards:

- IPSec—IP Security Protocol. IPSec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer; it uses IKE to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.
- ISAKMP—Internet Security Association and Key Management Protocol. A protocol framework that defines payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of a security association.
- Oakley—A key exchange protocol that defines how to derive authenticated keying material.
- Skeme—A key exchange protocol that defines how to derive authenticated keying material, with rapid key refreshment.

The component technologies implemented for use by IKE include the following:

- **AES**—Advanced Encryption Standard. A cryptographic algorithm that protects sensitive, unclassified information. AES is privacy transform for IPSec and IKE and has been developed to replace the DES. AES is designed to be more secure than DES: AES offers a larger key size, while ensuring that the only known approach to decrypt a message is for an intruder to try every possible key. AES has a variable key length—the algorithm can specify a 128-bit key (the default), a 192-bit key, or a 256-bit key.
- **DES**—Data Encryption Standard. An algorithm that is used to encrypt packet data. IKE implements the 56-bit DES-CBC with Explicit IV standard. Cipher Block Chaining (CBC) requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPSec packet.

Cisco IOS software also implements Triple DES (168-bit) encryption, depending on the software versions available for a specific platform. Triple DES (3DES) is a strong form of encryption that allows sensitive information to be transmitted over untrusted networks. It enables customers, particularly in the finance industry, to utilize network-layer encryption.

**Note**

Cisco IOS images that have strong encryption (including, but not limited to, 56-bit data encryption feature sets) are subject to United States government export controls, and have a limited distribution. Images that are to be installed outside the United States require an export license. Customer orders might be denied or subject to delay because of United States government regulations. Contact your sales representative or distributor for more information, or send e-mail to export@cisco.com.

- **SEAL**—Software Encryption Algorithm. An alternative algorithm to software-based DES, 3DES, and AES. SEAL encryption uses a 160-bit encryption key and has a lower impact to the CPU when compared to other software-based algorithms.
- **Diffie-Hellman**—A public-key cryptography protocol that allows two parties to establish a shared secret over an unsecure communications channel. Diffie-Hellman is used within IKE to establish session keys. 768-bit (the default), 1024-bit, and 1536-bit Diffie-Hellman groups are supported.
- **MD5 (HMAC variant)**—Message Digest 5. A hash algorithm used to authenticate packet data. HMAC is a variant that provides an additional level of hashing.
- **SHA (HMAC variant)**—Secure Hash Algorithm. A hash algorithm used to authenticate packet data. HMAC is a variant that provides an additional level of hashing.
- **RSA signatures and RSA encrypted nonces**—RSA is the public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA signatures provide nonrepudiation, and RSA encrypted nonces provide repudiation. (Repudiation and nonrepudiation have to do with traceability.)

IKE interoperates with the following standard:

X.509v3 certificates—Used with the IKE protocol when authentication requires public keys. This certificate support allows the protected network to scale by providing the equivalent of a digital ID card to each device. When two devices intend to communicate, they exchange digital certificates to prove their identity (thus removing the need to manually exchange public keys with each peer or to manually specify a shared key at each peer).

IKE Benefits

IKE automatically negotiates IPSec security associations (SAs) and enables IPSec secure communications without costly manual preconfiguration. Specifically, IKE provides the following benefits:

- Eliminates the need to manually specify all the IPSec security parameters in the crypto maps at both peers.
- Allows you to specify a lifetime for the IPSec SA.
- Allows encryption keys to change during IPSec sessions.
- Allows IPSec to provide anti-replay services.
- Permits certification authority (CA) support for a manageable, scalable IPSec implementation.
- Allows dynamic authentication of peers.

IKE Main Mode and Aggressive Mode

IKE has two phases of key negotiation: phase 1 and phase 2. Phase 1 negotiates a security association (a key) between two IKE peers. The key negotiated in phase 1 enables IKE peers to communicate securely in phase 2. During phase 2 negotiation, IKE establishes keys (security associations) for other applications, such as IPSec.

Phase 1 negotiation can occur using main mode or aggressive mode. Main mode tries to protect all information during the negotiation, meaning that no information is available to a potential attacker. When main mode is used, the identities of the two IKE peers are hidden. Although this mode of operation is very secure, it is relatively costly in terms of the time it takes to complete the negotiation. Aggressive mode takes less time to negotiate keys between peers; however, it gives up some of the security provided by main mode negotiation. For example, the identities of the two parties trying to establish a security association are exposed to an eavesdropper.

The two modes serve different purposes and have different strengths. Main mode is slower than aggressive mode, but main mode is more secure and more flexible because it can offer an IKE peer more security proposals than aggressive mode. Aggressive mode is less flexible and not as secure, but much faster.

In Cisco IOS software, the two modes are not configurable. The default action for IKE authentication (rsa-sig, rsa-encr, or preshared) is to initiate main mode; however, in cases where there is no corresponding information to initiate authentication, and there is a preshared key associated with the hostname of the peer, Cisco IOS software can initiate aggressive mode. Cisco IOS software will respond in aggressive mode to an IKE peer that initiates aggressive mode.

How to Configure IKE for IPSec VPNs

If you do not want IKE to be used with your IPSec implementation, you can disable it at all IPSec peers via the **no crypto isakmp** command, skip the rest of this chapter, and begin your IPSec VPN.



Note

If you disable IKE, you will have to manually specify all the IPSec SAs in the crypto maps at all peers, the IPSec SAs of the peers will never time out for a given IPSec session, the encryption keys will never change during IPSec sessions between the peers, anti-replay services will not be available between the peers, and public key infrastructure (PKI) support cannot be used.

IKE is enabled by default. IKE does not have to be enabled for individual interfaces, but it is enabled globally for all interfaces at the router.

Perform the following tasks to provide authentication of IPSec peers, negotiate IPSec SAs, and establish IPSec keys:

- [Creating IKE Policies: Security Parameters for IKE Negotiation, page 5](#) (required)
- [Configuring IKE Authentication, page 9](#) (required)
- [Configuring IKE Mode Configuration, page 17](#)

Creating IKE Policies: Security Parameters for IKE Negotiation

An IKE policy defines a combination of security parameters to be used during the IKE negotiation. You must create an IKE policy at each peer participating in the IKE exchange.

If you do not configure any IKE policies, your router will use the default policy, which is always set to the lowest priority and which contains the default value of each parameter.

About IKE Policies

Because IKE negotiations must be protected, each IKE negotiation begins by agreement of both peers on a common (shared) IKE policy. This policy states which security parameters will be used to protect subsequent IKE negotiations and mandates how the peers are authenticated.

After the two peers agree upon a policy, the security parameters of the policy are identified by an SA established at each peer, and these SAs apply to all subsequent IKE traffic during the negotiation.

You can configure multiple, prioritized policies on each peer—each with a different combination of parameter values. However, at least one of these policies must contain exactly the same encryption, hash, authentication, and Diffie-Hellman parameter values as one of the policies on the remote peer. For each policy that you create, you assign a unique priority (1 through 10,000, with 1 being the highest priority).



Tip

If you are interoperating with a device that supports only one of the values for a parameter, your choice is limited to the value supported by the other device. Aside from this limitation, there is often a trade-off between security and performance, and many of these parameter values represent such a trade-off. You should evaluate the level of security risks for your network and your tolerance for these risks.

IKE Peers Agreeing Upon a Matching IKE Policy

When the IKE negotiation begins, IKE searches for an IKE policy that is the same on both peers. The peer that initiates the negotiation will send all its policies to the remote peer, and the remote peer will try to find a match. The remote peer looks for a match by comparing its own highest priority policy against the policies received from the other peer. The remote peer checks each of its policies in order of its priority (highest priority first) until a match is found.

A match is made when both policies from the two peers contain the same encryption, hash, authentication, and Diffie-Hellman parameter values, and when the remote peer's policy specifies a lifetime that is less than or equal to the lifetime in the policy being compared. (If the lifetimes are not identical, the shorter lifetime—from the remote peer's policy—will be used.)

If a match is found, IKE will complete negotiation, and IPSec security associations will be created. If no acceptable match is found, IKE refuses negotiation and IPSec will not be established.

**Note**

Depending on which authentication method is specified in a policy, additional configuration might be required (as described in the section “[Configuring IKE Authentication](#)”). If a peer’s policy does not have the required companion configuration, the peer will not submit the policy when attempting to find a matching policy with the remote peer.

Restrictions

If you are configuring an AES IKE policy, note the following restrictions:

- Your router must support IPSec and long keys (the “k9” subsystem).
- AES cannot encrypt IPSec and IKE traffic if an acceleration card is present.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp policy** *priority*
4. **encryption** {des | 3des | aes | aes 192 | aes 256}
5. **hash** {sha | md5}
6. **authentication** {rsa-sig | rsa-encr | pre-share}
7. **group** {1 | 2 | 5}
8. **lifetime** *seconds*
9. **exit**
10. **exit**
11. **show crypto isakmp policy**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto isakmp policy <i>priority</i> Example: Router(config)# crypto isakmp policy 10	Defines an IKE policy and enters config-isakmp configuration mode. <ul style="list-style-type: none"> <i>priority</i>—Uniquely identifies the IKE policy and assigns a priority to the policy. Valid values: 1 to 10,000; 1 is the highest priority.
Step 4	encryption {des 3des aes aes 192 aes 256} Example: Router(config-isakmp)# encryption aes 256	Specifies the encryption algorithm. By default, the des keyword is used. <ul style="list-style-type: none"> des—56-bit DES-CBC 3des—168-bit DES aes—128-bit AES aes 192—192-bit AES aes 256—256-bit AES
Step 5	hash {sha md5} Example: Router(config-isakmp)# hash sha	Specifies the hash algorithm. By default, SHA-1 (sha) is the used. Note MD5 has a smaller digest and is considered to be slightly faster than SHA-1.
Step 6	authentication {rsa-sig rsa-encr pre-share} Example: Router(config-isakmp)# authentication pre-share	Specifies the authentication method. By default, RSA signatures are used. <ul style="list-style-type: none"> rsa-sig—RSA signatures require that you configure your peer routers to obtain certificates from a CA. rsa-encr—RSA encrypted nonces require that you ensure each peer has the other peer's RSA public keys. pre-share—Preshared keys require that you separately configure these preshared keys.

	Command or Action	Purpose
Step 7	group {1 2 5} Example: Router(config-isakmp)# group 1	Specifies the Diffie-Hellman group identifier. By default, D-H group 1 is used. <ul style="list-style-type: none"> 1—768-bit Diffie-Hellman 2—1024-bit Diffie-Hellman 5—1536-bit Diffie-Hellman Note The 1024-bit and 1536-bit Diffie-Hellman options are harder to “crack,” but require more CPU time to execute.
Step 8	lifetime <i>seconds</i> Example: Router(config-isakmp)# lifetime 180	Specifies the lifetime of the IKE SA. <ul style="list-style-type: none"> <i>seconds</i>—Time, in seconds, before each SA expires. Valid values: 60 to 86,400 seconds; default value: 86,400. Note The shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPSec SAs can be set up more quickly.
Step 9	exit Example: Router(config-isakmp)# exit	Exits config-isakmp configuration mode.
Step 10	exit Example: Router(config)# exit	Exits the global configuration mode.
Step 11	show crypto isakmp policy Example: Router# show crypto isakmp policy	(Optional) Displays all existing IKE policies.
Step 12	—	Repeat these steps for each policy you want to create.

**Note**

These parameters apply to the IKE negotiations after the IKE SA is established.

Examples

The following sample output from the **show crypto isakmp policy** command displays a warning message after a user tries to configure an IKE encryption method that the hardware does not support:

```
Router# show crypto isakmp policy
```

```
Protection suite of priority 1
  encryption algorithm: AES - Advanced Encryption Standard (256 bit keys).
WARNING:encryption hardware does not support the configured
encryption method for ISAKMP policy 1
  hash algorithm:      Secure Hash Standard
  authentication method: Pre-Shared Key
```

```
Diffie-Hellman group:  #1 (768 bit)
lifetime:              3600 seconds, no volume limit
```

Troubleshooting Tips

- Clear (and reinitialize) IPSec SAs by using the **clear crypto sa EXEC** command.
Using the **clear crypto sa** command without parameters will clear out the full SA database, which will clear out active security sessions. You may also specify the **peer**, **map**, or **entry** keywords to clear out only a subset of the SA database. For more information, see the **clear crypto sa** command in the *Cisco IOS Security Command Reference*, Release 12.4.
- The default policy and default values for configured policies do not show up in the configuration when you issue the **show running-config** command. To see the default policy and any default values within configured policies, use the **show crypto isakmp policy** command.
- Any IPSec transforms or IKE encryption methods that the current hardware does not support should be disabled; they are ignored whenever an attempt to negotiate with the peer is made.

If a user enters an IPSec transform or an IKE encryption method that the hardware does not support, a warning message will be generated. These warning messages are also generated at boot time. When an encrypted card is inserted, the current configuration is scanned. If any IPSec transforms or IKE encryption methods are found that are not supported by the hardware, a warning message will be generated.

What to Do Next

Depending on which authentication method you specified in your IKE policies (RSA signatures, RSA encrypted nonces, or preshared keys), you must do certain additional configuration tasks before IKE and IPSec can successfully use the IKE policies. For information on completing these additional tasks, refer to the following section “[Configuring IKE Authentication](#).”

To configure an AES-based transform set, see the module “Configuring Security for VPNs with IPSec.”

Configuring IKE Authentication

After you have created at least one IKE policy in which you specified an authentication method (or accepted the default method), you need to configure an authentication method. IKE policies cannot be used by IPSec until the authentication method is successfully configured.

To configure IKE authentication, you should perform one of the following tasks, as appropriate:

- [Configuring RSA Keys Manually for RSA Encrypted Nonces, page 11](#)
- [Configuring Preshared Keys, page 13](#)
- Configuring RSA Keys to Obtain Certificates from a CA. For information on completing this task, see the module “Deploying RSA Keys Within a PKI.”

IKE Authentication Methods: Overview

IKE authentication consists of three options—RSA signatures, RSA encrypted nonces, and preshared keys. Each authentication method requires additional configuration as follows:

RSA Signatures

With RSA signatures, you can configure the peers to obtain certificates from a CA. (The CA must be properly configured to issue the certificates.) Using a CA can dramatically improve the manageability and scalability of your IPSec network. Additionally, RSA signature-based authentication uses only two public key operations, whereas RSA encryption uses four public key operations, making it costlier in terms of overall performance. To properly configure CA support, see the chapter “Implementing and Managing a PKI.”

The certificates are used by each peer to exchange public keys securely. (RSA signatures requires that each peer has the public signature key of the remote peer.) When both peers have valid certificates, they will automatically exchange public keys with each other as part of any IKE negotiation in which RSA signatures are used.

You can also exchange the public keys manually, as described in the section “[Configuring RSA Keys Manually for RSA Encrypted Nonces](#).”

RSA signatures provide nonrepudiation for the IKE negotiation. And, you can prove to a third party after the fact that you did indeed have an IKE negotiation with the remote peer.

RSA Encrypted Nonces

With RSA encrypted nonces, you must ensure that each peer has the public keys of the other peers.

Unlike RSA signatures, the RSA encrypted nonces method can not use certificates to exchange public keys. Instead, you ensure that each peer has the others’ public keys by one of the following methods:

- Manually configuring RSA keys as described in the section “[Configuring RSA Keys Manually for RSA Encrypted Nonces](#).”
- or
- Ensuring that an IKE exchange using RSA signatures with certificates has already occurred between the peers. (The peers’ public keys are exchanged during the RSA-signatures-based IKE negotiations if certificates are used.)

To make that the IKE exchange happens, specify two policies: a higher-priority policy with RSA encrypted nonces and a lower-priority policy with RSA signatures. When IKE negotiations occur, RSA signatures will be used the first time because the peers do not yet have each other’s public keys. Then future IKE negotiations can use RSA encrypted nonces because the public keys will have been exchanged.



Note This alternative requires that you already have CA support configured.

RSA encrypted nonces provide repudiation for the IKE negotiation; however, unlike RSA signatures, you cannot prove to a third party that you had an IKE negotiation with the remote peer.

Preshared Keys

With preshared keys, you must configure them as described in the section “[Configuring Preshared Keys](#).”

Preshared keys are clumsy to use if your secured network is large, and they do not scale well with a growing network. However, they do not require use of a CA, as do RSA signatures, and might be easier to set up in a small network with fewer than ten nodes. RSA signatures also can be considered more secure when compared with preshared key authentication.

**Note**

If RSA encryption is configured and signature mode is negotiated (and certificates are used for signature mode), the peer will request both signature and encryption keys. Basically, the router will request as many keys as the configuration will support. If RSA encryption is not configured, it will just request a signature key.

Prerequisites

You must have configured at least one IKE policy, which is where the authentication method was specified (or RSA signatures was accepted by default).

Configuring RSA Keys Manually for RSA Encrypted Nonces

To manually configure RSA keys, perform this task for each IPSec peer that uses RSA encrypted nonces in an IKE policy.

**Note**

This task can be performed only if a CA is not in use.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto key generate rsa** {general-keys | usage-keys} [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*]
4. **exit**
5. **show crypto key mypubkey rsa**
6. **configure terminal**
7. **crypto key pubkey-chain rsa**
8. **named-key** *key-name* [encryption | signature]
or
addressed-key *key-address* [encryption | signature]
9. **address** *ip-address*
10. **key-string** *key-string*
11. **quit**
12. Repeat these steps at each peer that uses RSA encrypted nonces in an IKE policy.
13. **exit**
14. **exit**
15. **show crypto key pubkey-chain rsa** [**name** *key-name* | **address** *key-address*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto key generate rsa {general-keys usage-keys} [label key-label] [exportable] [modulus modulus-size] Example: Router(config)# crypto key generate rsa general-keys modulus 360	Generates RSA keys. <ul style="list-style-type: none"> If a <i>key-label</i> argument is not specified, the default value, which is the fully qualified domain name (FQDN) of the router, is used.
Step 4	exit Example: Router(config)# exit	(Optional) Exits global configuration mode.
Step 5	show crypto key mypubkey rsa Example: Router# show crypto key mypubkey rsa	(Optional) Displays the generated RSA public keys.
Step 6	configure terminal Example: Router# configure terminal	Returns to global configuration mode.
Step 7	crypto key pubkey-chain rsa Example: Router(config)# crypto key pubkey-chain rsa	Enters public key configuration mode (so you can manually specify the RSA public keys of other devices).
Step 8	named-key key-name [encryption signature] Example: Router(config-pubkey-chain)# named-key otherpeer.example.com or addressed-key key-address [encryption signature] Example: Router(config-pubkey-chain)# addressed-key 10.1.1.2 encryption	Indicates which remote peer's RSA public key you are going to specify and enters public key configuration mode. If the remote peer uses its host name as its ISAKMP identity, use the named-key command and specify the remote peer's FQDN, such as somerouter.example.com, as the <i>key-name</i> . If the remote peer uses its IP address as its ISAKMP identity, use the addressed-key command and specify the remote peer's IP address as the <i>key-address</i> .

	Command or Action	Purpose
Step 9	address <i>ip-address</i> Example: Router(config-pubkey-key)# address 10.5.5.1	Specifies the IP address of the remote peer. If you use the named-key command, you need to use this command to specify the IP address of the peer.
Step 10	key-string <i>key-string</i> Example: Router(config-pubkey-key)# key-string Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973 Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5 Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8 Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21	Specifies the RSA public key of the remote peer. (This key was previously viewed by the administrator of the remote peer when the RSA keys of the remote router were generated.)
Step 11	quit Example: Router(config-pubkey-k)# quit	Returns to public key chain configuration mode.
Step 12	—	Repeat these steps at each peer that uses RSA encrypted nonces in an IKE policy.
Step 13	exit Example: Router(config-pubkey-c)# exit	Returns to global configuration mode.
Step 14	exit Example: Router(config)# exit	Returns to EXEC mode.
Step 15	show crypto key pubkey-chain rsa [<i>name key-name</i> <i>address key-address</i>] Example: Router# show crypto key pubkey-chain rsa	(Optional) Displays either a list of all RSA public keys that are stored on your router or details of a particular RSA key that is stored on your router.

Configuring Preshared Keys

To configure preshared keys, perform these steps at each peer that uses preshared keys in an IKE policy.

Setting ISAKMP Identity for Preshared Keys

You should set the ISAKMP identity for each peer that uses preshared keys in an IKE policy.

When two peers use IKE to establish IPsec SAs, each peer sends its identity to the remote peer. Each peer sends either its host name or its IP address, depending on how you have set the ISAKMP identity of the router.

By default, a peer's ISAKMP identity is the IP address of the peer. If appropriate, you could change the identity to be the peer's host name instead. As a general rule, set the identities of all peers the same way—either all peers should use their IP addresses or all peers should use their hostnames. If some peers use their host names and some peers use their IP addresses to identify themselves to each other, IKE negotiations could fail if the identity of a remote peer is not recognized and a DNS lookup is unable to resolve the identity.

Mask Preshared Keys

A mask preshared key allows a group of remote users with the same level of authentication to share an IKE preshared key. The preshared key of the remote peer must match the preshared key of the local peer for IKE authentication to occur.

A mask preshared key is usually distributed through a secure out-of-band channel. In a remote peer-to-local peer scenario, any remote peer with the IKE preshared key configured can establish IKE SAs with the local peer.

If you specify the **mask** keyword with the **crypto isakmp key** command, it is up to you to use a subnet address, which will allow more peers to share the same key. That is, the preshared key is no longer restricted to use between two users.



Note

Using 0.0.0.0 as a subnet address is not recommended because it encourages group preshared keys, which allow all peers to have the same group key, thereby reducing the security of your user authentication.

Disable Xauth on a Specific IPsec Peer

Disabling Extended Authentication (Xauth) for static IPsec peers prevents the routers from being prompted for Xauth information—username and password.

Without the ability to disable Xauth, a user cannot select which peer on the same crypto map should use Xauth. That is, if a user has router-to-router IPsec on the same crypto map as a VPN-client-to-Cisco-IOS IPsec, both peers are prompted for a username and password. In addition, a remote static peer (a Cisco IOS router) cannot establish an IKE SA with the local Cisco IOS router. (Xauth is not an optional exchange, so if a peer does not respond to an Xauth request, the IKE SA is deleted.) Thus, the same interface cannot be used to terminate IPsec to VPN clients (that need Xauth) as well as other Cisco IOS routers (that cannot respond to Xauth) unless this feature is implemented.



Note

Xauth can be disabled only if preshared keys are used as the authentication mechanism for the given crypto map.

Restrictions

- Preshared do not scale well with a growing network.
- Mask preshared keys have the following restrictions:
 - The SA cannot be established between the IPsec peers until all IPsec peers are configured for the same preshared key.

- The mask preshared key must be distinctly different for remote users requiring varying levels of authorization. You must configure a new preshared key for each level of trust and assign the correct keys to the correct parties. Otherwise, an untrusted party may obtain access to protected data.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp identity {address | hostname}**
4. **ip host *hostname* *address1* [*address2*...*address8*]**
5. **crypto isakmp key *keystring* **address** *peer-address* [**mask**] [**no-xauth**]**
or
crypto isakmp key *keystring* **hostname *hostname* [**no-xauth**]**
6. **crypto isakmp key *keystring* **address** *peer-address* [**mask**] [**no-xauth**]**
or
crypto isakmp key *keystring* **hostname *hostname* [**no-xauth**]**
7. Repeat these steps for each peer that uses preshared keys.

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto isakmp identity {address hostname} Example: Router(config)# crypto isakmp identity address	Specifies the peer's ISAKMP identity by IP address or by hostname at the local peer. <ul style="list-style-type: none"> address—Typically used when there is only one interface (and therefore only one IP address) that will be used by the peer for IKE negotiations, and the IP address is known. hostname—Should be used if there is more than one interface on the peer that might be used for IKE negotiations, or if the interface's IP address is unknown (such as with dynamically assigned IP addresses).
Step 4	ip host hostname address1 [address2...address8] Example: Router(config)# ip host RemoteRouter.example.com 192.168.0.1	If the local peer's ISAKMP identity was specified using a hostname, maps the peer's host name to its IP address(es) at all the remote peers. (This step might be unnecessary if the hostname or address is already mapped in a DNS server.)
Step 5	crypto isakmp key keystring address peer-address [mask] [no-xauth] Example: Router(config)# crypto isakmp key sharedkeystring address 192.168.1.33 no-xauth or crypto isakmp key keystring hostname hostname [no-xauth] Example: Router(config) crypto isakmp key sharedkeystring hostname RemoteRouter.example.com	Specifies at the local peer the shared key to be used with a particular remote peer. If the remote peer specified its ISAKMP identity with an address, use the address keyword in this step; otherwise use the hostname keyword in this step. <ul style="list-style-type: none"> no-xauth—Prevents the router from prompting the peer for Xauth information. Use this keyword if router-to-router IPSec is on the same crypto map as VPN-client-to-Cisco IOS IPSec. <p>Note According to the design of preshared key authentication in IKE main mode, preshared keys must be based on the IP address of the peers. Although you can send hostname as the identity of preshared key authentication, the key is searched on the IP address of the peer; if the key is not found (based on the IP address) the negotiation will fail.</p>

	Command or Action	Purpose
Step 6	<pre>crypto isakmp key <i>keystring</i> address <i>peer-address</i> [<i>mask</i>] [<i>no-xauth</i>]</pre> <p>Example:</p> <pre>Router(config) crypto isakmp key sharedkeystring address 10.0.0.1</pre> <p>or</p> <pre>crypto isakmp key <i>keystring</i> <i>hostname</i> <i>hostname</i> [no-xauth]</pre> <p>Example:</p> <pre>Router(config) crypto isakmp key sharedkeystring hostname LocalRouter.example.com</pre>	<p>Specifies at the remote peer the shared key to be used with the local peer.</p> <p>This is the same key you just specified at the local peer.</p> <p>If the local peer specified its ISAKMP identity with an address, use the address keyword in this step; otherwise use the hostname keyword in this step.</p>
Step 7	—	Repeat these steps at each peer that uses preshared keys in an IKE policy.

Configuring IKE Mode Configuration

Perform the following task to configure IKE mode configuration.

About IKE Mode Configuration

IKE mode configuration, as defined by the Internet Engineering Task Force (IETF) , allows a gateway to download an IP address (and other network level configuration) to the client as part of an IKE negotiation. Using this exchange, the gateway gives IP addresses to the IKE client to be used as an “inner” IP address encapsulated under IPSec. This method provides a known IP address for the client that can be matched against IPSec policy.

To implement IPSec VPNs between remote access clients that have dynamic IP addresses and a corporate gateway, you have to dynamically administer scalable IPSec policy on the gateway once each client is authenticated. With IKE Mode Configuration, the gateway can set up scalable policy for a very large set of clients irrespective of the IP addresses of those clients.

There are two types of IKE Mode Configuration:

- Gateway initiation—Gateway initiates the configuration mode with the client. Once the client responds, the IKE modifies the identity of the sender, the message is processed, and the client receives a response.
- Client initiation—Client initiates the configuration mode with the gateway. The gateway responds with an IP address that it has allocated for the client.

Restrictions

IKE Mode Configuration has the following restrictions:

- Interfaces with crypto maps that are configured for IKE Mode Configuration may experience a slightly longer connection setup time, which is true even for IKE peers that refuse to be configured or do not respond to the configuration mode request. In both cases, the gateway initiates the configuration of the client.
- This feature was not designed to enable the configuration mode for every IKE connection by default. Configure this feature at the global crypto map level.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip local pool** *pool-name start-addr end-addr*
4. **crypto isakmp client configuration address-pool local** *pool-name*
5. **crypto map** *tag* **client configuration address** [**initiate** | **respond**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip local pool pool-name start-addr end-addr Example: Router(config) ip local pool ire 172.16.23.0 172.16.23.255	Defines an existing local address pool that defines a set of addresses.
Step 4	crypto isakmp client configuration address-pool local pool-name Example: Router(config) crypto isakmp client configuration address-pool local ire	References the local address pool in the IKE configuration.
Step 5	crypto map tag client configuration address [initiate respond] Example: Router(config)# crypto map dyn client configuration address initiate	Configures IKE Mode Configuration in global crypto map configuration mode.

Configuration Examples for an IKE Configuration

This section contains the following configuration examples:

- [Creating IKE Policies: Examples, page 19](#)
- [Configuring IKE Authentication: Example, page 21](#)

Creating IKE Policies: Examples

This section contains the following examples, which show how to configure a 3DES IKE policy and an AES IKE policy:

- [Creating 3DES IKE Policies: Example, page 20](#)
- [Creating an AES IKE Policy: Example, page 20](#)

Creating 3DES IKE Policies: Example

This example creates two IKE policies, with policy 15 as the highest priority, policy 20 as the next priority, and the existing default priority as the lowest priority. It also creates a preshared key to be used with policy 20 with the remote peer whose IP address is 192.168.224.33.

```
crypto isakmp policy 15
  encryption 3des
  hash md5
  authentication rsa-sig
  group 2
  lifetime 5000
!
crypto isakmp policy 20
  authentication pre-share
  lifetime 10000
!
crypto isakmp key 1234567890 address 192.168.224.33
```

In the example, the encryption des of policy 15 would not appear in the written configuration because this is the default value for the encryption algorithm parameter.

If the **show crypto isakmp policy** command is issued with this configuration, the output is as follows:

```
Protection suite priority 15
encryption algorithm:3DES - Triple Data Encryption Standard (168 bit keys)
hash algorithm:Message Digest 5
authentication method:Rivest-Shamir-Adleman Signature
Diffie-Hellman group:#2 (1024 bit)
lifetime:5000 seconds, no volume limit
Protection suite priority 20
encryption algorithm:DES - Data Encryption Standard (56 bit keys)
hash algorithm:Secure Hash Standard
authentication method:preshared Key
Diffie-Hellman group:#1 (768 bit)
lifetime:10000 seconds, no volume limit
Default protection suite
encryption algorithm:DES - Data Encryption Standard (56 bit keys)
hash algorithm:Secure Hash Standard
authentication method:Rivest-Shamir-Adleman Signature
Diffie-Hellman group:#1 (768 bit)
lifetime:86400 seconds, no volume limit
```

Note that although the output shows “no volume limit” for the lifetimes, you can configure only a time lifetime (such as 86,400 seconds); volume-limit lifetimes are not configurable.

Creating an AES IKE Policy: Example

The following example is sample output from the **show running-config** command. In this example, the AES 256-bit key is enabled.

```
Current configuration : 1665 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname "Router1"
!
!
ip subnet-zero
!
```

```

!
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 10
  encryption aes 256
  authentication pre-share
  lifetime 180
crypto isakmp key cisco123 address 10.0.110.1
!
!
crypto ipsec transform-set aesset esp-aes 256 esp-sha-hmac
  mode transport
!
crypto map aesmap 10 ipsec-isakmp
  set peer 10.0.110.1
  set transform-set aesset
  match address 120
!
.
.
.

```

Configuring IKE Authentication: Example

The following example shows how to manually specify the RSA public keys of two IPSec peer—the peer at 10.5.5.1 uses general-purpose keys, and the other peer uses special-usage keys:

```

crypto key pubkey-chain rsa
  named-key otherpeer.example.com
  address 10.5.5.1
  key-string
005C300D 06092A86 4886F70D 01010105
00034B00 30480241 00C5E23B 55D6AB22
04AEF1BA A54028A6 9ACC01C5 129D99E4
64CAB820 847EDAD9 DF0B4E4C 73A05DD2
BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
D58AD221 B583D7A4 71020301 0001
  quit
  exit
  addressed-key 10.1.1.2 encryption
  key-string
00302017 4A7D385B 1234EF29 335FC973
2DD50A37 C4F4B0FD 9DADE748 429618D5
18242BA3 2EDFBDD3 4296142A DDF7D3D8
08407685 2F2190A0 0B43F1BD 9A8A26DB
07953829 791FCDE9 A98420F0 6A82045B
90288A26 DBC64468 7789F76E EE21
  quit
  exit
  addressed-key 10.1.1.2 signature
  key-string
0738BC7A 2BC3E9F0 679B00FE 53987BCC
01030201 42DD06AF E228D24C 458AD228
58BB5DDD F4836401 2A2D7163 219F882E
64CE69D4 B583748A 241BED0F 6E7F2F16
0DE0986E DF02031F 4B0B0912 F68200C4
C625C389 0BFF3321 A2598935 C1B1
  quit
  exit

```

```
exit
```

Where to Go Next

After you have successfully configured IKE negotiation, you can begin configuring IPSec. For information on completing these tasks, see the module “Configuring Security for VPNs With IPSec.”

Additional References

The following sections provide references related to configuring IKE for IPSec VPNs.

Related Documents

Related Topic	Document Title
IPSec configuration	“Configuring Security for VPNs with IPSec” module
Configuring RSA keys to obtain certificates from a CA	“Deploying RSA Keys Within a PKI” module
IKE, IPSec, and PKI configuration commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<i>Cisco IOS Security Command Reference</i> , Release 12.4

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2408	<i>Internet Security Association and Key Management Protocol (ISAKMP)</i>
RFC 2409	<i>The Internet Key Exchange (IKE)</i>
RFC 2412	<i>The OAKLEY Key Determination Protocol</i>

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Glossary

anti-replay—Security service in which the receiver can reject old or duplicate packets to protect itself against replay attacks. IPsec provides optional anti-replay services by use of a sequence number and the use of authentication.

data authentication—Verification of the integrity and origin of the data.

Data authentication can refer either to integrity alone or to both of these concepts (although data origin authentication is dependent upon data integrity).

peer—In the context of this chapter, a “peer” is a router or other device that participates in IPsec and IKE.

PFS—perfect forward secrecy. Cryptographic characteristic associated with a derived shared secret value. With PFS, if one key is compromised, previous and subsequent keys are not also compromised, because subsequent keys are not derived from previous keys.

repudiation—Quality that prevents a third party from being able to prove that a communication between two other parties ever took place. Repudiation is a desirable quality if you do not want your communications to be traceable.

nonrepudiation—Quality that allows a third party to prove that a communication between two other parties took place. Nonrepudiation is desirable if you want to be able to trace your communications and prove that they occurred.

SA—security association. How two or more entities utilize security services to communicate securely.

For example, an IPsec SA defines the encryption algorithm (if used), the authentication algorithm, and the shared session key to be used during the IPsec connection. Both IPsec and IKE require and use SAs to identify the parameters of their connections. IKE can negotiate and establish its own SA. The IPsec SA is established either by IKE or by manual user configuration.



Note

Refer to *Internetworking Terms and Acronyms* for terms not included in this glossary.

Feature Information for Configuring IKE for IPsec VPNs

[Table 43](#) lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for a specific command was introduced, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Note

[Table 43](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 43 *Feature Information for Configuring IKE for IPsec VPNs*

Feature Name	Software Releases	Feature Configuration Information
Ability to Disable Extended Authentication for Static IPsec Peers	12.2(4)T	<p>This feature allows a user to disable Xauth while configuring the preshared key for router-to-router IPsec. Thus, the router will not prompt the peer for a username and password, which are transmitted when Xauth occurs for VPN-client-to-Cisco-IOS IPsec.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> • Configuring Preshared Keys <p>The following command was modified by this feature: crypto isakmp key</p>
Advanced Encryption Standard (AES)	12.2(8)T	<p>This feature adds support for the new encryption standard AES, which is a privacy transform for IPsec and IKE and has been developed to replace DES.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Supported Standards for Use with IKE • Creating IKE Policies: Security Parameters for IKE Negotiation <p>The following commands were modified by this feature: crypto ipsec transform-set, encryption (IKE policy), show crypto isakmp policy, show crypto ipsec transform-set</p>
SEAL Encryption	12.3(7)T	<p>This feature adds support for SEAL encryption in IPsec.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> • Supported Standards for Use with IKE <p>The following command was modified by this feature: crypto ipsec transform-set</p>
IKE Extended Authentication (Xauth)	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
Wildcard Pre-Shared Key	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
IKE - Diffie-Hellman (768 Bit or 1024 Bit) PKCS #3 Support	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Table 43 *Feature Information for Configuring IKE for IPSec VPNs (continued)*

Feature Name	Software Releases	Feature Configuration Information
IKE Phase 1 Main Mode and Phase 1 Aggressive Mode	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
IKE - RSA Signature	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Call Admission Control for IKE

First Published: May 17, 2004

Last Updated: August 04, 2008

The Call Admission Control for IKE feature describes the application of Call Admission Control (CAC) to the Internet Key Exchange (IKE) protocol in Cisco IOS. CAC limits the number of simultaneous IKE security associations (SAs) (that is, calls to CAC) that a router can establish.

History for the Call Admission Control for IKE Feature

Release	Modification
12.3(8)T	This feature was introduced.
12.2(18)SXD1	This feature was integrated into Cisco IOS Release 12.2(18)SXD1 on the Cisco 6500 and Cisco 7600.
12.4(6)T	This feature was integrated into Cisco IOS Release 12.4(6)T. The ability to configure a limit on the number of in-negotiation IKE connections was added only to this and subsequent T-train releases.
12.2(33)SRA	This feature was integrated into Cisco IOS Release 12.2(33)SRA on the Cisco 7600. The in-negotiation IKE connection feature was not added to this SRA release.
12.2(33)SXH	This feature was integrated into Cisco IOS Release 12.2(33)SXH. The in-negotiation IKE connection feature was not added to this SXH release.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008 Cisco Systems, Inc. All rights reserved.

Contents

- [Prerequisites for Call Admission Control for IKE, page 2](#)
- [Information About Call Admission Control for IKE, page 2](#)
- [How to Configure Call Admission Control for IKE, page 3](#)
- [Verifying the Call Admission Control for IKE Configuration, page 5](#)
- [Configuration Examples for Call Admission Control for IKE, page 6](#)
- [Additional References, page 7](#)
- [Command Reference, page 8](#)

Prerequisites for Call Admission Control for IKE

- Configure IKE on the router. Refer to the *Cisco IOS Security Configuration Guide*, Release 12.3.

Information About Call Admission Control for IKE

To configure CAC for IKE, you need to understand the following concepts:

- [IKE Session, page 2](#)
- [Security Association Limit, page 2](#)
- [System Resource Usage, page 3](#)

IKE Session

There are two ways to limit the number of IKE SAs that a router can establish to or from another router:

- Configure the absolute IKE SA limit by entering the **crypto call admission limit** command. The router drops new IKE SA requests when the value has been reached.
- Configure the system resource limit by entering the **call admission limit** command. The router drops new IKE SA requests when the level of system resources that are configured in the unit of charge is being used.

For information about using these commands, see the “[Command Reference](#)” section on page 8.

CAC is applied only to new SAs (that is, when an SA does not already exist between the peers). Every effort is made to preserve existing SAs. Only new SA requests will ever be denied due to a lack of system resources or because the configured IKE SA limit has been reached.

Security Association Limit

An SA is a description of how two or more entities will utilize security services to communicate securely on behalf of a particular data flow. IKE requires and uses SAs to identify the parameters of its connections. IKE can negotiate and establish its own SA. An IKE SA is used by IKE only, and it is bidirectional. An IKE SA cannot limit IPsec.

IKE drops SA requests based on a user-configured SA limit. To configure an IKE SA limit, enter the **crypto call admission limit** command. When there is a new SA request from a peer router, IKE determines if the number of active IKE SAs plus the number of SAs being negotiated meets or exceeds the configured SA limit. If the number is greater than or equal to the limit, the new SA request is rejected and a syslog is generated. This log contains the source destination IP address of the SA request.

Limit on Number of In-negotiation IKE Connections

Effective with Cisco IOS Release 12.4(6)T, a limit on the number of in-negotiation IKE connections can be configured. This type of IKE connection represents either an aggressive mode IKE SA or a main mode IKE SA prior to its authentication and actual establishment.

Using the **crypto call admission limit ike in-negotiation-sa {number}** command allows the configured number of in-negotiation IKE SAs to start negotiation without contributing to the maximum number of IKE SAs allowed.

System Resource Usage

CAC polls a global resource monitor so that IKE knows when the router is running short of CPU cycles or memory buffers. You can configure a resource limit, from 1 to 100000, that represents the level of system resources that are configured in the unit of charge. When that level of resources is being used, IKE drops (will not accept new) SA requests. To configure the system resource usage, enter the **call admission control** command.

How to Configure Call Admission Control for IKE

This section contains the following procedures:

- [Configure the IKE Security Association Limit, page 3](#) (optional)
- [Configure the System Resource Limit, page 4](#) (optional)



Note

You must perform one of the procedures.

Configure the IKE Security Association Limit

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto call admission limit {ike {in-negotiation-sa *number* | sa *number* } }**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto call admission limit {ike {in-negotiation-sa number} sa number}} Example: Router(config)# crypto call admission limit ike sa 25	Specifies the maximum number of IKE SAs that the router can establish before IKE begins rejecting new SA requests. Note An ISAKMP connection needs to be built in two directions. If you have 500 spokes in your network, you should set this value at a minimum of 1000 (500 x 2).
Step 4	exit Example: Router(config)# exit	Returns to privileged EXEC mode.

Configure the System Resource Limit

SUMMARY STEPS

1. enable
2. configure terminal
3. call admission limit *charge*
4. exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	call admission limit <i>charge</i> Example: Router(config)# call admission limit 90000	Sets the level of the system resources that, when used, causes IKE to stop accepting new SA requests. <ul style="list-style-type: none"> <i>charge</i>—Valid values are 1 to 100000.
Step 4	exit Example: Router(config)# exit	Returns to privileged EXEC mode.

Verifying the Call Admission Control for IKE Configuration

To verify the CAC for IKE configuration, perform the following steps.

SUMMARY STEPS

1. show call admission statistics
2. show crypto call admission statistics

DETAILED STEPS



Note

For detailed field descriptions of the command output, see the [“Command Reference” section on page 8](#).

Step 1 show call admission statistics

Use this command to monitor the global CAC configuration parameters and the behavior of CAC.

```
Router# show call admission statistics
```

```
Total Call admission charges: 0, limit 25
Total calls rejected 12, accepted 51
Load metric: charge 0, unscaled 0
```

Step 2 show crypto call admission statistics

Use this command to monitor Crypto CAC statistics.

```
Router# show crypto call admission statistics
```

```
-----
Crypto Call Admission Control Statistics
-----
System Resource Limit: 0    Max IKE SAs 0
Total IKE SA Count:      0    active:      0    negotiating: 0
Incoming IKE Requests: 0    accepted:   0    rejected:   0
Outgoing IKE Requests: 0    accepted:   0    rejected:   0
Rejected IKE Requests: 0    rsrc low:   0    SA limit:   0
-----
```

Configuration Examples for Call Admission Control for IKE

This section provides the following configuration examples:

- [Configuring the IKE Security Association Limit: Example, page 6](#)
- [Configuring the System Resource Limit: Example, page 6](#)

Configuring the IKE Security Association Limit: Example

The following example shows how to specify that there can be a maximum of 25 SAs before IKE starts rejecting new SA requests:

```
Router(config)# crypto call admission limit ike sa 25
```

Configuring the System Resource Limit: Example

The following example shows how to specify that IKE should drop SA requests when the level of system resources that are configured in the unit of charge reaches 90000:

```
Router(config)# call admission limit 90000
```

Additional References

The following sections provide references related to Call Admission Control for IKE.

Related Documents

Related Topic	Document Title
IKE commands	<ul style="list-style-type: none">Cisco IOS Security Command Reference

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC #2409	<i>The Internet Key Exchange</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **call admission limit**
- **clear crypto call admission statistics**
- **crypto call admission limit**
- **show call admission statistics**
- **show crypto call admission statistics**

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.



Certificate to ISAKMP Profile Mapping

First Published: May 17, 2004

Last Updated: August 21, 2007

The Certificate to ISAKMP Profile Mapping feature enables you to assign an Internet Security Association and Key Management Protocol (ISAKMP) profile to a peer on the basis of the contents of arbitrary fields in the certificate. In addition, this feature allows you to assign a group name to those peers that are assigned an ISAKMP profile.

History for Certificate to ISAKMP Profile Mapping Feature

Release	Modification
12.3(8)T	This feature was introduced.
12.2(33)SRA	This feature was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This feature was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Certificate to ISAKMP Profile Mapping, page 2](#)
- [Restrictions for Certificate to ISAKMP Profile Mapping, page 2](#)
- [Information About Certificate to ISAKMP Profile Mapping, page 2](#)
- [How to Configure Certificate to ISAKMP Profile Mapping, page 3](#)
- [Configuration Examples for Certificate to ISAKMP Profile Mapping, page 7](#)
- [Additional References, page 10](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Command Reference, page 12](#)

Prerequisites for Certificate to ISAKMP Profile Mapping

- You should be familiar with configuring certificate maps.
- You should be familiar with configuring ISAKMP profiles.

Restrictions for Certificate to ISAKMP Profile Mapping

This feature will not be applicable if you use Rivest, Shamir, and Adelman- (RSA-) signature or RSA-encryption authentication without certificate exchange. ISAKMP peers must be configured to do RSA-signature or RSA-encryption authentication using certificates.

Information About Certificate to ISAKMP Profile Mapping

To configure the Certificate to ISAKMP Profile Mapping feature, you should understand the following concepts:

- [Certificate to ISAKMP Profile Mapping Overview, page 2](#)
- [How Certificate to ISAKMP Profile Mapping Works, page 2](#)
- [Assigning an ISAKMP Profile and Group Name to a Peer, page 3](#)

Certificate to ISAKMP Profile Mapping Overview

Prior to Cisco IOS Release 12.3(8)T, the only way to map a peer to an ISAKMP profile was as follows. The ISAKMP identity field in the ISAKMP exchange was used for mapping a peer to an ISAKMP profile. When certificates were used for authentication, the ISAKMP identity payload contained the subject name from the certificate. If a certificate authority (CA) did not provide the required group value in the first Organizational Unit (OU) field of a certificate, an ISAKMP profile could not be assigned to a peer.

Effective with Cisco IOS Release 12.3(8)T, a peer can still be mapped as explained above. However, the Certificate to ISAKMP Profile Mapping feature enables you to assign an ISAKMP profile to a peer on the basis of the contents of arbitrary fields in the certificate. You are no longer limited to assigning an ISAKMP profile on the basis of the subject name of the certificate. In addition, this feature allows you to assign a group to a peer to which an ISAKMP profile has been assigned.

How Certificate to ISAKMP Profile Mapping Works

[Figure 1](#) illustrates how certificate maps may be attached to ISAKMP profiles and assigned group names.

Figure 1 *Certificate Maps Mapped for Profile Group Assignment*



A certificate map can be attached to only one ISAKMP profile although an ISAKMP profile can have several certificate maps attached to it.

Certificate maps provide the ability for a certificate to be matched with a given set of criteria. ISAKMP profiles can bind themselves to certificate maps, and if the presented certificate matches the certificate map present in an ISAKMP profile, the peer will be assigned the ISAKMP profile. If the ISAKMP profile contains a client configuration group name, the same group name will be assigned to the peer. This ISAKMP profile information will override the information in the ID_KEY_ID identity or in the first OU field of the certificate.

Assigning an ISAKMP Profile and Group Name to a Peer

To assign an ISAKMP profile to a peer on the basis of arbitrary fields in the certificate, use the **match certificate** command after the ISAKMP profile has been defined.

To associate a group name with an ISAKMP profile that will be assigned to a peer, use the **client configuration group** command, also after the ISAKMP profile has been defined.

How to Configure Certificate to ISAKMP Profile Mapping

This section contains the following procedures:

- [Mapping the Certificate to the ISAKMP Profile, page 4](#) (required)
- [Verifying That the Certificate Has Been Mapped, page 4](#) (optional)
- [Assigning the Group Name to the Peer, page 5](#) (required)
- [Monitoring and Maintaining Your Certificate to ISAKMP Profile Mapping, page 6](#) (optional)

Mapping the Certificate to the ISAKMP Profile

To map the certificate to the ISAKMP profile, perform the following steps. This configuration will enable you to assign the ISAKMP profile to a peer on the basis of the contents of arbitrary fields in the certificate.

SUMMARY STEPS

- `enable`
- `configure terminal`
- `crypto isakmp profile profile-name`
- `match certificate certificate-map`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure <i>terminal</i> Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto isakmp profile <i>profile-name</i> Example: Router (config)# crypto isakmp profile vpnprofile	Defines an ISAKMP profile and enters into crypto ISAKMP profile configuration mode.
Step 4	match certificate <i>certificate-map</i> Example: Router (conf-isa-prof)# match certificate map1	Accepts the name of a certificate map.

Verifying That the Certificate Has Been Mapped

The following **show** command may be used to verify that the subject name of the certificate map has been properly configured.

SUMMARY

- `enable`
- `show crypto ca certificates`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	show crypto ca certificates Example: Router# show crypto ca certificates	Displays information about your certificate.

Assigning the Group Name to the Peer

To associate a group name with a peer when the peer is mapped to an ISAKMP profile, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp profile** *profile-name*
4. **client configuration group** *group-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto isakmp profile <i>profile-name</i> Example: Router (config)# crypto isakmp profile vpnprofile	Defines an ISAKMP profile and enters into isakmp profile configuration mode.
Step 4	client configuration group <i>group-name</i> Example: Router (conf-isa-prof)# client configuration group group1	Accepts the name of a group that will be assigned to a peer when the peer is assigned this crypto ISAKMP profile.

Monitoring and Maintaining Your Certificate to ISAKMP Profile Mapping

To monitor and maintain your certificate to ISAKMP profile mapping, you may use the following **debug** command.

SUMMARY STEPS

1. **enable**
2. **debug crypto isakmp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example: Router# enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	debug crypto isakmp	Displays output showing that the certificate has gone through certificate map matching and that the certificate matches the ISAKMP profile.
	Example: Router# debug crypto isakmp	The command may also be used to verify that the peer has been assigned a group.

Configuration Examples for Certificate to ISAKMP Profile Mapping

This section contains the following configuration examples:

- [Certificates Mapped to the ISAKMP Profile on the Basis of Arbitrary Fields: Example, page 7](#)
- [Group Name Assigned to a Peer That Is Associated with an ISAKMP Profile: Example, page 7](#)
- [Mapping a Certificate to an ISAKMP Profile Verification: Example, page 8](#)
- [Group Name Assigned to a Peer Verification: Example, page 9](#)

Certificates Mapped to the ISAKMP Profile on the Basis of Arbitrary Fields: Example

The following configuration example shows that whenever a certificate contains “ou = green,” the ISAKMP profile “cert_pro” will be assigned to the peer:

```
crypto pki certificate map cert_map 10
  subject-name co ou = green
!
!
crypto isakmp identity dn
crypto isakmp profile cert_pro
  ca trust-point 2315
  ca trust-point LaBcA
  initiate mode aggressive
  match certificate cert_map
```

Group Name Assigned to a Peer That Is Associated with an ISAKMP Profile: Example

The following example shows that the group “some_group” is to be associated with a peer that has been assigned an ISAKMP profile:

```
crypto isakmp profile id_profile
  ca trust-point 2315
```

```
match identity host domain cisco.com
client configuration group some_group
```

Mapping a Certificate to an ISAKMP Profile Verification: Example

The following examples show that a certificate has been mapped to an ISAKMP profile. The examples include the configurations for the responder and initiator, **show command** output verifying that the subject name of the certificate map has been configured, and **debug** command output showing that the certificate has gone through certificate map matching and been matched to the ISAKMP profile.

Responder Configuration

```
crypto pki certificate map cert_map 10
! The above line is the certificate map definition.
subject-name co ou = green
! The above line shows that the subject name must have "ou = green."
!
crypto isakmp profile certpro
! The above line shows that this is the ISAKMP profile that will match if the certificate
of the peer matches cert_map (shown on third line below).
ca trust-point 2315
ca trust-point LaBcA
match certificate cert_map
initiate mode aggressive
```

Initiator Configuration

```
crypto ca trustpoint LaBcA
enrollment url http://10.76.82.20:80/cgi-bin/openscep
subject-name ou=green,c=IN
! The above line ensures that the subject name "ou = green" is set.
revocation-check none
```

show crypto ca certificates Command Output for the Initiator

```
Router# show crypto ca certificates
```

```
Certificate
Status: Available
Certificate Serial Number: 21
Certificate Usage: General Purpose
Issuer:
  cn=blue-lab CA
  o=CISCO
  c=IN
Subject:
  Name: Router1.cisco.com
  c=IN
  ou=green
! The above line is a double check that "ou = green" has been set as the subject name.
  hostname=Router1.cisco.com
Validity Date:
  start date: 14:34:30 UTC Mar 31 2004
  end date: 14:34:30 UTC Apr 1 2009
  renew date: 00:00:00 UTC Jan 1 1970
Associated Trustpoints: LaBcA
```

debug crypto isakmp Command Output for the Responder

```
Router# debug crypto isakmp
```

```

6d23h: ISAKMP (0:268435460): received packet from 192.0.0.2 dport 500 sport 500 Global (R)
MM_KEY_EXCH
6d23h: ISAKMP: Main Mode packet contents (flags 1, len 892):
6d23h:      ID payload
6d23h:      FQDN <Router1.cisco.com> port 500 protocol 17
6d23h:      CERT payload
6d23h:      SIG payload
6d23h:      KEEPALIVE payload
6d23h:      NOTIFY payload
6d23h: ISAKMP:(0:4:HW:2):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
6d23h: ISAKMP:(0:4:HW:2):Old State = IKE_R_MM4 New State = IKE_R_MM5

6d23h: ISAKMP:(0:4:HW:2): processing ID payload. message ID = 0
6d23h: ISAKMP (0:268435460): ID payload
      next-payload : 6
      type          : 2
      FQDN name     : Router1.cisco.com
      protocol      : 17
      port          : 500
      length        : 28
6d23h: ISAKMP:(0:4:HW:2):: peer matches *none* of the profiles
6d23h: ISAKMP:(0:4:HW:2): processing CERT payload. message ID = 0
6d23h: ISAKMP:(0:4:HW:2): processing a CT_X509_SIGNATURE cert
6d23h: ISAKMP:(0:4:HW:2): peer's pubkey isn't cached
6d23h: ISAKMP:(0:4:HW:2): OU = green
6d23h: ISAKMP:(0:4:HW:2): certificate map matches certpro profile
! The above line shows that the certificate has gone through certificate map matching and
that it matches the "certpro" profile.
6d23h: ISAKMP:(0:4:HW:2): Trying to re-validate CERT using new profile
6d23h: ISAKMP:(0:4:HW:2): Creating CERT validation list: 2315, LaBcA,
6d23h: ISAKMP:(0:4:HW:2): CERT validity confirmed.

```

Group Name Assigned to a Peer Verification: Example

The following configuration and debug output show that a group has been assigned to a peer.

Initiator Configuration

```

crypto isakmp profile certpro
  ca trust-point 2315
  ca trust-point LaBcA
  match certificate cert_map
  client configuration group new_group
! The statement on the above line will assign the group "new_group" to any peer that
matches the ISAKMP profile "certpro."
  initiate mode aggressive
!

```

debug crypto isakmp profile Command Output for the Responder

The following debug output example shows that the peer has been matched to the ISAKMP profile named "certpro" and that it has been assigned a group named "new_group."

```

Router# debug crypto isakmp profile
6d23h: ISAKMP (0:268435461): received packet from 192.0.0.2 dport 500 sport 500 Global (R)
MM_KEY_EXCH
6d23h: ISAKMP: Main Mode packet contents (flags 1, len 892):
6d23h:      ID payload
6d23h:      FQDN <Router1.cisco.com> port 500 protocol 17
6d23h:      CERT payload
6d23h:      SIG payload
6d23h:      KEEPALIVE payload

```

```

6d23h:          NOTIFY payload
6d23h: ISAKMP:(0:5:HW:2):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
6d23h: ISAKMP:(0:5:HW:2):Old State = IKE_R_MM4 New State = IKE_R_MM5

6d23h: ISAKMP:(0:5:HW:2): processing ID payload. message ID = 0
6d23h: ISAKMP (0:268435461): ID payload
      next-payload : 6
      type          : 2
      FQDN name     : Router1.cisco.com
      protocol      : 17
      port          : 500
      length        : 28
6d23h: ISAKMP:(0:5:HW:2):: peer matches *none* of the profiles
6d23h: ISAKMP:(0:5:HW:2): processing CERT payload. message ID = 0
6d23h: ISAKMP:(0:5:HW:2): processing a CT_X509_SIGNATURE cert
6d23h: ISAKMP:(0:5:HW:2): peer's pubkey isn't cached
6d23h: ISAKMP:(0:5:HW:2): OU = green
6d23h: ISAKMP:(0:5:HW:2): certificate map matches certpro profile
6d23h: ISAKMP:(0:5:HW:2): Trying to re-validate CERT using new profile
6d23h: ISAKMP:(0:5:HW:2): Creating CERT validation list: 2315, LaBcA,
6d23h: ISAKMP:(0:5:HW:2): CERT validity confirmed.
6d23h: ISAKMP:(0:5:HW:2):Profile has no keyring, aborting key search
6d23h: ISAKMP:(0:5:HW:2): Profile certpro assigned peer the group named new_group

```

Additional References

The following sections provide references related to Certificate to ISAKMP Profile Mapping.

Related Documents

Related Topic	Document Title
Configuring certificate maps	<i>Certificate Security Attribute-Based Access Control</i> , Release 12.2 T
Configuring ISAKMP profiles	<i>VRF-Aware IPSec</i> , Release 12.2 T
Security commands	<i>Cisco IOS Security Command Reference</i> , Release 12.4 T

Standards

Standards	Title
There are no new or modified standards associated with this feature.	—

MIBs

MIBs	MIBs Link
There are no new or modified MIBs associated with this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
There are no new or modified RFCs associated with this feature.	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **client configuration group**
- **match certificate (ISAKMP)**



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Encrypted Preshared Key

The Encrypted Preshared Key feature allows you to securely store plain text passwords in type 6 (encrypted) format in NVRAM.

Feature History for Encrypted Preshared Key

Release	Modification
12.3(2)T	This feature was introduced.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions for Encrypted Preshared Key, page 2](#)
- [Information About Encrypted Preshared Key, page 2](#)
- [How to Configure an Encrypted Preshared Key, page 3](#)
- [Configuration Examples for Encrypted Preshared Key, page 11](#)
- [Where to Go Next, page 13](#)
- [Additional References, page 14](#)
- [Command Reference, page 14](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Restrictions for Encrypted Preshared Key

- Old ROM monitors (ROMMONs) and boot images cannot recognize the new type 6 passwords. Therefore, errors are expected if you boot from an old ROMMON.
- For Cisco 836 routers, please note that support for Advanced Encryption Standard (AES) is available only on IP plus images.

Information About Encrypted Preshared Key

Before Using the Encrypted Preshared Key feature, you should understand the following concepts:

- [Using the Encrypted Preshared Key Feature to Securely Store Passwords, page 2](#)
- [How to Configure an Encrypted Preshared Key, page 3](#)

Using the Encrypted Preshared Key Feature to Securely Store Passwords

Using the Encrypted Preshared Key feature, you can securely store plain text passwords in type 6 format in NVRAM using a command-line interface (CLI). Type 6 passwords are encrypted. Although the encrypted passwords can be seen or retrieved, it is difficult to decrypt them to find out the actual password. Use the **key config-key password-encryption** command with the **password encryption aes** command to configure and enable the password (symmetric cipher AES is used to encrypt the keys). The password (key) configured using the **config-key password-encryption** command is the master encryption key that is used to encrypt all other keys in the router.

If you configure the **password encryption aes** command without configuring the **key config-key password-encryption** command, the following message is printed at startup or during any nonvolatile generation (NVGEN) process, such as when the **show running-config** or **copy running-config startup-config** commands have been configured:

```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```

Changing a Password

If the password (master key) is changed, or reencrypted, using the **key config-key password-encryption** command, the list registry passes the old key and the new key to the application modules that are using type 6 encryption.

Deleting a Password

If the master key that was configured using the **key config-key password-encryption** command is deleted from the system, a warning is printed (and a confirm prompt is issued) that states that all type 6 passwords will become useless. As a security measure, after the passwords have been encrypted, they will never be decrypted in the Cisco IOS software. However, passwords can be reencrypted as explained in the previous paragraph.



Caution

If the password configured using the **key config-key password-encryption** command is lost, it cannot be recovered. The password should be stored in a safe location.

Unconfiguring Password Encryption

If you later unconfigure password encryption using the **no password encryption aes** command, all existing type 6 passwords are left unchanged, and as long as the password (master key) that was configured using the **key config-key password-encryption** command exists, the type 6 passwords will be decrypted as and when required by the application.

Storing Passwords

Because no one can “read” the password (configured using the **key config-key password-encryption** command), there is no way that the password can be retrieved from the router. Existing management stations cannot “know” what it is unless the stations are enhanced to include this key somewhere, in which case the password needs to be stored securely within the management system. If configurations are stored using TFTP, the configurations are not standalone, meaning that they cannot be loaded onto a router. Before or after the configurations are loaded onto a router, the password must be manually added (using the **key config-key password-encryption** command). The password can be manually added to the stored configuration but is not recommended because adding the password manually allows anyone to decrypt all passwords in that configuration.

Configuring New or Unknown Passwords

If you enter or cut and paste cipher text that does not match the master key, or if there is no master key, the cipher text is accepted or saved, but an alert message is printed. The alert message is as follows:

```
"ciphertext>[for username bar>] is incompatible with the configured master key."
```

If a new master key is configured, all the plain keys are encrypted and made type 6 keys. The existing type 6 keys are not encrypted. The existing type 6 keys are left as is.

If the old master key is lost or unknown, you have the option of deleting the master key using the **no key config-key password-encryption** command. Deleting the master key using the **no key config-key password-encryption** command causes the existing encrypted passwords to remain encrypted in the router configuration. The passwords will not be decrypted.

Enabling the Encrypted Preshared Key

The **password encryption aes** command is used to enable the encrypted password.

How to Configure an Encrypted Preshared Key

This section contains the following procedures:

- [Configuring an Encrypted Preshared Key, page 4](#) (required)
- [Monitoring Encrypted Preshared Keys, page 5](#) (optional)
- [Configuring an ISAKMP Preshared Key, page 6](#) (optional)
- [Configuring an ISAKMP Preshared Key in ISAKMP Keyrings, page 7](#) (optional)
- [Configuring ISAKMP Aggressive Mode, page 8](#) (optional)
- [Configuring a Unity Server Group Policy, page 9](#) (optional)

- [Configuring an Easy VPN Client, page 10](#) (optional)

Configuring an Encrypted Preshared Key

To configure an encrypted preshared key, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key config-key password-encryption** *[text]*
4. **password encryption aes**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	key config-key password-encryption <i>[text]</i> Example: Router (config)# key config-key password-encryption	Stores a type 6 encryption key in private NVRAM. <ul style="list-style-type: none"> • If you want to key in interactively (using the enter key) and an encrypted key already exists, you will be prompted for the following: Old key, New key, and Confirm key. • If you want to key in interactively but an encryption key is not present, you will be prompted for the following: New key and Confirm key. • If you want to remove the password that is already encrypted, you will see the following prompt: “WARNING: All type 6 encrypted keys will become unusable. Continue with master key deletion? [yes/no]:”.
Step 4	password encryption aes Example: Router (config)# password-encryption aes	Enables the encrypted preshared key.

Troubleshooting Tips

If you see the warning message “ciphertext >[for username bar] is incompatible with the configured master key,” you have entered or cut and pasted cipher text that does not match the master key or there is no master key. (The cipher text will be accepted or saved.) The warning message will allow you to locate the broken configuration line or lines.

Monitoring Encrypted Preshared Keys

To get logging output for encrypted preshared keys, perform the following steps.

1. **enable**
2. **password logging**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	password logging Example: Router# password logging	Provides a log of debugging output for a type 6 password operation.

Examples

The following **password logging** debug output shows that a new master key has been configured and that the keys have been encrypted with the new master key:

```
Router (config)# key config-key password-encrypt
New key:
Confirm key:
Router (config)#
01:40:57: TYPE6_PASS: New Master key configured, encrypting the keys with
the new master keypas

Router (config)# key config-key password-encrypt
Old key:
New key:
Confirm key:
Router (config)#
01:42:11: TYPE6_PASS: Master key change heralded, re-encrypting the keys
with the new master key
01:42:11: TYPE6_PASS: Mac verification successful
01:42:11: TYPE6_PASS: Mac verification successful
01:42:11: TYPE6_PASS: Mac verification successful
```

What To Do Next

You can perform any of the following procedures. Each procedure is independent of the others.

- [Configuring an ISAKMP Preshared Key, page 6](#)
- [Configuring an ISAKMP Preshared Key in ISAKMP Keyrings, page 7](#)
- [Configuring ISAKMP Aggressive Mode, page 8](#)
- [Configuring a Unity Server Group Policy, page 9](#)
- [Configuring an Easy VPN Client, page 10](#)

Configuring an ISAKMP Preshared Key

To configure an ISAKMP preshared key, perform the following procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp key *keystring* address *peer-address***
4. **crypto isakmp key *keystring* hostname *hostname***

DETAILED STEPS

	Command	Description
Step 1	enable Example: Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto isakmp key <i>keystring</i> address <i>peer-address</i> Example: Router (config)# crypto isakmp key cisco address 10.2.3.4	Configures a preshared authentication key. <ul style="list-style-type: none">• The <i>peer-address</i> argument specifies the IP address of the remote peer.
Step 4	crypto isakmp key <i>keystring</i> hostname <i>hostname</i> Example: Router (config)# crypto isakmp key foo hostname foo.com	Configures a preshared authentication key. <ul style="list-style-type: none">• The <i>hostname</i> argument specifies the fully qualified domain name (FQDN) of the peer.

Example

The following sample output shows that an encrypted preshared key has been configured:

```
crypto isakmp key 6 _Hg[^^ECgLGgPF^RXTQfDDWQ][YAAB address 10.2.3.4
crypto isakmp key 6 `eR\eTRaKCUZPYYQfDgXRWi_AAB hostname foo.com
```

Configuring an ISAKMP Preshared Key in ISAKMP Keyrings

To configure an ISAKMP preshared key in ISAKMP keyrings, which are used in IPSec Virtual Route Forwarding (VRF) configurations, perform the following procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto keyring** *keyring-name*
4. **pre-shared-key address** *address* **key** *key*
5. **pre-shared-key hostname** *hostname* **key** *key*

DETAILED STEPS

	Command	Description
Step 1	enable Example: Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto keyring <i>keyring-name</i> Example: Router (config)# crypto keyring foo	Defines a crypto keyring to be used during Internet Key Exchange (IKE) authentication and enters keyring configuration mode.
Step 4	pre-shared-key address <i>address</i> key <i>key</i> Example: Router (config-keyring)# pre-shared-key address 10.2.3.5 key cisco	Defines a preshared key to be used for IKE authentication. <ul style="list-style-type: none">• The <i>address</i> argument specifies the IP address of the remote peer.
Step 5	pre-shared-key hostname <i>hostname</i> key <i>key</i> Example: Router (config-keyring)# pre-shared-key hostname foo.com key cisco	Defines a preshared key to be used for IKE authentication. <ul style="list-style-type: none">• The <i>hostname</i> argument specifies the FQDN of the peer.

Example

The following **show-running-config** sample output shows that an encrypted preshared key in ISAKMP keyrings has been configured.

```
crypto keyring foo
  pre-shared-key address 10.2.3.5 key 6 `WHCJYR_Z]GRPF^RXTQfDcfZ]GPAAB
  pre-shared-key hostname foo.com key 6 aE_REHDcOfYCPF^RXTQfDJYVVNSAAB
```

Configuring ISAKMP Aggressive Mode

To configure ISAKMP aggressive mode, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp peer ip-address** *ip-address*
4. **set aggressive-mode client-endpoint** *client-endpoint*
5. **set aggressive-mode password** *password*

DETAILED STEPS

	Command	Description
Step 1	enable Example: Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto isakmp peer ip-address <i>ip-address</i> Example: Router (config)# crypto isakmp peer ip-address 10.2.3.4	To enable an IP Security (IPSec) peer for IKE querying of authentication, authorization, and accounting (AAA) for tunnel attributes in aggressive mode and to enter ISAKMP peer configuration mode.
Step 4	set aggressive-mode client-endpoint <i>client-endpoint</i> Example: Router (config-isakmp-peer)# set aggressive-mode client-endpoint fqdn cisco.com	Specifies the Tunnel-Client-Endpoint attribute within an ISAKMP peer configuration.
Step 5	set aggressive-mode password <i>password</i> Example: Router (config-isakmp-peer)# set aggressive-mode password cisco	Specifies the Tunnel-Password attribute within an ISAKMP peer configuration.

Example

The following **show-running-config** sample output shows that an encrypted preshared key in ISAKMP aggressive mode has been configured.

```
crypto isakmp peer address 10.2.3.4
  set aggressive-mode password 6 ^aKPIQ_KJE_PPF^RXTQfDTIaLNeAAB
  set aggressive-mode client-endpoint fqdn cisco.com
```

Configuring a Unity Server Group Policy

To configure a unity server group policy, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** *group-name*
4. **pool** *name*
5. **domain** *name*
6. **key** *name*

DETAILED STEPS

	Command	Description
Step 1	enable Example: Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto isakmp client configuration group <i>group-name</i> Example: Router (config)# crypto isakmp client configuration group foo	Specifies the policy profile of the group that will be defined and enters ISAKMP group configuration mode.
Step 4	pool <i>name</i> Example: Router (config-isakmp-group)# pool foopool	Defines a local pool address.

	Command	Description
Step 5	domain name Example: Router (config-isakmp-group)# domain cisco.com	Specifies the Domain Name Service (DNS) domain to which a group belongs.
Step 6	key name Example: Router (config-isakmp-group)# key cisco	Specifies the IKE preshared key for group policy attribute definition.

Example

The following **show-running-config** sample output shows that an encrypted key has been configured for a unity server group policy:

```
crypto isakmp client configuration group foo
key 6 cZZgDZPOE\ddPF^RXTQfDTIaLNeAAB
domain cisco.com
pool foopool
```

Configuring an Easy VPN Client

To configure an Easy VPN client, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec client ezvpn name**
4. **peer ipaddress**
5. **mode client**
6. **group group-name key group-key**
7. **connect manual**

DETAILED STEPS

	Command	Description
Step 1	enable Example: Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command	Description
Step 3	crypto ipsec client ezvpn <i>name</i> Example: Router (config)# crypto ipsec client ezvpn foo	Creates a Cisco Easy VPN remote configuration and enters Cisco Easy VPN remote configuration mode.
Step 4	peer <i>ipaddress</i> Example: Router (config-isakmp-peer)# peer 10.2.3.4	Sets the peer IP address for the VPN connection.
Step 5	mode client Example: Router (config-isakmp-ezvpn)# mode client	Automatically configures the router for Cisco Easy VPNclient mode operation, which uses Network Address Translation (NAT) or Peer Address Translation (PAT) address translations.
Step 6	group <i>group-name</i> key <i>group-key</i> Example: Router (config-isakmp-ezvpn)# group foo key cisco	Specifies the group name and key value for the VPN connection.
Step 7	connect manual Example: Router (config-isakmp-ezvpn)# connect manual	Specifies the manual setting for directing the Cisco Easy VPN remote client to wait for a command or application program interface (API) call before attempting to establish the Cisco Easy VPN remote connection.

Example

The following **show-running-config** sample output shows that an Easy VPN client has been configured. The key has been encrypted.

```
crypto ipsec client ezvpn foo
connect manual
group foo key 6 gdMI`S^[GicPF^RXTQfDFKEO\RAAB
mode client
peer 10.2.3.4
```

Configuration Examples for Encrypted Preshared Key

This section provides the following configuration examples:

- [Encrypted Preshared Key: Example, page 12](#)
- [No Previous Key Present: Example, page 12](#)
- [Key Already Exists: Example, page 12](#)
- [Key Already Exists But the User Wants to Key In Interactively: Example, page 12](#)
- [No Key Present But the User Wants to Key In Interactively: Example, page 12](#)
- [Removal of the Password Encryption: Example, page 13](#)

Encrypted Preshared Key: Example

The following is an example of a configuration for which a type 6 preshared key has been encrypted. It includes the prompts and messages that a user might see.

```
Router (config)# crypto isakmp key cisco address 10.0.0.2
Router (config)# exit
Router# show running-config | include crypto isakmp key
crypto isakmp key cisco address 10.0.0.2
Router#
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router (config)# password encryption aes
Router (config)# key config-key password-encrypt
New key:
Confirm key:
Router (config)#
01:46:40: TYPE6_PASS: New Master key configured, encrypting the keys with
the new master key
Router (config)# exit
Router # show running-config | include crypto isakmp key
crypto isakmp key 6 CXWdhVTZYB_Vcd^`cIHDOahiFTa address 10.0.0.2
```

No Previous Key Present: Example

In the following configuration example, no previous key is present:

```
Router (config)# key config-key password-encryption testkey 123
```

Key Already Exists: Example

In the following configuration example, a key already exists:

```
Router (config)# key config-key password-encryption testkey123
Old key:
Router (config)#
```

Key Already Exists But the User Wants to Key In Interactively: Example

In the following configuration example, the user wants to key in interactively, but a key already exists. The Old key, New key, and Confirm key prompts will show on your screen if you enter the **key config-key password-encryption** command and press the enter key to get into interactive mode.

```
Router (config)# key config-key password-encryption
Old key:
New key:
Confirm key:
```

No Key Present But the User Wants to Key In Interactively: Example

In the following example, the user wants to key in interactively, but no key is present. The New key and Confirm key prompts will show on your screen if you are in interactive mode.

```
Router (config)# key config-key password-encryption
New key:
```

Confirm key:

Removal of the Password Encryption: Example

In the following configuration example, the user wants to remove the encrypted password. The “WARNING: All type 6 encrypted keys will become unusable. Continue with master key deletion? [yes/no]:” prompt will show on your screen if you are in interactive mode.

```
Router (config)# no key config-key password-encryption
```

```
WARNING: All type 6 encrypted keys will become unusable. Continue with master key  
deletion ? [yes/no]: y
```

Where to Go Next

Configure any other preshared keys.

Additional References

The following sections provide references related to Encrypted Preshared Key.

Related Documents

Related Topic	Document Title
Configuring passwords	<i>The section “Part 4: IP Security and Encryption” of the <i>Cisco IOS Security Configuration Guide</i> <i>Cisco IOS Security Command Reference</i>, Release 12.3 T</i>

Standards

Standards	Title
This feature has no new or modified standards.	—

MIBs

MIBs	MIBs Link
This feature has no new or modified MIBs.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
This feature has no new or modified RFCs.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **crypto ipsec client ezvpn (global)**
- **crypto isakmp client configuration group**
- **crypto isakmp key**
- **key config-key password-encryption**
- **password encryption aes**
- **password logging**
- **pre-shared-key**
- **set aggressive-mode password**



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Security for VPNs with IPSec



Configuring Security for VPNs with IPSec

This module describes how to configure basic IP Security (IPSec) virtual private networks (VPNs). IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF). It provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices (“peers”), such as Cisco routers.

Module History

This module was first published on May 2, 2005, and last updated on May 2, 2005.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all features. To find information about feature support and configuration, use the [“Feature Information for Security for VPNs with IPSec” section on page 35](#).

Contents

- [Prerequisites for Configuring Security for VPNs with IPSec, page 2](#)
- [Restrictions for Configuring Security for VPNs with IPSec, page 2](#)
- [Information About Configuring Security for VPNs with IPSec, page 2](#)
- [How to Configure IPSec VPNs, page 8](#)
- [Configuration Examples for Configuring an IPSec VPN, page 32](#)
- [Additional References, page 33](#)
- [Glossary, page 34](#)
- [Feature Information for Security for VPNs with IPSec, page 35](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for Configuring Security for VPNs with IPSec

IKE Configuration

You must configure Internet Key Exchange (IKE) as described in the module “Configuring Internet Key Exchange Security for IPSec VPNs.”

Even if you decide to not use IKE, you still must disable it as described in the module “Configuring Internet Key Exchange for IPSec VPNs.”

Ensure Access Lists Are Compatible with IPSec

IKE uses UDP port 500. The IPSec Encapsulating Security Payload (ESP) and Authentication Header (AH) protocols use protocol numbers 50 and 51. Ensure that your access lists are configured so that protocol 50, 51, and User Datagram Protocol (UDP) port 500 traffic is not blocked at interfaces used by IPSec. In some cases you might need to add a statement to your access lists to explicitly permit this traffic.

Restrictions for Configuring Security for VPNs with IPSec

Unicast IP Datagram Application Only

At this time, IPSec can be applied to unicast IP datagrams only. Because the IPSec Working Group has not yet addressed the issue of group key distribution, IPSec does not currently work with multicasts or broadcast IP datagrams.

NAT Configuration

If you use Network Address Translation (NAT), you should configure static NAT translations so that IPSec works properly. In general, NAT translation should occur before the router performs IPSec encapsulation; in other words, IPSec should be working with global addresses.

Information About Configuring Security for VPNs with IPSec

To configure basic IPSec VPNs, you should understand the following concepts:

- [Supported Standards, page 2](#)
- [Supported Hardware, Switching Paths, and Encapsulation, page 4](#)
- [IPSec Functionality Overview, page 6](#)
- [IPSec Traffic Nested to Multiple Peers, page 8](#)

Supported Standards

Cisco implements the following standards with this feature:

- IPSec—IP Security Protocol. IPSec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer; it uses IKE to handle negotiation of protocols and algorithms

based on local policy, and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.



Note The term IPSec is sometimes used to describe the entire protocol of IPSec data services and IKE security protocols and is also sometimes used to describe only the data services.

IPSec is documented in a series of Internet Drafts, all available at <http://www.ietf.org/html.charters/ipsec-charter.html>.

- IKE—A hybrid protocol that implements Oakley and SKEME key exchanges inside the ISAKMP framework. While IKE can be used with other protocols, its initial implementation is with the IPSec protocol. IKE provides authentication of the IPSec peers, negotiates IPSec security associations, and establishes IPSec keys.

The component technologies implemented for IPSec include:

- AES—Advanced Encryption Standard. A cryptographic algorithm that protects sensitive, unclassified information. AES is privacy transform for IPSec and IKE and has been developed to replace the DES. AES is designed to be more secure than DES: AES offers a larger key size, while ensuring that the only known approach to decrypt a message is for an intruder to try every possible key. AES has a variable key length—the algorithm can specify a 128-bit key (the default), a 192-bit key, or a 256-bit key.
- DES—Data Encryption Standard. An algorithm that is used to encrypt packet data. Cisco IOS implements the mandatory 56-bit DES-CBC with Explicit IV. Cipher Block Chaining (CBC) requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPSec packet. For backwards compatibility, Cisco IOS IPSec also implements the RFC 1829 version of ESP DES-CBC.

Cisco IOS also implements Triple DES (168-bit) encryption, depending on the software versions available for a specific platform. Triple DES (3DES) is a strong form of encryption that allows sensitive information to be transmitted over untrusted networks. It enables customers to utilize network layer encryption.



Note Cisco IOS images with strong encryption (including, but not limited to, 56-bit data encryption feature sets) are subject to United States government export controls, and have a limited distribution. Images to be installed outside the United States require an export license. Customer orders might be denied or subject to delay due to United States government regulations. Contact your sales representative or distributor for more information, or send e-mail to export@cisco.com.

- SEAL—Software Encryption Algorithm. An alternative algorithm to software-based DES, 3DES, and AES. SEAL encryption uses a 160-bit encryption key and has a lower impact to the CPU when compared to other software-based algorithms.
- MD5 (HMAC variant)—MD5 (Message Digest 5) is a hash algorithm. HMAC is a keyed hash variant used to authenticate data.
- SHA (HMAC variant)—SHA (Secure Hash Algorithm) is a hash algorithm. HMAC is a keyed hash variant used to authenticate data.

IPSec as implemented in Cisco IOS software supports the following additional standards:

- AH—Authentication Header. A security protocol which provides data authentication and optional anti-replay services. AH is embedded in the data to be protected (a full IP datagram).

- ESP—Encapsulating Security Payload. A security protocol which provides data privacy services and optional data authentication, and anti-replay services. ESP encapsulates the data to be protected.

Supported Hardware, Switching Paths, and Encapsulation

IPSec has certain requirements for hardware, switching paths, and encapsulation methods as follows:

- [Supported Hardware](#)
- [Supported Switching Paths](#)
- [Supported Encapsulation](#)

Supported Hardware

This section contains the following subsections:

- [VPN Accelerator Module \(VAM\) Support](#)
- [AIMs and NM Support](#)

VPN Accelerator Module (VAM) Support

The VAM is a single-width acceleration module. It provides high-performance, hardware-assisted tunneling and encryption services suitable for VPN remote access, site-to-site intranet, and extranet applications. It also provides platform scalability and security while working with all services necessary for successful VPN deployments—security, quality of service (QoS), firewall and intrusion detection, service-level validation, and management. The VAM off-loads IPSec processing from the main processor, thus freeing resources on the processor engines for other tasks.

The VAM provides hardware-accelerated support for the following multiple encryption functions:

- 56-bit DES standard mode: CBC
- 3-Key Triple DES (168-bit)
- SHA-1 and MD5
- Rivest, Shamir, Adelman (RSA) public-key algorithm
- Diffie-Hellman key exchange RC4-40

For more information on VAMs, see the document “VPN Acceleration Module (VAM).”

AIMs and NM Support

The data encryption Advanced Integration Module (AIM) and Network Module (NM) provide hardware-based encryption.

The data encryption AIMs and NM are hardware Layer 3 (IPSec) encryption modules and provide DES and Triple DES IPSec encryption for multiple T1s or E1s of bandwidth. These products also have hardware support for Diffie-Hellman, RSA, and DSA key generation.

Before using either module, note that RSA manual keying is not supported.

See [Table 44](#) to determine which VPN encryption module to use.

IPPCP Software for Use with AIMS and NMs in Cisco 2600 and Cisco 3600 Series Routers

Software IPPCP with AIMS and NMs allow customers to use Lempel-Ziv-Stac (LZS) software compression with IPSec when a VPN module is in Cisco 2600 and Cisco 3600 series routers, allowing users to effectively increase the bandwidth on their interfaces.

Without IPPCP software, compression is not supported with the VPN encryption hardware AIM and NM; that is, a user had to remove the VPN module from the router and run software encryption with software compression. IPPCP enables all VPN modules to support LZS compression in software when the VPN module is in the router, thereby, allowing users to configure data compression and increase their bandwidth, which is useful for a low data link.

Without IPPCP, compression occurs at Layer 2, and encryption occurs at Layer 3. After a data stream is encrypted, it is passed on for compression services. When the compression engine receives the encrypted data streams, the data expands and does not compress. This feature enables both compression and encryption of the data to occur at Layer 3 by selecting LZS with the IPSec transform set; that is, LZS compression occurs before encryption, and it is able to get better compression ratio.

Table 44 AIM/VPN Encryption Module Support by Cisco IOS Release

	Encryption Module Support by Cisco IOS Release				
Platform	12.2(13)T	12.3(4)T	12.3(5)	12.3(6)	12.3(7)T
Cisco 831	Software-based AES				
Cisco 1710	Software-based AES				
Cisco 1711					
Cisco 1721					
Cisco 1751					
Cisco 1760					
Cisco 2600 XM	—			AIM-VPN/BPII-Plus Hardware Encryption Module	
Cisco 2611 XM	—	AIM-VPN/BPII Hardware Encryption Module			AIM-VPN/BPII-Plus Hardware Encryption Module
Cisco 2621 XM					
Cisco 2651 XM					
Cisco 2691 XM	AIM-VPN/EPII Hardware Encryption Module				AIM-VPN/EPII-Plus Hardware Encryption Module
Cisco 3735	AIM-VPN/EPII Hardware Encryption Module		AIM-VPN/EPII-Plus Hardware Encryption Module		
Cisco 3660	AIM-VPN/HPPII Hardware Encryption Module		AIM-VPN/HPPII-Plus Hardware Encryption Module		
Cisco 3745					

For more information on AIMS and NM, see [Installing Advanced Integration Modules in Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers](#).

Supported Switching Paths

Table 45 lists the supported switching paths that work with IPSec.

Table 45 **Supported Switching Paths for IPSec**

Switching Paths	Examples
Process switching	<pre>interface ethernet0/0 no ip route-cache</pre>
Fast switching	<pre>interface ethernet0/0 ip route-cache ! Ensure that you will not hit flow switching. no ip route-cache flow ! Disable CEF for the interface, which supercedes global CEF. no ip route-cache cef</pre>
Cisco Express Forwarding (CEF)	<pre>ip cef interface ethernet0/0 ip route-cache ! Ensure that you will not hit flow switching. no ip route-cache flow</pre>
Fast-flow switching	<pre>interface ethernet0/0 ip route-cache ! Enable flow switching p route-cache flow ! Disable CEF for the interface. no ip route-cache cef</pre>
CEF-flow switching	<pre>! Enable global CEF. ip cef interface ethernet0/0 ip route-cache ip route-cache flow ! Enable CEF for the interface ip route-cache cef</pre>

Supported Encapsulation

IPSec works with the following serial encapsulations: High-Level Data-Links Control (HDLC), PPP, and Frame Relay.

IPSec also works with the Generic Routing Encapsulation (GRE) and IPinIP Layer 3, Layer 2 Forwarding (L2F), Layer 2 Tunneling Protocol (L2TP), Data Link Switching+ (DLSw+), and SRB tunneling protocols; however, multipoint tunnels are not supported. Other Layer 3 tunneling protocols may not be supported for use with IPSec.

Because the IPSec Working Group has not yet addressed the issue of group key distribution, IPSec currently cannot be used to protect group traffic (such as broadcast or multicast traffic).

IPSec Functionality Overview

IPSec provides the following network security services. (In general, local security policy dictates the use of one or more of these services.)

- **Data Confidentiality**—The IPSec sender can encrypt packets before transmitting them across a network.
- **Data Integrity**—The IPSec receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.

- **Data Origin Authentication**—The IPSec receiver can authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity service.
- **Anti-Replay**—The IPSec receiver can detect and reject replayed packets.

IPSec provides secure *tunnels* between two peers, such as two routers. You define which packets are considered sensitive and should be sent through these secure tunnels, and you define the parameters that should be used to protect these sensitive packets, by specifying characteristics of these tunnels. Then, when the IPSec peer recognizes such a sensitive packet, the peer sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer. (The use of the term *tunnel* in this chapter does not refer to using IPSec in tunnel mode.)

More accurately, these *tunnels* are sets of security associations (SAs) that are established between two IPSec peers. The SAs define which protocols and algorithms should be applied to sensitive packets and specify the keying material to be used by the two peers. SAs are unidirectional and are established per security protocol (AH or ESP).

With IPSec you define what traffic should be protected between two IPSec peers by configuring access lists and applying these access lists to interfaces by way of crypto map sets. Therefore, traffic may be selected on the basis of source and destination address, and optionally Layer 4 protocol, and port. (The access lists used for IPSec are used only to determine which traffic should be protected by IPSec, not which traffic should be blocked or permitted through the interface. Separate access lists define blocking and permitting at the interface.)

A crypto map set can contain multiple entries, each with a different access list. The crypto map entries are searched in order—the router attempts to match the packet to the access list specified in that entry.

When a packet matches a **permit** entry in a particular access list, and the corresponding crypto map entry is tagged as **cisco**, connections are established if necessary. If the crypto map entry is tagged as **ipsec-isakmp**, IPSec is triggered. If no SA exists that IPSec can use to protect this traffic to the peer, IPSec uses IKE to negotiate with the remote peer to set up the necessary IPSec SAs on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry. (The behavior is different for dynamic crypto map entries. See the section “[Creating Dynamic Crypto Maps](#)” section later in this module.)

If the crypto map entry is tagged as **ipsec-manual**, IPSec is triggered. If no SA exists that IPSec can use to protect this traffic to the peer, the traffic is dropped. In this case, the SAs are installed via the configuration, without the intervention of IKE. If the SAs did not exist, IPSec did not have all of the necessary pieces configured.

Once established, the set of SAs (outbound, to the peer) is then applied to the triggering packet and to subsequent applicable packets as those packets exit the router. “Applicable” packets are packets that match the same access list criteria that the original packet matched. For example, all applicable packets could be encrypted before being forwarded to the remote peer. The corresponding inbound SAs are used when processing the incoming traffic from that peer.

Multiple IPSec tunnels can exist between two peers to secure different data streams, with each tunnel using a separate set of SAs. For example, some data streams might be authenticated only while other data streams must both be encrypted and authenticated.

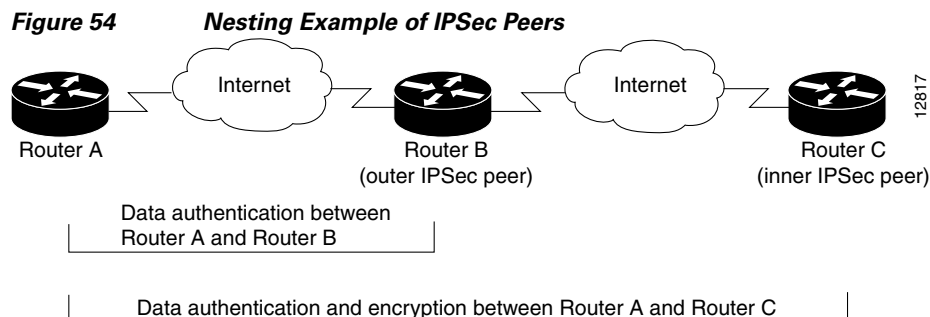
Access lists associated with IPSec crypto map entries also represent which traffic the router requires to be protected by IPSec. Inbound traffic is processed against the crypto map entries—if an unprotected packet matches a **permit** entry in a particular access list associated with an IPSec crypto map entry, that packet is dropped because it was not sent as an IPSec-protected packet.

Crypto map entries also include transform sets. A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPSec protected traffic. During the IPSec SA negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

IPSec Traffic Nested to Multiple Peers

You can nest IPSec traffic to a series of IPSec peers. For example, in order for traffic to traverse multiple firewalls (these firewalls have a policy of not letting through traffic that they have not authenticated), the router must establish IPSec tunnels with each firewall in turn. The “nearer” firewall becomes the “outer” IPSec peer.

In the example shown in [Figure 54](#), Router A encapsulates the traffic destined for Router C in IPSec (Router C is the inner IPSec peer). However, before Router A can send this traffic, it must first reencapsulate this traffic in IPSec in order to send it to Router B (Router B is the “outer” IPSec peer).



It is possible for the traffic between the “outer” peers to have one kind of protection (such as data authentication) and for traffic between the “inner” peers to have different protection (such as both data authentication and encryption).

How to Configure IPSec VPNs

Perform the tasks in the following sections to create IPSec VPNs:

- [Creating Crypto Access Lists, page 8](#)
- [Defining Transform Sets: A Combination of Security Protocols and Algorithms, page 14](#)
- [Creating Crypto Map Sets, page 17](#)
- [Applying Crypto Map Sets to Interfaces, page 30](#)

Creating Crypto Access Lists

To create crypto access lists that define which traffic is protected via IPSec tunnels, you should understand the following concepts:

- [Crypto Access List Overview](#)
- [When to Use the permit and deny Keywords in Crypto Access Lists](#)
- [Mirror Image Crypto Access Lists at Each IPSec Peer](#)
- [When to Use the any Keyword in Crypto Access Lists](#)

Crypto Access List Overview

Crypto access lists are used to define which IP traffic is protected by crypto and which traffic is not protected by crypto. (These access lists are *not* the same as regular access lists, which determine what traffic to forward or block at an interface.) For example, access lists can be created to protect all IP traffic between Subnet A and Subnet Y or Telnet traffic between Host A and Host B.

The access lists themselves are not specific to IPSec. It is the crypto map entry referencing the specific access list that defines whether IPSec processing is applied to the traffic matching a **permit** in the access list.

Crypto access lists associated with IPSec crypto map entries have four primary functions:

- Select outbound traffic to be protected by IPSec (permit = protect).
- Indicate the data flow to be protected by the new SAs (specified by a single **permit** entry) when initiating negotiations for IPSec security associations.
- Process inbound traffic in order to filter out and discard traffic that should have been protected by IPSec.
- Determine whether or not to accept requests for IPSec security associations on behalf of the requested data flows when processing IKE negotiation from the IPSec peer.
- Negotiation is performed only for **ipsec-isakmp** crypto map entries. In order to be accepted, if the peer initiates the IPSec negotiation, it must specify a data flow that is “permitted” by a crypto access list associated with an **ipsec-isakmp** crypto map entry.

If you want certain traffic to receive one combination of IPSec protection (for example, authentication only) and other traffic to receive a different combination of IPSec protection (for example, both authentication and encryption), you need to create two different crypto access lists to define the two different types of traffic. These different access lists are then used in different crypto map entries which specify different IPSec policies.

When to Use the permit and deny Keywords in Crypto Access Lists

Crypto protection can be permitted or denied for certain IP traffic in a crypto access list as follows:

- To protect IP traffic that matches the specified policy conditions in its corresponding crypto map entry, use the **permit** keyword in an access list.
- To refuse protection for IP traffic that matches the specified policy conditions in its corresponding crypto map entry, use the **deny** keyword in an access list.



Note

IP traffic is not protected by crypto if it is refused protection in all of the crypto map entries for an interface.

After the corresponding crypto map entry is defined and the crypto map set is applied to the interface, the defined crypto access list is applied to an interface. Different access lists must be used in different entries of the same crypto map set. However, both inbound and outbound traffic is evaluated against the same “outbound” IPSec access list. Therefore, the access list’s criteria is applied in the forward direction to traffic exiting your router and in the reverse direction to traffic entering your router.

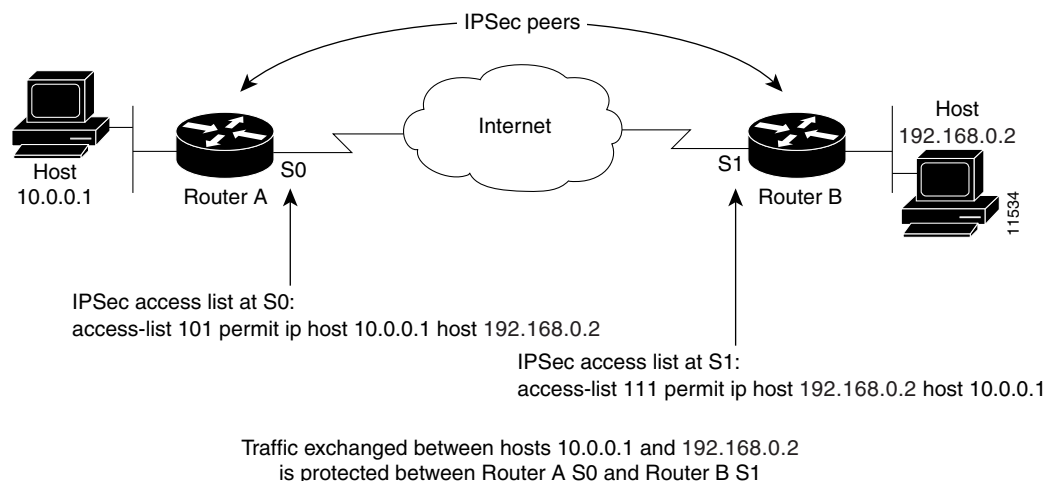
In [Figure 55](#), IPSec protection is applied to traffic between Host 10.0.0.1 and Host 192.168.0.2 as the data exits Router A’s S0 interface en route to Host 192.168.0.2. For traffic from Host 10.0.0.1 to Host 192.168.0.2, the access list entry on Router A is evaluated as follows:

```
source = host 10.0.0.1
dest = host 192.168.0.2
```

For traffic from Host 192.168.0.2 to Host 10.0.0.1, that same access list entry on Router A is evaluated as follows:

```
source = host 192.168.0.2
dest = host 10.0.0.1
```

Figure 55 How Crypto Access Lists Are Applied for Processing IPSec



If you configure multiple statements for a given crypto access list that is used for IPSec, in general the first **permit** statement that is matched is the statement used to determine the scope of the IPSec SA. That is, the IPSec SA is set up to protect traffic that meets the criteria of the matched statement only. Later, if traffic matches a different **permit** statement of the crypto access list, a new, separate IPSec SA is negotiated to protect traffic matching the newly matched access list statement.

Any unprotected inbound traffic that matches a **permit** entry in the crypto access list for a crypto map entry flagged as IPSec is dropped, because this traffic was expected to be protected by IPSec.



Note

If you view your router's access lists by using a command such as **show ip access-lists**, *all* extended IP access lists are shown in the command output. This display output includes extended IP access lists that are used for traffic filtering purposes and those that are used for crypto. The **show** command output does not differentiate between the different uses of the extended access lists.

The following example shows that if overlapping networks are used, then the most specific networks are defined in crypto sequence numbers before less specific networks are defined. In this example, the more specific network is covered by the crypto map sequence number 10, followed by the less specific network in the crypto map, which is sequence number 20.

```
crypto map mymap 10 ipsec-isakmp
  set peer 192.168.1.1
  set transform-set test
  match address 101
crypto map mymap 20 ipsec-isakmp
  set peer 192.168.1.2
  set transform-set test
  match address 102
```

```
access-list 101 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255  
access-list 102 permit ip 10.0.0.0 0.255.255.255 172.16.0.0 0.15.255.255
```

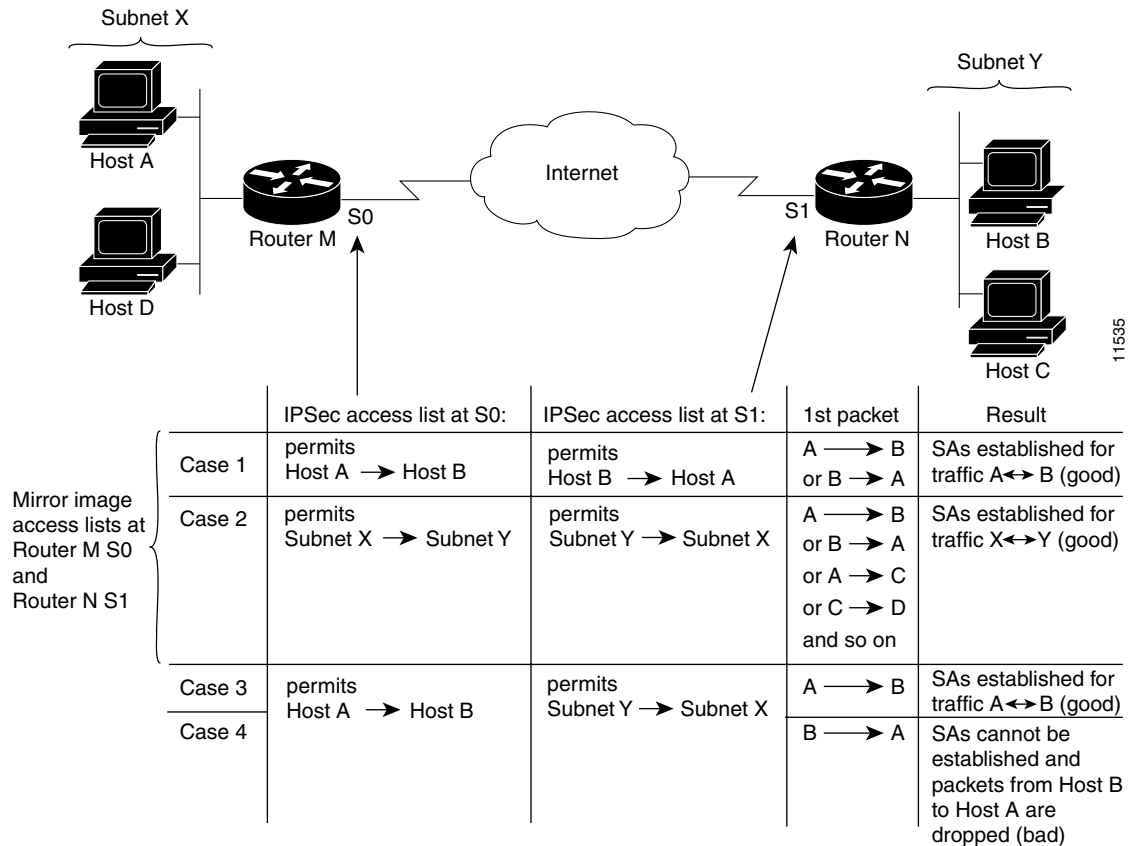
The following example shows how having a **deny** keyword in one crypto map sequence number and having a **permit** keyword for the same subnet and IP range in another crypto map sequence number is not supported.

```
crypto map mymap 10 ipsec-isakmp  
  set peer 192.168.1.1  
  set transform-set test  
  match address 101  
crypto map mymap 20 ipsec-isakmp  
  set peer 192.168.1.2  
  set transform-set test  
  match address 102  
  
access-list 101 deny ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255  
access-list 101 permit ip 10.0.0.0 0.255.255.255 172.16.0.0 0.15.255.255  
  
access-list 102 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
```

Mirror Image Crypto Access Lists at Each IPSec Peer

Cisco recommends that for every crypto access list specified for a static crypto map entry that you define at the local peer, you define a “mirror image” crypto access list at the remote peer. This ensures that traffic that has IPSec protection applied locally can be processed correctly at the remote peer. (The crypto map entries themselves must also support common transforms and must refer to the other system as a peer.)

[Figure 56](#) shows some sample scenarios when you have mirror image access lists and when you do not have mirror image access lists.

Figure 56 Mirror Image vs. Nonmirror Image Crypto Access Lists (for IPSec)

As Figure 56 indicates, IPSec SAs can be established as expected whenever the two peers' crypto access lists are mirror images of each other. However, an IPSec SA can be established only some of the time when the access lists are not mirror images of each other. This can happen in the case where an entry in one peer's access list is a subset of an entry in the other peer's access list, such as shown in Cases 3 and 4 of Figure 56. IPSec SA establishment is critical to IPSec—without SAs, IPSec does not work, causing any packets matching the crypto access list criteria to be silently dropped instead of being forwarded with IPSec.

In Figure 56, an SA cannot be established in Case 4. This is because SAs are always requested according to the crypto access lists at the initiating packet's end. In Case 4, Router N requests that all traffic between Subnet X and Subnet Y be protected, but this is a superset of the specific flows permitted by the crypto access list at Router M so the request is therefore not permitted. Case 3 works because Router M's request is a subset of the specific flows permitted by the crypto access list at Router N.

Because of the complexities introduced when crypto access lists are not configured as mirror images at peer IPSec devices, Cisco strongly encourages you to use mirror image crypto access lists.

When to Use the **any** Keyword in Crypto Access Lists

When you create crypto access lists, using the **any** keyword could cause problems. Cisco discourages the use of the **any** keyword to specify source or destination addresses.

The **any** keyword in a **permit** statement is discouraged when you have multicast traffic flowing through the IPSec interface; the **any** keyword can cause multicast traffic to fail.

The **permit any any** statement is strongly discouraged, because this causes all outbound traffic to be protected (and all protected traffic sent to the peer specified in the corresponding crypto map entry) and requires protection for all inbound traffic. Then, all inbound packets that lack IPSec protection are silently dropped, including packets for routing protocols, Network Time Protocol (NTP), echo, echo response, and so on.

You need to be sure you define which packets to protect. If you *must* use the **any** keyword in a **permit** statement, you must preface that statement with a series of **deny** statements to filter out any traffic (that would otherwise fall within that **permit** statement) that you do not want to be protected.

Also, use of **any** keyword in access control lists (ACLs) with reverse route injection (RRI) is not supported. (For more information on RRI, see the section “[Creating Crypto Map Sets](#).”)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**log**]
or
ip access-list extended *name*
4. Repeat Step 3 for each crypto access list you want to create.

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	access-list <i>access-list-number</i> { deny permit } <i>protocol source source-wildcard destination destination-wildcard</i> [log] Example: Router(config)# access-list 100 permit ip 10.0.68.0 0.0.0.255 10.1.1.0 0.0.0.255 or ip access-list extended <i>name</i> Example: Router(config)# ip access-list extended vpn-tunnel	Specifies conditions to determine which IP packets are protected. ¹ Enable or disable crypto for traffic that matches these conditions. Tip Cisco recommends that you configure “mirror image” crypto access lists for use by IPSec and that you avoid using the any keyword.
Step 4	—	Repeat Step 3 for each crypto access list you want to create.

1. You specify conditions using an IP access list designated by either a number or a name. The **access-list** command designates a numbered extended access list; the **ip access-list extended** command designates a named access list.

What to Do Next

After at least one crypto access list is created, a transform set needs to be defined as described in the section [“Defining Transform Sets: A Combination of Security Protocols and Algorithms.”](#)

Next the crypto access lists need to be associated to particular interfaces when you configure and apply crypto map sets to the interfaces are configured and applied (following instructions in the sections [“Creating Crypto Map Sets”](#) and [“Applying Crypto Map Sets to Interfaces”](#)).

Defining Transform Sets: A Combination of Security Protocols and Algorithms

Perform this task to define a transform set that is to be used by the IPSec peers during IPSec security association negotiations with IKE.

Restrictions

If you are specifying SEAL encryption, note the following restrictions:

- Your router and the other peer must not have hardware IPSec encryption.
- Your router and the other peer must support IPSec.
- Your router and the other peer must support the k9 subsystem.
- SEAL encryption is available only on Cisco equipment. Therefore, interoperability is not possible.

About Transform Sets

A transform set represents a certain combination of security protocols and algorithms. During the IPSec SA negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

You can specify multiple transform sets, and then specify one or more of these transform sets in a crypto map entry. The transform set defined in the crypto map entry is used in the IPSec SA negotiation to protect the data flows specified by that crypto map entry’s access list.

During IPSec security association negotiations with IKE, the peers search for a transform set that is the same at both peers. When such a transform set is found, it is selected and is applied to the protected traffic as part of both peers’ IPSec SAs. (With manually established SAs, there is no negotiation with the peer, so both sides must specify the same transform set.)

If you change a transform set definition, the change is only applied to crypto map entries that reference the transform set. The change is not applied to existing security associations, but is used in subsequent negotiations to establish new SAs. If you want the new settings to take effect sooner, you can clear all or part of the SA database by using the **clear crypto sa** command

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2* [*transform3*]]

4. **mode** [**tunnel** | **transport**]
5. **exit**
6. **clear crypto sa** [peer {*ip-address* | **peer-name**} | sa map *map-name* | sa entry *destination-address protocol spi*]
7. **show crypto ipsec transform-set** [**tag** *transform-set-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto ipsec transform-set <i>transform-set-name transform1</i> [<i>transform2</i> [<i>transform3</i>]] Example: Router(config)# crypto ipsec transform-set aesset esp-aes 256 esp-sha-hmac	Defines a transform set and enters crypto transform configuration mode. There are complex rules defining which entries you can use for the transform arguments. These rules are explained in the command description for the crypto ipsec transform-set command, and Table 46 provides a list of allowed transform combinations.
Step 4	mode [tunnel transport] Example: Router(cfg-crypto-tran)# mode transport	(Optional) Changes the mode associated with the transform set. The mode setting is applicable only to traffic whose source and destination addresses are the IPSec peer addresses; it is ignored for all other traffic. (All other traffic is in tunnel mode only.)
Step 5	exit Example: Router(config)# exit	Exits global configuration mode.

	Command or Action	Purpose
Step 6	<pre>clear crypto sa [peer {ip-address peer-name} sa map map-name sa entry destination-address protocol spi]</pre> <p>Example: Router# clear crypto sa</p>	<p>(Optional) Clears existing IPSec security associations so that any changes to a transform set takes effect on subsequently established security associations.</p> <p>Manually established SAs are reestablished immediately.</p> <ul style="list-style-type: none"> Using the clear crypto sa command without parameters clear out the full SA database, which clears out active security sessions. You may also specify the peer, map, or entry keywords to clear out only a subset of the SA database.
Step 7	<pre>show crypto ipsec transform-set [tag transform-set-name]</pre> <p>Example: Router# show crypto ipsec transform-set</p>	<p>(Optional) Displays the configured transform sets.</p>

Table 46 shows allowed transform combinations.

Table 46 Allowed Transform Combinations

Transform Type	Transform	Description
AH Transform	ah-md5-hmac	AH with the MD5 (a Hash-based Message Authentication Code [HMAC] variant) authentication algorithm
	ah-sha-hmac	AH with the SHA (an HMAC variant) authentication algorithm
ESP Encryption Transform	esp-aes	ESP with the 128-bit AES encryption algorithm
	esp-aes 192	ESP with the 192-bit AES encryption algorithm
	esp-aes 256	ESP with the 256-bit AES encryption algorithm
	esp-des	ESP with the 56-bit DES encryption algorithm
	esp-3des	ESP with the 168-bit DES encryption algorithm (3DES or Triple DES)
	esp-null	Null encryption algorithm
	esp-seal	ESP with the 160-bit SEAL encryption algorithm.

Table 46 *Allowed Transform Combinations (continued)*

Transform Type	Transform	Description
ESP Authentication Transform	esp-md5-hmac	ESP with the MD5 (HMAC variant) authentication algorithm
	esp-sha-hmac	ESP with the SHA (HMAC variant) authentication algorithm
IP Compression Transform	comp-lzs	IP compression with the LZS algorithm

What to Do Next

After you have defined a transform set, you should create a crypto map as specified in the section [“Creating Crypto Map Sets.”](#)

Creating Crypto Map Sets

See one of the following sections, as appropriate, to help create crypto map sets:

- [Creating Static Crypto Maps](#)
- [Creating Dynamic Crypto Maps](#)
- [Creating Crypto Map Entries to Establish Manual SAs](#)

Prerequisites

Before you create crypto map entries, you should determine which type of crypto map—static, dynamic, or manual—best addresses the needs of your network. You should also understand the following concepts:

- [About Crypto Maps](#)
- [Load Sharing Among Crypto Maps](#)
- [Crypto Map Guidelines](#)

About Crypto Maps

Crypto map entries created for IPSec pull together the various parts used to set up IPSec SAs, including:

- Which traffic should be protected by IPSec (per a crypto access list)
- The granularity of the flow to be protected by a set of SAs
- Where IPSec-protected traffic should be sent (who the remote IPSec peer is)
- The local address to be used for the IPSec traffic (See the section [“Applying Crypto Map Sets to Interfaces”](#) for more details.)
- What IPSec SA should be applied to this traffic (selecting from a list of one or more transform sets)
- Whether SAs are manually established or are established via IKE
- Other parameters that might be necessary to define an IPSec SA

How Crypto Maps Work

Crypto map entries with the same crypto map name (but different map sequence numbers) are grouped into a crypto map set. Later, you apply these crypto map sets to interfaces; then, all IP traffic passing through the interface is evaluated against the applied crypto map set. If a crypto map entry sees outbound IP traffic that should be protected and the crypto map specifies the use of IKE, a SA is negotiated with the remote peer according to the parameters included in the crypto map entry; otherwise, if the crypto map entry specifies the use of manual SAs, an SA should have already been established via configuration. (If a dynamic crypto map entry sees outbound traffic that should be protected and no security association exists, the packet is dropped.)

The policy described in the crypto map entries is used during the negotiation of SAs. If the local router initiates the negotiation, it uses the policy specified in the static crypto map entries to create the offer to be sent to the specified IPSec peer. If the IPSec peer initiates the negotiation, the local router checks the policy from the static crypto map entries, as well as any referenced dynamic crypto map entries to decide whether to accept or reject the peer's request (offer).

For IPSec to succeed between two IPSec peers, both peers' crypto map entries must contain compatible configuration statements.

Compatible Crypto Maps: Establishing an SA

When two peers try to establish a SA, they must each have at least one crypto map entry that is compatible with one of the other peer's crypto map entries. For two crypto map entries to be compatible, they must at least meet the following criteria:

- The crypto map entries must contain compatible crypto access lists (for example, mirror image access lists). In the case where the responding peer is using dynamic crypto maps, the entries in the local crypto access list must be "permitted" by the peer's crypto access list.
- The crypto map entries must each identify the other peer (unless the responding peer is using dynamic crypto maps).
- The crypto map entries must have at least one transform set in common.

Load Sharing Among Crypto Maps

You can define multiple remote peers using crypto maps to allow for load sharing. Load sharing is useful because if one peer fails, there continues to be a protected path. The peer that packets are actually sent to is determined by the last peer that the router heard from (received either traffic or a negotiation request from) for a given data flow. If the attempt fails with the first peer, IKE tries the next peer on the crypto map list.

If you are not sure how to configure each crypto map parameter to guarantee compatibility with other peers, you might consider configuring dynamic crypto maps as described in the section "[Creating Dynamic Crypto Maps](#)." Dynamic crypto maps are useful when the establishment of the IPSec tunnels is initiated by the remote peer (such as in the case of an IPSec router fronting a server). They are not useful if the establishment of the IPSec tunnels is locally initiated, because the dynamic crypto maps are policy templates, not complete statements of policy. (Although the access lists in any referenced dynamic crypto map entry are used for crypto packet filtering.)

Crypto Map Guidelines

You can apply only one crypto map set to a single interface. The crypto map set can include a combination of IPSec/IKE and IPSec/manual entries. Multiple interfaces can share the same crypto map set if you want to apply the same policy to multiple interfaces.

If you create more than one crypto map entry for a given interface, use the *seq-num* argument of each map entry to rank the map entries: the lower the *seq-num* argument, the higher the priority. At the interface that has the crypto map set, traffic is evaluated against higher priority map entries first.

You must create multiple crypto map entries for a given interface if any of the following conditions exist:

- If different data flows are to be handled by separate IPSec peers.
- If you want to apply different IPSec security to different types of traffic (to the same or separate IPSec peers); for example, if you want traffic between one set of subnets to be authenticated, and traffic between another set of subnets to be both authenticated and encrypted. In this case the different types of traffic should have been defined in two separate access lists, and you must create a separate crypto map entry for each crypto access list.
- If you are not using IKE to establish a particular set of security associations, and want to specify multiple access list entries, you must create separate access lists (one per **permit** entry) and specify a separate crypto map entry for each access list.

Creating Static Crypto Maps


When IKE is used to establish SAs, the IPSec peers can negotiate the settings they use for the new security associations. This means that you can specify lists (such as lists of acceptable transforms) within the crypto map entry.

Perform this task to create crypto map entries that use IKE to establish the SAs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num ipsec-isakmp*
4. **match address** *access-list-id*
5. **set peer** {*hostname* | *ip-address*}
6. **set transform-set** *transform-set-name1* [*transform-set-name2...transform-set-name6*]
7. **set security-association lifetime** {*seconds seconds* | *kilobytes kilobytes*}
8. **set security-association level per-host**
9. **set pfs** [*group1* | *group2* | *group5*]
10. **exit**
11. **exit**
12. **show crypto map** [**interface** *interface* | tag *map-name*]

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto map <i>map-name seq-num ipsec-isakmp</i> Example: Router(config)# crypto map static-map 1 ipsec-isakmp	Names the crypto map entry to create (or modify), and enters crypto map configuration mode.
Step 4	match address <i>access-list-id</i> Example: Router(config-crypto-m)# match address vpn-tunnel	Names an extended access list. This access list determines which traffic should be protected by IPsec and which traffic should not be protected by IPsec security in the context of this crypto map entry.
Step 5	set peer { <i>hostname</i> <i>ip-address</i> } Example: Router(config-crypto-m)# set-peer 192.168.101.1	Specifies a remote IPsec peer, the peer to which IPsec protected traffic can be forwarded. Repeat for multiple remote peers.
Step 6	set transform-set <i>transform-set-name1</i> [<i>transform-set-name2</i> ... <i>transform-set-name6</i>] Example: Router(config-crypto-m)# set transform-set aasset	Specifies which transform sets are allowed for this crypto map entry. List multiple transform sets in order of priority (highest priority first).
Step 7	set security-association lifetime { seconds <i>seconds</i> kilobytes <i>kilobytes</i> } Example: Router (config-crypto-m)# set security-association lifetime seconds 2700	(Optional) Specifies a SA lifetime for the crypto map entry. By default, the SAs of the crypto map are negotiated according to the global lifetimes.
Step 8	set security-association level per-host Example: Router(config-crypto-m)# set security-association level per-host	(Optional) Specifies that separate SAs should be established for each source and destination host pair. By default, a single IPsec “tunnel” can carry traffic for multiple source hosts and multiple destination hosts.
		 Caution Use this command with care, because multiple streams between given subnets can rapidly consume resources.

	Command	Purpose
Step 9	set pfs [group1 group2 group 5] Example: Router(config-crypto-m)# set pfs group2	(Optional) Specifies that IPSec either should ask for perfect forward secrecy (PFS) when requesting new SAs for this crypto map entry or should demand PFS in requests received from the IPSec peer. By default, PFS is not requested. If no group is specified with this command, group1 is used as the default.
Step 10	exit Example: Router(config-crypto-m)# exit	Exits crypto-map configuration mode.
Step 11	exit Example: Router(config)# exit	Exits global configuration mode.
Step 12	show crypto map [interface <i>interface</i> tag <i>map-name</i>] Example: Router# show crypto map	Displays your crypto map configuration.

Troubleshooting Tips

Certain configuration changes take effect only when negotiating subsequent SAs. If you want the new settings to take immediate effect, you must clear the existing SAs so that they are re-established with the changed configuration. If the router is actively processing IPSec traffic, it is desirable to clear only the portion of the SA database that would be affected by the configuration changes (that is, clear only the SAs established by a given crypto map set). Clearing the full SA database should be reserved for large-scale changes, or when the router is processing very little other IPSec traffic.

To clear IPSec SAs, use the **clear crypto sa** command with appropriate parameters. (Omitting all parameters clears out the full SA database, which clears active security sessions.)

What to Do Next

After you have successfully created a static crypto map, you must apply the crypto map set to each interface through which IPSec traffic flows. To complete this task, see the section “[Applying Crypto Map Sets to Interfaces](#).”

Creating Dynamic Crypto Maps

Dynamic crypto maps can ease IPSec configuration and are recommended for use with networks where the peers are not always predetermined. To create dynamic crypto maps, you should understand the following concepts:

- [Dynamic Crypto Maps Overview](#)
- [Tunnel Endpoint Discovery \(TED\)](#)

Dynamic Crypto Maps Overview

Dynamic crypto maps are only available for use by IKE.

A dynamic crypto map entry is essentially a static crypto map entry without all the parameters configured. It acts as a policy template where the missing parameters are later dynamically configured (as the result of an IPSec negotiation) to match a remote peer's requirements. This allows remote peers to exchange IPSec traffic with the router even if the router does not have a crypto map entry specifically configured to meet all of the remote peer's requirements.

Dynamic crypto maps are not used by the router to initiate new IPSec security associations with remote peers. Dynamic crypto maps are used when a remote peer tries to initiate an IPSec security association with the router. Dynamic crypto maps are also used in evaluating traffic.

A dynamic crypto map set is included by reference as part of a crypto map set. Any crypto map entries that reference dynamic crypto map sets should be the lowest priority crypto map entries in the crypto map set (that is, have the highest sequence numbers) so that the other crypto map entries are evaluated first; that way, the dynamic crypto map set is examined only when the other (static) map entries are not successfully matched.

If the router accepts the peer's request, at the point that it installs the new IPSec security associations it also installs a temporary crypto map entry. This entry is filled in with the results of the negotiation. At this point, the router performs normal processing, using this temporary crypto map entry as a normal entry, even requesting new security associations if the current ones are expiring (based upon the policy specified in the temporary crypto map entry). Once the flow expires (that is, all of the corresponding security associations expire), the temporary crypto map entry is then removed.

For both static and dynamic crypto maps, if unprotected inbound traffic matches a **permit** statement in an access list, and the corresponding crypto map entry is tagged as "IPSec," then the traffic is dropped because it is not IPSec-protected. (This is because the security policy as specified by the crypto map entry states that this traffic must be IPSec-protected.)

For static crypto map entries, if outbound traffic matches a **permit** statement in an access list and the corresponding SA is not yet established, the router initiates new SAs with the remote peer. In the case of dynamic crypto map entries, if no SA existed, the traffic would simply be dropped (because dynamic crypto maps are not used for initiating new SAs).



Note

Use care when using the **any** keyword in **permit** entries in dynamic crypto maps. If it is possible for the traffic covered by such a **permit** entry to include multicast or broadcast traffic, the access list should include **deny** entries for the appropriate address range. Access lists should also include **deny** entries for network and subnet broadcast traffic, and for any other traffic that should not be IPSec protected.

Restrictions for Dynamic Crypto Maps

Dynamic crypto map entries specify crypto access lists that limit traffic for which IPSec SAs can be established. A dynamic crypto map entry that does not specify an access list is ignored during traffic filtering. A dynamic crypto map entry with an empty access list causes traffic to be dropped. If there is only one dynamic crypto map entry in the crypto map set, it must specify acceptable transform sets.

Tunnel Endpoint Discovery (TED)

Defining a dynamic crypto map allows only the receiving router to dynamically determine an IPSec peer. TED allows the initiating router to dynamically determine an IPSec peer for secure IPSec communications.

Dynamic TED helps to simplify IPSec configuration on the individual routers within a large network. Each node has a simple configuration that defines the local network that the router is protecting and the required IPSec transforms.

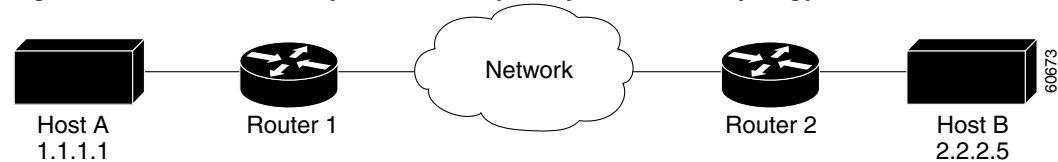
To have a large, fully-meshed network *without* TED, each peer needs to have static crypto maps to every other peer in the network. For example, if there are 100 peers in a large, fully-meshed network, each router needs 99 static crypto maps for each of its peers. With TED, only a single dynamic crypto map with TED enabled is needed because the peer is discovered dynamically. Thus, static crypto maps do not need to be configured for each peer.

**Note**

TED helps only in discovering peers; otherwise, TED does not function any differently than normal IPSec. TED does not improve the scalability of IPSec (in terms of performance or the number of peers or tunnels).

Figure 57 and the corresponding steps explain a sample TED network topology.

Figure 57 Tunnel Endpoint Discovery Sample Network Topology



- Step 1** Host A sends a packet that is destined for Host B.
- Step 2** Router 1 intercepts and reads the packet. According to the IKE policy, Router 1 contains the following information: the packet must be encrypted, there are no SAs for the packet, and TED is enabled. Thus, Router 1 drops the packet and sends a TED probe into the network. (The TED probe contains the IP address of Host A (as the source IP address) and the IP address of Host B (as the destination IP address) embedded in the payload.
- Step 3** Router 2 intercepts the TED probe and checks the probe against the ACLs that it protects; after the probe matches an ACL, it is recognized as a TED probe for proxies that the router protects. It then sends a TED reply with the IP address of Host B (as the source IP address) and the IP address of Host A (as the destination IP address) embedded in the payload.
- Step 4** Router 1 intercepts the TED reply and checks the payloads for the IP address and half proxy of Router 2. It then combines the source side of its proxy with the proxy found in the second payload and initiates an IKE session with Router 2; thereafter, Router 1 initiates an IPSec session with Router 2.

**Note**

IKE cannot occur until the peer is identified.

TED Versions

The following table lists the available TED versions:

Version	First Available Release	Description
TEDv1	12.0(5)T	Performs basic TED functionality on nonredundant networks.
TEDv2	12.1M	Enhanced to work with redundant networks with paths through multiple security gateways between the source and the destination.
TEDv3	12.2M	Enhanced to allow non-IP-related entries to be used in the access list.

TED Restrictions

TED has the following restrictions:

- It is Cisco proprietary.
- It is available only on dynamic crypto maps. (The dynamic crypto map template is based on the dynamic crypto map performing peer discovery. Although there are no access-list restrictions on the dynamic crypto map template, the dynamic crypto map template should cover data sourced from the protected traffic and the receiving router using the **any** keyword. When using the **any** keyword, include explicit **deny** statements to exempt routing protocol traffic prior to entering the **permit any** command.)
- TED works only in tunnel mode; that is, it does not work in transport mode.
- It is limited by the performance and scalability of limitation of IPsec on each individual platform.



Note

Enabling TED slightly decreases the general scalability of IPsec because of the set-up overhead of peer discovery, which involves an additional “round-trip” of IKE messages (TED probe and reply). Although minimal, the additional memory used to store data structures during the peer discovery stage adversely affects the general scalability of IPsec.

- The IP addresses must be able to be routed within the network.
- The access list used in the crypto map for TED can only contain IP-related entries—TCP, UDP, or any other protocol cannot be used in the access list.



Note

This restriction is no longer applicable in TEDv3.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto dynamic-map** *dynamic-map-name* *dynamic-seq-num*
4. **set transform-set** *transform-set-name1* [*transform-set-name2...transform-set-name6*]
5. **match address** *access-list-id*
6. **set peer** {*hostname* | *ip-address*}
7. **set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}

8. **set pfs** [group1 | group2 | group5]
9. **exit**
10. **exit**
11. **show crypto dynamic-map** [tag *map-name*]
12. **configure terminal**
13. **crypto map** *map-name seq-num ipsec-isakmp dynamic dynamic-map-name* [discover]

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto dynamic-map <i>dynamic-map-name dynamic-seq-num</i> Example: Router(config)# crypto dynamic-map test-map 1	Creates a dynamic crypto map entry and enters crypto map configuration mode.
Step 4	set transform-set <i>transform-set-name1</i> [<i>transform-set-name2...transform-set-name6</i>] Example: Router(config-crypto-m)# set transform-set aasset	Specifies which transform sets are allowed for the crypto map entry. List multiple transform sets in order of priority (highest priority first). This is the only configuration statement required in dynamic crypto map entries.

	Command	Purpose
Step 5	match address <i>access-list-id</i> Example: Router(config-crypto-m)# match address 101	<p>(Optional) Accesses list number or name of an extended access list.</p> <p>This access list determines which traffic should be protected by IPSec and which traffic should not be protected by IPSec security in the context of this crypto map entry.</p> <p>Note Although access-lists are optional for dynamic crypto maps, they are highly recommended.</p> <p>If this is configured, the data flow identity proposed by the IPSec peer must fall within a permit statement for this crypto access list.</p> <p>If this is not configured, the router accepts any data flow identity proposed by the IPSec peer. However, if this is configured but the specified access list does not exist or is empty, the router drops all packets. This is similar to static crypto maps because they also require that an access list be specified.</p> <p>Care must be taken if the any keyword is used in the access list, because the access list is used for packet filtering as well as for negotiation.</p> <p>You must configure a match address; otherwise, the behavior is not secure, and you cannot enable TED because packets are sent in the clear (unencrypted.)</p>
Step 6	set peer { <i>hostname</i> <i>ip-address</i> } Example: Router(config-crypto-m)# set peer 192.168.101.1	<p>(Optional) Specifies a remote IPSec peer. Repeat for multiple remote peers.</p> <p>Note This is rarely configured in dynamic crypto map entries. Dynamic crypto map entries are often used for unknown remote peers.</p>
Step 7	set security-association lifetime { seconds <i>seconds</i> kilobytes <i>kilobytes</i> } Example: Router (config-crypto-m)# set security-association lifetime seconds 7200	<p>(Optional) Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IP Security SAs.</p>
Step 8	set pfs [group1 group2 group5] Example: Router(config-crypto-m)# set pfs group2	<p>(Optional) Specifies that IPSec should ask for PFS when requesting new security associations for this crypto map entry or should demand PFS in requests received from the IPSec peer.</p> <p>By default, PFS is not requested. If no group is specified with this command, group1 is used as the default.</p>
Step 9	exit Example: Router(config-crypto-m)# exit	<p>Exits crypto-map configuration mode and returns to global configuration mode.</p>

	Command	Purpose
Step 10	exit Example: Router(config)# exit	Exits global configuration mode.
Step 11	show crypto dynamic-map [<i>tag map-name</i>] Example: Router# show crypto dynamic-map	(Optional) Displays information about dynamic crypto maps.
Step 12	configure terminal Example: Router# configure terminal	Returns to global configuration mode.
Step 13	crypto map <i>map-name</i> <i>seq-num</i> ipsec-isakmp dynamic <i>dynamic-map-name</i> [discover] Example: Router(config)# crypto map static-map 1 ipsec-isakmp dynamic test-map discover	(Optional) Adds a dynamic crypto map to a crypto map set. You should set the crypto map entries referencing dynamic maps to the lowest priority entries in a crypto map set. Note You must issue the discover keyword to enable TED.

Troubleshooting Tips

Certain configuration changes take effect only when negotiating subsequent SAs. If you want the new settings to take immediate effect, you must clear the existing SAs so that they are reestablished with the changed configuration. If the router is actively processing IPSec traffic, it is desirable to clear only the portion of the SA database that would be affected by the configuration changes (that is, clear only the SAs established by a given crypto map set). Clearing the full SA database should be reserved for large-scale changes, or when the router is processing very little other IPSec traffic.

To clear IPSec SAs, use the **clear crypto sa** command with appropriate parameters. (Omitting all parameters clears the full SA database, which clears active security sessions.)

What to Do Next

After you have successfully created a crypto map set, you must apply the crypto map set to each interface through which IPSec traffic flows. To complete this task, see the section “[Applying Crypto Map Sets to Interfaces](#).”

Creating Crypto Map Entries to Establish Manual SAs

The use of manual security associations is a result of a prior arrangement between the users of the local router and the IPSec peer. The two parties may begin with manual SAs and then move to using SAs established via IKE, or the remote party’s system may not support IKE. If IKE is not used for establishing the SAs, there is no negotiation of SAs, so the configuration information in both systems must be the same in order for traffic to be processed successfully by IPSec.

The local router can simultaneously support manual and IKE-established SAs, even within a single crypto map set.

There is very little reason to disable IKE on the local router (unless the router only supports manual SAs, which is unlikely).

**Note**

Access lists for crypto map entries tagged as **ipsec-manual** are restricted to a single **permit** entry and subsequent entries are ignored. In other words, the SAs established by that particular crypto map entry are only for a single data flow. To be able to support multiple manually established SAs for different kinds of traffic, define multiple crypto access lists, and then apply each one to a separate **ipsec-manual** crypto map entry. Each access list should include one **permit** statement defining what traffic to protect.

To create crypto map entries to establish manual SAs (that is, when IKE is not used to establish the SAs), perform this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num ipsec-manual*
4. **match address** *access-list-id*
5. **set peer** {*hostname* | *ip-address*}
6. **set transform-set** *transform-set-name*
7. **set session-key inbound ah spi hex-key-string**
or
set session-key outbound ah spi hex-key-string
8. **set session-key inbound esp spi cipher hex-key-string** [**authenticator** *hex-key-string*]
or
set session-key outbound esp spi cipher hex-key-string [**authenticator** *hex-key-string*]
9. **exit**
10. **exit**
11. **show crypto map** [**interface** *interface* | **tag** *map-name*]

DETAILED STEPS

	Command	Purpose
Step 1	enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
	Example: Router> enable	
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	

	Command	Purpose
Step 3	crypto map <i>map-name seq-num ipsec-manual</i> Example: Router(config)# crypto map mymap 10 ipsec-manual	Specifies the crypto map entry to create or modify and enters crypto map configuration mode.
Step 4	match address <i>access-list-id</i> Example: Router(config-crypto-m)# match address 102	Names an IPSec access list that determines which traffic should be protected by IPSec and which traffic should not be protected by IPSec in the context of this crypto map entry. (The access list can specify only one permit entry when IKE is not used.)
Step 5	set peer { <i>hostname</i> <i>ip-address</i> } Example: Router(config-crypto-m)# set peer 10.0.0.5	Specifies the remote IPSec peer. This is the peer to which IPSec protected traffic should be forwarded. (Only one peer can be specified when IKE is not used.)
Step 6	set transform-set <i>transform-set-name</i> Example: Router(config-crypto-m)# set transform-set someset	Specifies which transform set should be used. This must be the same transform set that is specified in the remote peer's corresponding crypto map entry. Note Only one transform set can be specified when IKE is not used.
Step 7	set session-key inbound ah <i>spi hex-key-string</i> Example: Router(config-crypto-m)# set session-key inbound ah 256 98765432109876549876543210987654 and set session-key outbound ah <i>spi hex-key-string</i> Example: Router(config-crypto-m)# set session-key outbound ah 256 fedcbafedcbafedcfedcbafedcbafedc	Sets the AH security parameter indexes (SPIs) and keys to apply to inbound and outbound protected traffic if the specified transform set includes the AH protocol. (This manually specifies the AH security association to be used with protected traffic.)
Step 8	set session-key inbound esp <i>spi cipher hex-key-string</i> [authenticator <i>hex-key-string</i>] Example: Router(config-crypto-m)# set session-key inbound esp 256 cipher 0123456789012345 and set session-key outbound esp <i>spi cipher hex-key-string</i> [authenticator <i>hex-key-string</i>] Example: Router(config-crypto-m)# set session-key outbound esp 256 cipher abcdefabcdefabcd	Sets the ESP SPIs and keys to apply to inbound and outbound protected traffic if the specified transform set includes the ESP protocol. Specifies the cipher keys if the transform set includes an ESP cipher algorithm. Specifies the authenticator keys if the transform set includes an ESP authenticator algorithm. (This manually specifies the ESP security association to be used with protected traffic.)

	Command	Purpose
Step 9	exit Example: Router(config-crypto-m)# exit	Exits crypto-map configuration mode and returns to global configuration mode.
Step 10	exit Example: Router(config)# exit	Exits global configuration mode.
Step 11	show crypto map [interface <i>interface</i> tag <i>map-name</i>] Example: Router# show crypto map	Displays your crypto map configuration.

Troubleshooting Tips

For manually established SAs, you must clear and reinitialize the SAs for the changes to take effect. To clear IPSec SAs, use the **clear crypto sa** command with appropriate parameters. (Omitting all parameters clears the full SA database, which clears active security sessions.)

What to Do Next

After you have successfully created a crypto map set, you must apply the crypto map set to each interface through which IPSec traffic flows. To complete this task, see the section “[Applying Crypto Map Sets to Interfaces](#).”

Applying Crypto Map Sets to Interfaces

You need to apply a crypto map set to each interface through which IPSec traffic flows. Applying the crypto map set to an interface instructs the router to evaluate all the interface’s traffic against the crypto map set and to use the specified policy during connection or security association negotiation on behalf of traffic to be protected by crypto.

Perform this task to apply a crypto map to an interface.

Redundant Interfaces Sharing the Same Crypto Map

For redundancy, you could apply the same crypto map set to more than one interface. The default behavior is as follows:

- Each interface has its own piece of the security association database.
- The IP address of the local interface is used as the local address for IPSec traffic originating from or destined to that interface.

If you apply the same crypto map set to multiple interfaces for redundancy purposes, you need to specify an identifying interface. One suggestion is to use a loopback interface as the identifying interface. This has the following effects:

- The per-interface portion of the IPSec security association database is established one time and shared for traffic through all the interfaces that share the same crypto map.

- The IP address of the identifying interface is used as the local address for IPSec traffic originating from or destined to those interfaces sharing the same crypto map set.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **crypto map** *map-name*
5. **exit**
6. **crypto map** *map-name* **local-address** *interface-id*
7. **exit**
8. **show crypto map** [**interface** *interface*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Router(config)# Interface FastEthernet 0/0	Configures an interface and enters interface configuration mode.
Step 4	crypto map <i>map-name</i> Example: Router(config-if)# crypto map mymap	Applies a crypto map set to an interface.
Step 5	exit Example: Router(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.
Step 6	crypto map <i>map-name</i> local-address <i>interface-id</i> Example: Router(config)# crypto map mymap local-address loopback0	(Optional) Permits redundant interfaces to share the same crypto map using the same local identity.

	Command or Action	Purpose
Step 7	exit Example: Router(config)# exit	(Optional) Exits global configuration mode.
Step 8	show crypto map [interface <i>interface</i>] Example: Router# show crypto map	(Optional) Displays your crypto map configuration

Configuration Examples for Configuring an IPsec VPN

This section contains the following configuration example:

- [AES-Based Static Crypto Map: Example, page 32](#)

AES-Based Static Crypto Map: Example

The following example is a portion of the **show running-config** command. This example shows how to configure a static crypto map and define AES as the encryption method.

```
crypto isakmp policy 10
  encryption aes 256
  authentication pre-share
  lifetime 180

crypto isakmp key cisco123 address 10.0.110.1
!
!
crypto ipsec transform-set aasset esp-aes 256 esp-sha-hmac
mode transport
!
crypto map aesmap 10 ipsec-isakmp
  set peer 10.0.110.1
  set transform-set aasset
  match address 120
!
!
!
voice call carrier capacity active
!
!
mta receive maximum-recipients 0
!
!
interface FastEthernet0/0
  ip address 10.0.110.2 255.255.255.0
  ip nat outside
  no ip route-cache
  no ip mroute-cache
  duplex auto
  speed auto
  crypto map aesmap
!
interface Serial0/0
```

```

no ip address
shutdown
!
interface FastEthernet0/1
 ip address 11.0.110.1 255.255.255.0
 ip nat inside
 no ip route-cache
 no ip mroute-cache
 duplex auto
 speed auto
!
ip nat inside source list 110 interface FastEthernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 10.5.1.1
ip route 12.0.110.0 255.255.255.0 FastEthernet0/0
ip route 172.18.124.0 255.255.255.0 10.5.1.1
ip route 172.18.125.3 255.255.255.255 10.5.1.1
ip http server
!
!
access-list 110 deny ip 11.0.110.0 0.0.0.255 12.0.110.0 0.0.0.255
access-list 110 permit ip 11.0.110.0 0.0.0.255 any
access-list 120 permit ip 11.0.110.0 0.0.0.255 12.0.110.0 0.0.0.255
!

```

Additional References

The following sections provide references related to IPSec VPN configuration.

Related Documents

Related Topic	Document Title
IKE configuration	“Configuring IKE for IPSec VPNs” module
IKE, IPSec, and PKI configuration commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<i>Cisco IOS Security Command Reference</i> , Release 12.4

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
<ul style="list-style-type: none"> CISCO-IPSEC-FLOW-MONITOR- MIB CISCO-IPSEC-MIB CISCO-IPSEC-POLICY-MAP-MIB 	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

RFCs

RFCs	Title
RFC 2401	Security Architecture for the Internet Protocol
RFC 2402	<i>IP Authentication Header</i>
RFC 2403	The Use of HMAC-MD5-96 within ESP and AH
RFC 2404	The Use of HMAC-SHA-1-96 within ESP and AH
RFC 2405	The ESP DES-CBC Cipher Algorithm With Explicit IV
RFC 2406	<i>IP Encapsulating Security Payload (ESP)</i>
RFC 2407	The Internet IP Security Domain of Interpretation for ISAKMP
RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Glossary

anti-replay—Security service where the receiver can reject old or duplicate packets to protect itself against replay attacks. IPSec provides this optional service by use of a sequence number combined with the use of data authentication. Cisco IOS IPSec provides this service whenever it provides the data authentication service, except for manually established SAs (that is, SAs established by configuration and not by IKE).

data authentication—Verification of the integrity and origin of the data.

Data authentication can refer either to integrity alone or to both of these concepts (although data origin authentication is dependent upon data integrity).

data confidentiality—Security service in which the protected data cannot be observed.

data flow—Grouping of traffic, identified by a combination of source address or mask; destination address or mask; IP next protocol field, and source and destination ports, where the protocol and port fields can have the values of **any**. IPSec protection is applied to data flows.

peer—In the context of this module, a “peer” is a router or other device that participates in IPSec.

PFS—perfect forward secrecy. Cryptographic characteristic associated with a derived shared secret value. With PFS, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys.

SA—security association. Description of how two or more entities use security services in the context of a particular security protocol (AH or ESP) to communicate securely on behalf of a particular data flow. The transform and the shared secret keys are used for protecting the traffic.

SPI—security parameter index. A number which, together with a destination IP address and security protocol, uniquely identifies a particular security association. Without IKE, the SPI is manually specified for each security association.

transform—List of operations performed on a dataflow to provide data authentication, data confidentiality, and data compression. For example, one transform is the ESP protocol with the HMAC-MD5 authentication algorithm; another transform is the AH protocol with the 56-bit DES encryption algorithm and the ESP protocol with the HMAC-SHA authentication algorithm.

tunnel—In the context of this module, “tunnel” is a secure communication path between two peers, such as two routers. It does not refer to using IPSec in tunnel mode.



Note

Refer to *Internetworking Terms and Acronyms* for terms not included in this glossary.

Feature Information for Security for VPNs with IPSec

[Table 47](#) lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for a specific command was introduced, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

[Table 47](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 47 *Feature Information for Configuring Security for IPSec VPNs*

Feature Name	Software Releases	Feature Configuration Information
Advanced Encryption Standard (AES)	12.2(8)T	<p>This feature adds support for the new encryption standard AES, which is a privacy transform for IPSec and IKE and has been developed to replace DES.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Supported Standards • Defining Transform Sets: A Combination of Security Protocols and Algorithms <p>The following commands were modified by this feature: crypto ipsec transform-set, encryption (IKE policy), show crypto ipsec transform-set, show crypto isakmp policy</p>
DES/3DES/AES VPN Encryption Module (AIM-VPN/EPII, AIM-VPN/HPII, AIM-VPN/BPII Family)	12.3(7)T	<p>This feature describes which VPN encryption hardware AI) and NM are supported in certain Cisco IOS software releases.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> • AIMs and NM Support
SEAL Encryption	12.3(7)T	<p>This feature adds support for SEAL encryption in IPSec.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> • Supported Standards • Defining Transform Sets: A Combination of Security Protocols and Algorithms <p>The following command was modified by this feature: crypto ipsec transform-set</p>
Software IPPCP (LZS) with Hardware Encryption	12.2(13)T	<p>This feature allows customers to use LZS software compression with IPSec when a VPN module is in Cisco 2600 and Cisco 3600 series routers.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> • AIMs and NM Support
IKE Shared Secret Using AAA Server	Cisco IOS XE Release 2.1	<p>This feature was introduced on Cisco ASR 1000 Series Routers.</p>



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Cisco Easy VPN Remote

First Published: November 25, 2002

Last Updated: July 11, 2008

This document provides information on configuring and monitoring the Cisco Easy VPN Remote feature to create IPsec Virtual Private Network (VPN) tunnels between a supported router and an Easy VPN server (Cisco IOS router, VPN 3000 concentrator, or Cisco PIX Firewall) that supports this form of IPsec encryption and decryption.

For the benefits of this feature, see the section “[Benefits of the Cisco Easy VPN Remote Feature.](#)”

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Easy VPN Remote](#)” section on page 107.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Cisco Easy VPN Remote, page 2](#)
- [Restrictions for Cisco Easy VPN Remote, page 2](#)
- [Information About Cisco Easy VPN Remote, page 4](#)
- [How to Configure Cisco Easy VPN Remote, page 35](#)
- [Configuration Examples for Cisco Easy VPN Remote, page 66](#)
- [Additional References, page 101](#)
- [Command Reference, page 106](#)
- [Feature Information for Easy VPN Remote, page 107](#)
- [Glossary, page 111](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008 Cisco Systems, Inc. All rights reserved.

Prerequisites for Cisco Easy VPN Remote

Cisco Easy VPN Remote Feature

- A Cisco 800 series router running Cisco IOS Release 12.2(15)T, 12.3(2)T, 12.3(4)T, 12.3(7)T, or 12.3(7)XR2 configured as a Cisco Easy VPN remote.
- A Cisco 1700 series router running Cisco IOS Release 12.2(15)T, 12.3(2)T, 12.3(4)T, 12.3(7)T, or 12.3(7)XR, configured as a Cisco Easy VPN remote.
- A Cisco 1800 series fixed configuration router running Cisco IOS Release 12.3(8)YI.
- A Cisco uBR905 or Cisco uBR925 cable access router running Cisco IOS Release 12.2(15)T, configured as a Cisco Easy VPN remote.
- Another Cisco router or VPN concentrator that supports the Cisco Easy VPN Server feature and that is configured as a Cisco IOS Easy VPN server. See the “[Required Easy VPN Servers](#)” section for a detailed list.

Reactivate Primary Peer Feature

- An existing Easy VPN remote configuration can be enhanced to accommodate the Reactivate Primary Peer feature using the **peer** command (and **default** keyword) and the **idle-time** command. After the tunnel between the Easy VPN remote and a nondefault peer is working, the Reactivate Primary Peer features takes effect, that is, the Easy VPN remote periodically tries to check the connectivity with the primary peer. Any time the Easy VPN remote detects that the link is working, the Easy VPN remote tears down the existing connection and brings up the tunnel with the primary peer.

Restrictions for Cisco Easy VPN Remote

Required Easy VPN Servers

The Cisco Easy VPN Remote feature requires that the destination peer be a Cisco IOS Easy VPN server or VPN concentrator that supports the Cisco Easy VPN Server feature. At the time of publication, servers or concentrators that support this feature include the following platforms when running the indicated software releases:

- Cisco 806, Cisco 826, Cisco 827, Cisco 828, Cisco 831, Cisco 836, and Cisco 837 routers—Cisco IOS Release 12.2(8)T or later release. Cisco 800 series routers are not supported in Cisco IOS Release 12.3(7)XR, but they are supported in Cisco IOS Release 12.3(7)XR2.
- Cisco 870 series—Cisco IOS Release 12.3(8)YI1.
- Cisco 1700 series—Cisco IOS Release 12.2(8)T or later release.
- Cisco 1800 series fixed configuration router—Cisco IOS Release 12.3(8)YI.
- Cisco 1812 router—Cisco IOS Release 12.3(8)YH.
- Cisco 2600 series—Cisco IOS Release 12.2(8)T or later release.
- Cisco 3620—Cisco IOS Release 12.2(8)T or later release.
- Cisco 3640—Cisco IOS Release 12.2(8)T or later release.
- Cisco 3660—Cisco IOS Release 12.2(8)T or later release.
- Cisco 7100 series VPN routers—Cisco IOS Release 12.2(8)T or later release.
- Cisco 7200 series routers—Cisco IOS Release 12.2(8)T or later release.

- Cisco 7500 series routers—Cisco IOS Release 12.2(8)T or later release.
- Cisco PIX 500 series—Software Release 6.2 or later release.
- Cisco VPN 3000 series—Software Release 3.11 or later release.

Only ISAKMP Policy Group 2 Supported on Easy VPN Servers

The Unity Protocol supports only Internet Security Association Key Management Protocol (ISAKMP) policies that use group 2 (1024-bit Diffie-Hellman) Internet Key Exchange (IKE) negotiation, so the Easy VPN server being used with the Cisco Easy VPN Remote feature must be configured for a group 2 ISAKMP policy. The Easy VPN server cannot be configured for ISAKMP group 1 or group 5 when being used with a Cisco Easy VPN client.

Transform Sets Supported

To ensure a secure tunnel connection, the Cisco Easy VPN Remote feature does not support transform sets that provide encryption without authentication (ESP-DES and ESP-3DES) or transform sets that provide authentication without encryption (ESP-NUL ESP-SHA-HMAC and ESP-NUL ESP-MD5-HMAC).



Note

The Cisco Unity Client Protocol does not support Authentication Header (AH) authentication, but Encapsulation Security Protocol (ESP) is supported.

Dial Backup for Easy VPN Remotes

Line-status-based backup is not supported in this feature.

Network Address Translation Interoperability Support

Network Address Translation (NAT) interoperability is not supported in client mode with split tunneling.

Virtual IPsec Interface Restrictions

- For the Virtual IPsec Interface Support feature to work, virtual templates support is needed.
- If you are using a virtual tunnel interface on the Easy VPN remote device, it is recommended that you configure the server for a virtual tunnel interface.

Dual Tunnel Support

The following restrictions apply if you are using dual tunnels that share common inside and outside interfaces:

- If dual tunnels are configured, one of the tunnels should have a split tunnel configured on the server.
- Web Intercept can be configured for only one of the tunnels. Web Intercept should not be used for the voice tunnel.
- Web Intercept cannot be used for IP phones until authorization proxy becomes aware of how to bypass the IP phone.
- Some features, such as Pushing a Configuration URL Through a Mode-Configuration Exchange, can be used only through a single tunnel.

cTCP Support on Easy VPN Clients

- cTCP listens on only up to 10 ports.
- If there are other applications registered for the port on which cTCP is enabled, those applications will not work.

Information About Cisco Easy VPN Remote

To configure the Cisco Easy VPN Remote features, you should understand the following concepts:

- [Benefits of the Cisco Easy VPN Remote Feature, page 4](#)
- [Cisco Easy VPN Remote Overview, page 4](#)
- [Modes of Operation, page 5](#)
- [Authentication, page 8](#)
- [Tunnel Activation Options, page 17](#)
- [Dead Peer Detection Stateless Failover Support, page 18](#)
- [Cisco Easy VPN Remote Features, page 19](#)

Benefits of the Cisco Easy VPN Remote Feature

- Allows dynamic configuration of end-user policy, requiring less manual configuration by end users and field technicians, thus reducing errors and further service calls.
- Allows the provider to change equipment and network configurations as needed, with little or no reconfiguration of the end-user equipment.
- Provides for centralized security policy management.
- Enables large-scale deployments with rapid user provisioning.
- Eliminates the need for end users to purchase and configure external VPN devices.
- Eliminates the need for end users to install and configure Easy VPN Client software on their PCs.
- Offloads the creation and maintenance of the VPN connections from the PC to the router.
- Reduces interoperability problems between the different PC-based software VPN clients, external hardware-based VPN solutions, and other VPN applications.
- Sets up a single IPsec tunnel regardless of the number of multiple subnets that are supported and the size of the split-include list.

Cisco Easy VPN Remote Overview

Cable modems, xDSL routers, and other forms of broadband access provide high-performance connections to the Internet, but many applications also require the security of VPN connections that perform a high level of authentication and that encrypt the data between two particular endpoints. However, establishing a VPN connection between two routers can be complicated and typically requires tedious coordination between network administrators to configure the VPN parameters of the two routers.

The Cisco Easy VPN Remote feature eliminates much of this tedious work by implementing Cisco Unity Client Protocol, which allows most VPN parameters to be defined at a Cisco IOS Easy VPN server. This server can be a dedicated VPN device, such as a Cisco VPN 3000 concentrator or a Cisco PIX Firewall or a Cisco IOS router that supports the Cisco Unity Client Protocol.

After the Cisco Easy VPN server has been configured, a VPN connection can be created with minimal configuration on an Easy VPN remote, such as a Cisco 800 series router or a Cisco 1700 series router. When the Easy VPN remote initiates the VPN tunnel connection, the Cisco Easy VPN server pushes the IPsec policies to the Easy VPN remote and creates the corresponding VPN tunnel connection.

The Cisco Easy VPN Remote feature provides for automatic management of the following details:

- Negotiating tunnel parameters, such as addresses, algorithms, and lifetime.
- Establishing tunnels according to the parameters that were set.
- Automatically creating the NAT or Port Address Translation (PAT) and associated access lists that are needed, if any.
- Authenticating users, that is, ensuring that users are who they say they are by way of usernames, group names, and passwords.
- Managing security keys for encryption and decryption.
- Authenticating, encrypting, and decrypting data through the tunnel.

Modes of Operation

The Cisco Easy VPN Remote feature supports three modes of operation: client, network extension, and network extension plus:

- **Client**—Specifies that NAT or PAT be done so that the PCs and other hosts at the remote end of the VPN tunnel form a private network that does not use any IP addresses in the IP address space of the destination server.

An enhancement has been made so that the IP address that is received via mode configuration is automatically assigned to an available loopback interface. The IPsec Security Associations (SAs) for this IP address are automatically created by Easy VPN Remote. The IP address is typically used for troubleshooting (using ping, Telnet, and Secure Shell).

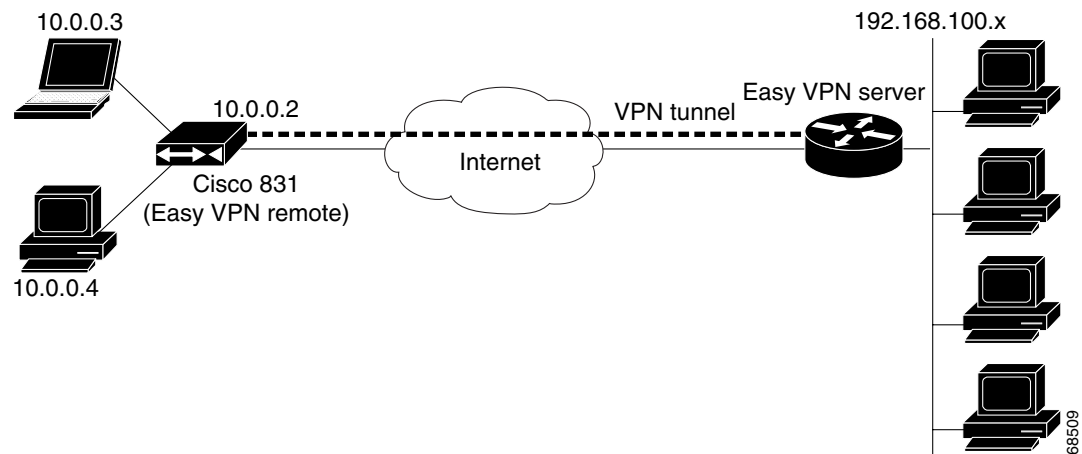
- **Network extension**—Specifies that the PCs and other hosts at the client end of the VPN tunnel should be given IP addresses that are fully routable and reachable by the destination network over the tunneled network so that they form one logical network. PAT is not used, which allows the client PCs and hosts to have direct access to the PCs and hosts at the destination network.
- **Network extension plus (mode network-plus)**—Identical to network extension mode with the additional capability of being able to request an IP address via mode configuration and automatically assign it to an available loopback interface. The IPsec SAs for this IP address are automatically created by Easy VPN Remote. The IP address is typically used for troubleshooting (using ping, Telnet, and Secure Shell).

All modes of operation also optionally support split tunneling, which allows secure access to corporate resources through the VPN tunnel while also allowing Internet access through a connection to an Internet service provider (ISP) or other service—thereby eliminating the corporate network from the path for web access.

Client Mode and Network Extension Mode Scenarios

[Figure 1](#) illustrates the client mode of operation. In this example, the Cisco 831 router provides access to two PCs, which have IP addresses in the 10.0.0.0 private network space. These PCs connect to the Ethernet interface on the Cisco 831 router, which also has an IP address in the 10.0.0.0 private network space. The Cisco 831 router performs NAT or PAT translation over the VPN tunnel so that the PCs can access the destination network.

Figure 1 Cisco Easy VPN Remote Connection



Note

The diagram in [Figure 1](#) could also represent a split tunneling connection, in which the client PCs can access public resources in the global Internet without including the corporate network in the path for the public resources.

[Figure 2](#) also illustrates the client mode of operation, in which a VPN concentrator provides destination endpoints to multiple xDSL clients. In this example, Cisco 800 series routers provide access to multiple small business clients, each of which uses IP addresses in the 10.0.0.0 private network space. The Cisco 800 series routers perform NAT or PAT translation over the VPN tunnel so that the PCs can access the destination network.

Figure 2 Cisco Easy VPN Remote Connection (using a VPN concentrator)

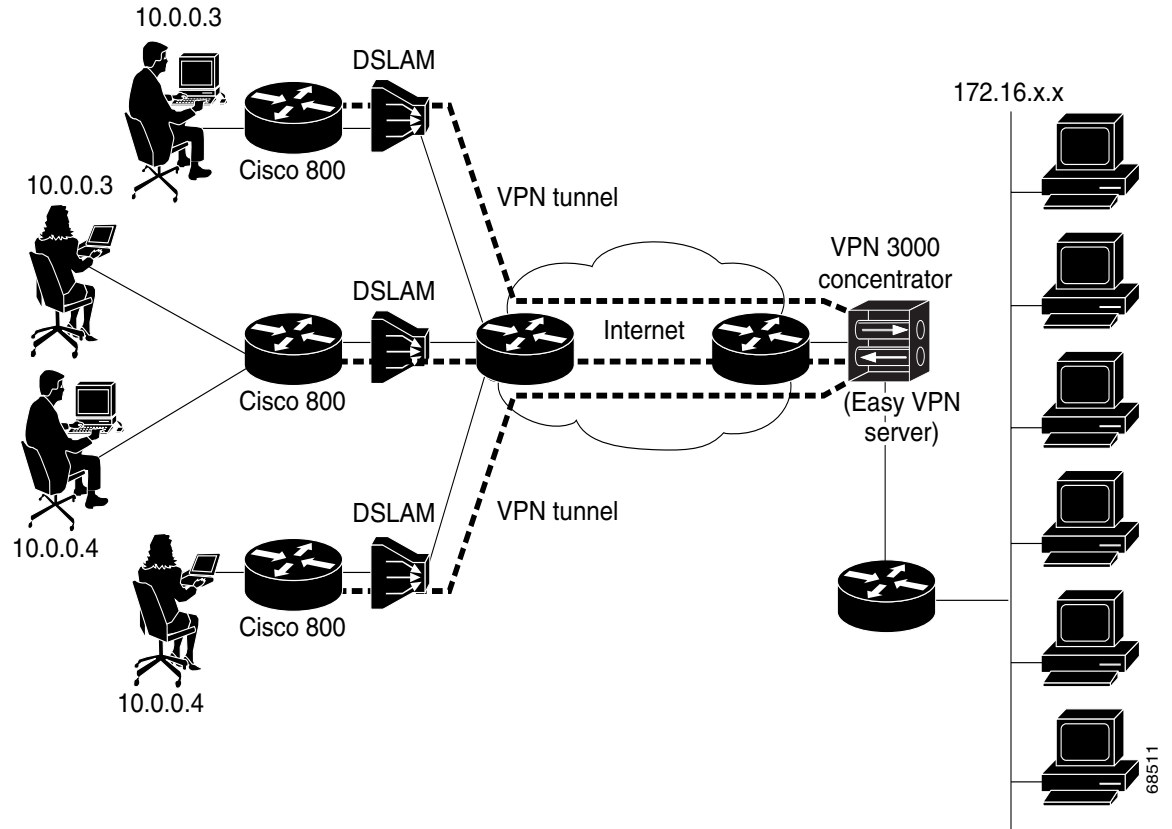
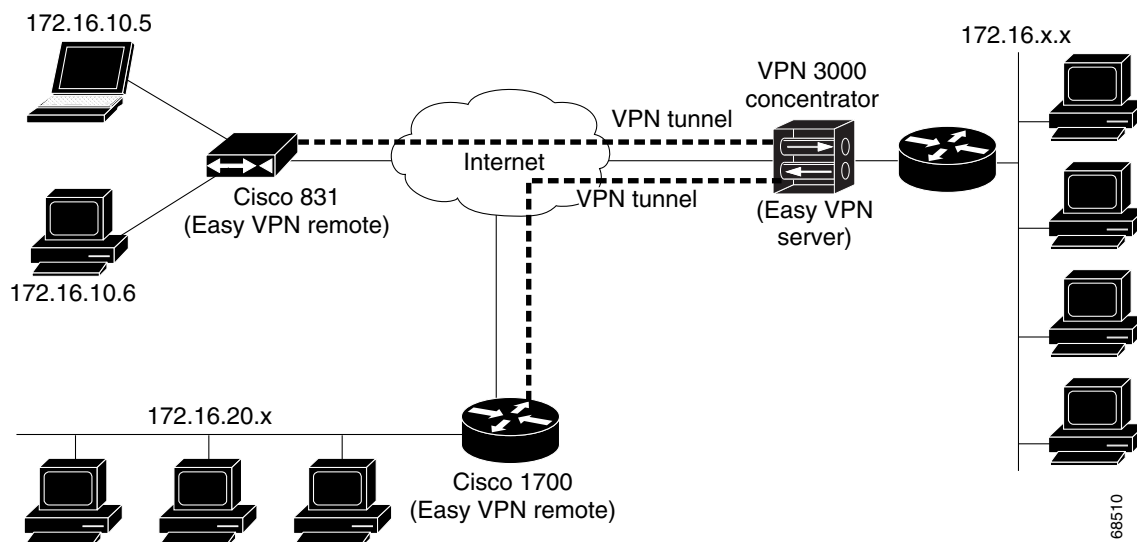


Figure 3 illustrates the network extension mode of operation. In this example, the Cisco 831 router and Cisco 1700 series router both act as Cisco Easy VPN remote devices, connecting to a Cisco VPN 3000 concentrator.

The client hosts are given IP addresses that are fully routable by the destination network over the tunnel. These IP addresses could be either in the same subnet space as the destination network or in separate subnets, assuming that the destination routers are configured to properly route those IP addresses over the tunnel.

In this example, the PCs and hosts attached to the two routers have IP addresses that are in the same address space as the destination enterprise network. The PCs connect to the Ethernet interface of the Cisco 831 router, which also has an IP address in the enterprise address space. This scenario provides a seamless extension of the remote network.

Figure 3 Cisco Easy VPN Network Extension Connection



Authentication

The Cisco Easy VPN Remote feature supports a two-stage process for authenticating the remote router to the central concentrator. The first step is Group Level Authentication and is part of the control channel creation. In this first stage, two types of authentication credentials can be used: either preshared keys or digital certificates. The following paragraphs provide details about these options.

The second authentication step is called Extended Authentication or Xauth. In this step, the remote side (in this case the Easy VPN router) submits a username and password to the central site router. This step is the same process as that which occurs when a user of the Cisco VPN software client on a PC enters his or her username and password to activate his or her VPN tunnel. When using the router, the difference is that the router itself is being authenticated to the network, not a PC with Cisco VPN Client software. Xauth is an optional step (it can be disabled) but is normally enabled to improve security. After Xauth is successful and the tunnel comes up, all PCs behind the Easy VPN remote router have access to the tunnel.

If Xauth is enabled, it is key to decide how to input the username and password. There are two options. The first option is to store the Xauth username and password in the configuration file of the router. This option is typically used if the router is shared between several PCs and the goal is to keep the VPN tunnel up all the time (see the section "[Automatic Activation](#)") or to have the router automatically bring up the tunnel whenever there is data to be sent (see the section "[Traffic-Triggered Activation](#)"). An example of this application is a branch office situation, in which the users in the branch office want the VPN tunnel to be available whenever they have data to send and do not want to have to do anything special to activate the VPN tunnel. If the PCs in the branch office must be individually authenticated on the basis of the ID of each user, the correct configuration is to put the Easy VPN router in Automatic Activation mode to keep the tunnel "up" all the time and to use Cisco IOS Authentication Proxy or 802.1x to authenticate the individual PCs. Because the tunnel is always up, Authentication Proxy or 802.1x can access a central site user database such as AAA/RADIUS to authenticate the individual user requests as they are submitted by PC users. (See the "[Related Documents](#)" sections "General information on IPsec and VPN" for a reference to configuring Authentication Proxy and "802.1x authentication" for a reference to configuring 802.1x authentication.)

The second option for entry of the Xauth username and password is not to store it on the router. Instead, a PC user who is connected to the router is presented with a special web page that allows the user to manually enter the username and password (see the section “[Manual Activation](#)”). The router sends the username and password to the central site concentrator, and if the username and password are correct, the tunnel comes up. The typical application for this configuration is a teleworker network. The teleworker wants to control when the tunnel is up and has to enter his or her personal user credentials (which could include one-time passwords) to activate the tunnel. Also, the network administrator may want teleworker tunnels up only when someone is using them to conserve resources on the central concentrators. (See the section “[Web-Based Activation](#)” for details about this configuration.)

The Xauth username and password can also be manually entered from the command-line interface (CLI) of the router. This method is not recommended for most situations because the user must first log in to the router (and needs a user ID on the router to do so). However, it can be useful for network administrators during troubleshooting.

Using Preshared Keys

Using preshared keys, each peer is aware of the key of the other peer. Preshared keys are displayed in running configurations, so they can be seen by anyone (referred to as clear format). When a more secure type of authentication is required, Cisco software also supports another type of preshared key: the encrypted preshared key.

Using an encrypted preshared key for authentication allows you to securely store plain-text passwords in type 6 (encrypted) format in NVRAM. A group preshared key can be preconfigured on both VPN-tunnel peers. The encrypted form of the keyword can be seen in the running configuration, but the actual keyword is not visible. (For more information about encrypted preshared keys, see [Encrypted Preshared Key](#).)

Using Digital Certificates

Digital certificates provide for the support of Rivest, Shamir, and Adelman (RSA) signatures on Easy VPN remote devices. The support is provided through a RSA certificate that can be stored on or off the remote device.



Note

The recommended timeout for Easy VPN using digital certificates is 40 seconds.

For more information about digital certificates, see the [Easy VPN Remote RSA Signature Support](#) feature guide, Release 12.3(7)T1.

Using Xauth

Xauth is an additional level of authentication that can be used. Xauth is applicable when either group preshared keys or digital certificates are used. Xauth credentials can be entered using a web interface manager, such as Security Device Manager (SDM), or using the CLI. (See the section “[Cisco Easy VPN Remote Web Managers](#).”)

The Save Password feature allows the Xauth username and password to be saved in the Easy VPN Remote configuration so that you are not required to enter the username and password manually. One-Time Passwords (OTPs) are not supported by the Save Password feature and must be entered manually when Xauth is requested. The Easy VPN server must be configured to “Allow Saved Passwords.” (For more information about how to configure the Save Password feature, see the section “[Dead Peer Detection Periodic Message Option](#).”)

Xauth is controlled by the Easy VPN server. When the Cisco IOS Easy VPN server requests Xauth authentication, the following messages are displayed on the console of the router:

```
EZVPN: Pending XAuth Request, Please enter the following command:
crypto ipsec client ezvpn xauth
```

When you see this message, you can provide the necessary user ID, password, and other information by entering the **crypto ipsec client ezvpn connect** command and responding to the prompts that follow.

The recommended Xauth timeout is 50 seconds or fewer.



Note

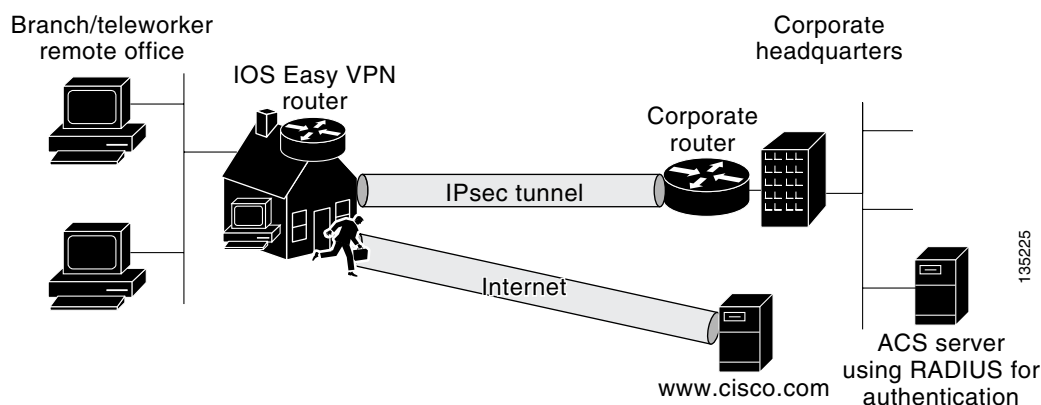
The timeout for entering the username and password is determined by the configuration of the Cisco IOS Easy VPN server. For servers running Cisco IOS software, this timeout value is specified by the **crypto isakmp xauth timeout** command.

Web-Based Activation

Web-Based Activation provides a user-friendly method for a remote teleworker to authenticate the VPN tunnel between his or her remote Easy VPN router and the central site router. This feature allows administrators to set up their remote LANs so that the initial HTTP request that is coming from any of the remote PCs is intercepted by the remote Easy VPN router. A login page is returned to the user, whereby the user may enter credentials to authenticate the VPN tunnel. After the VPN tunnel comes up, all users behind this remote site can access the corporate LAN without being reprompted for the username and password. Alternatively, the user may choose to bypass the VPN tunnel and connect only to the Internet, in which case a password is not required.

A typical application for web-based activation is a home teleworker who brings up the Easy VPN tunnel only when he or she needs to connect to the corporate LAN. If the remote teleworker is not present, other members of the household (such as a spouse or children) can use the Internet Only option to browse the Internet without activating the VPN tunnel. [Figure 4](#) shows a typical scenario for web-based activation.

Figure 4 Typical Web-Based Activation Scenario



Note

Entering the Xauth credentials brings up the tunnel for all users who are behind this remote site. After the tunnel is up, any additional PCs that are behind the remote site do not get prompted for Xauth credentials. Web-Based Activation is an authentication to bring up the VPN tunnel for all remote PCs and cannot be considered individual user authentication. Individual user authentication for VPN tunnel access is available using the Cisco IOS Authentication Proxy or 802.1x features, which can be

configured on the remote Easy VPN router. (See the “[Related Documents](#)” sections “General information on IPsec and VPN” for a reference to configuring Authentication Proxy and “802.1x authentication” for a reference to configuring 802.1x authentication.)

To configure web-based activation, see the section “[Configuring Web-Based Activation](#).”

The following sections show the various screen shots that a remote teleworker sees when the Web-Based Activation feature is turned on:

- [Web-Based Activation Portal Page, page 11](#)
- [VPN Authentication Bypass, page 12](#)
- [VPN Tunnel Authentication, page 13](#)
- [Successful Authentication, page 14](#)
- [Deactivation, page 15](#)

Web-Based Activation Portal Page

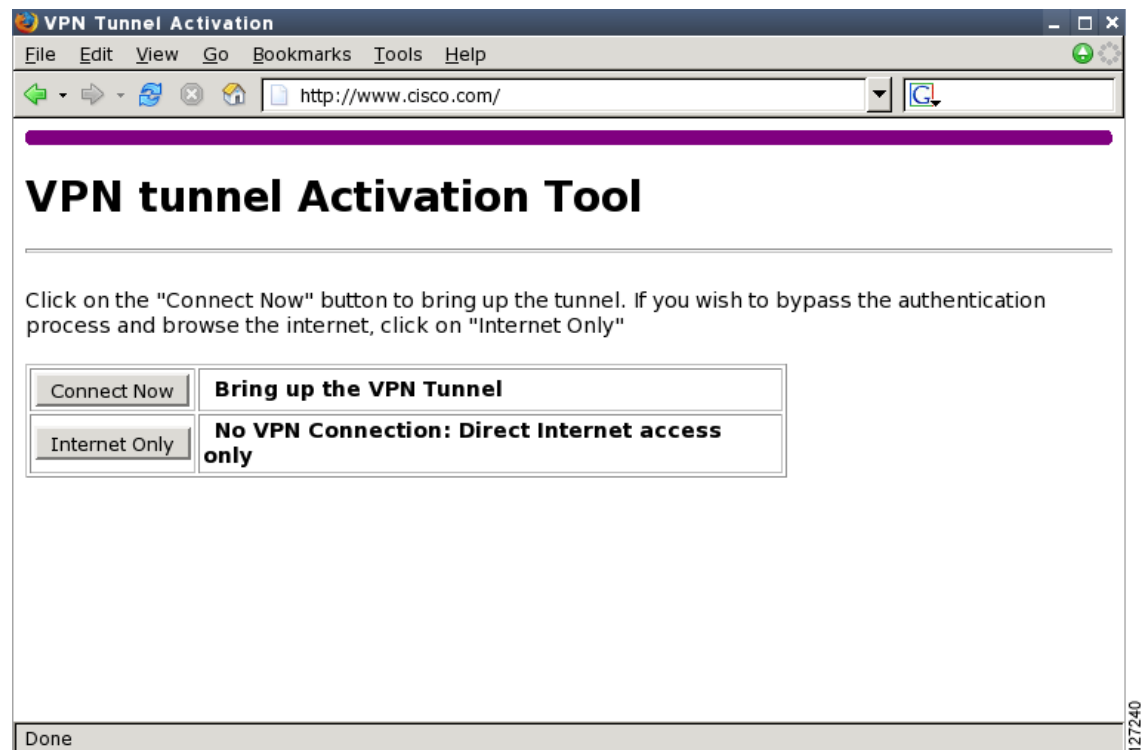
[Figure 5](#) is an example of a web-based activation portal page. The user may choose to connect to the corporate LAN by clicking Connect Now or he or she may choose to connect only to the Internet by clicking Internet Only.



Note

If the user chooses to connect only to the Internet, a password is not required.

Figure 5 *Portal Page*

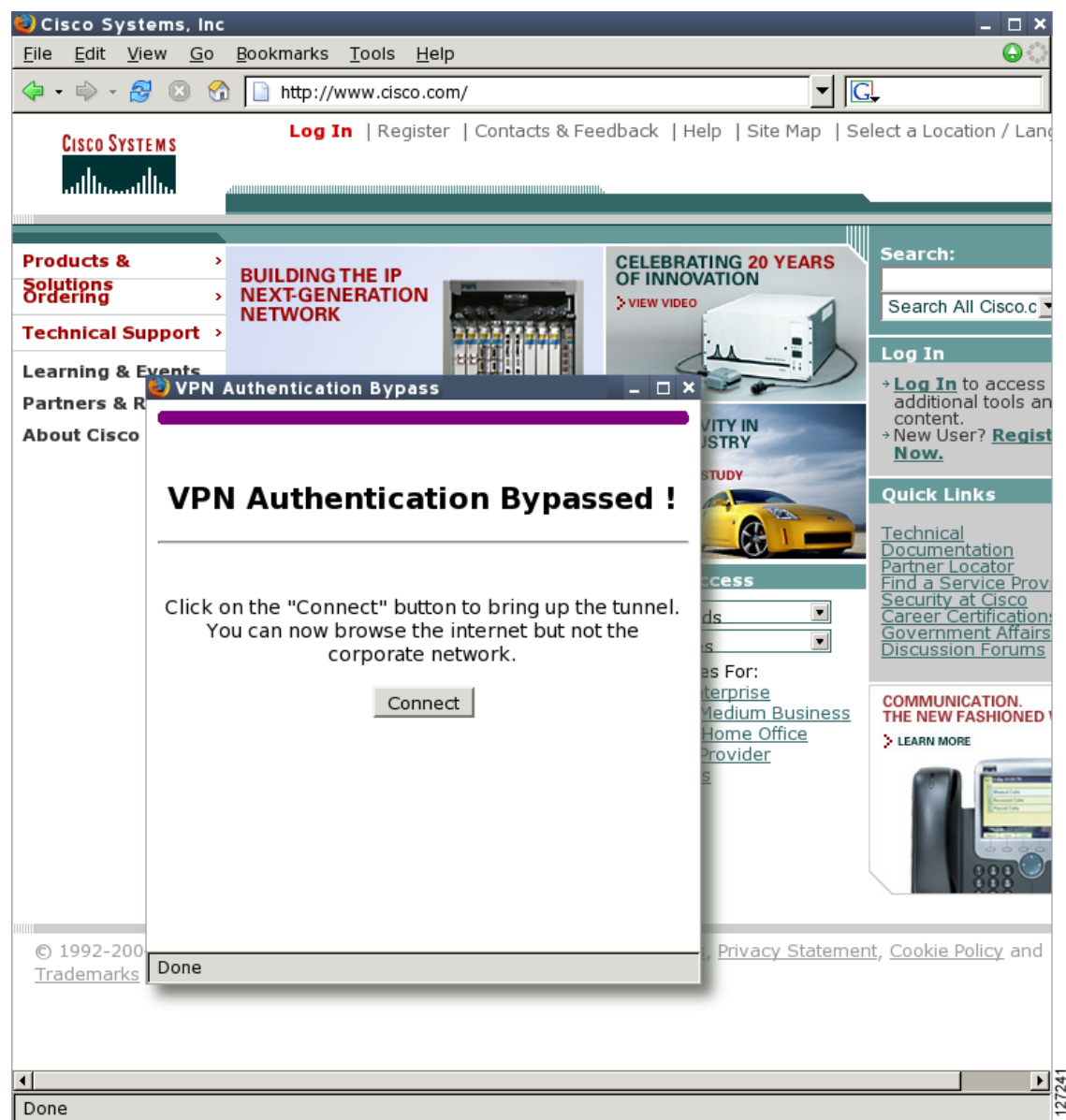


127240

VPN Authentication Bypass

Figure 6 is an example of a web-based activation in which the user chose to connect only to the Internet by clicking the Internet Only option. This option is most useful for household members who need to browse the Internet while the remote teleworker is not available to authenticate the VPN tunnel for corporate use.

Figure 6 VPN Authentication Bypass Page



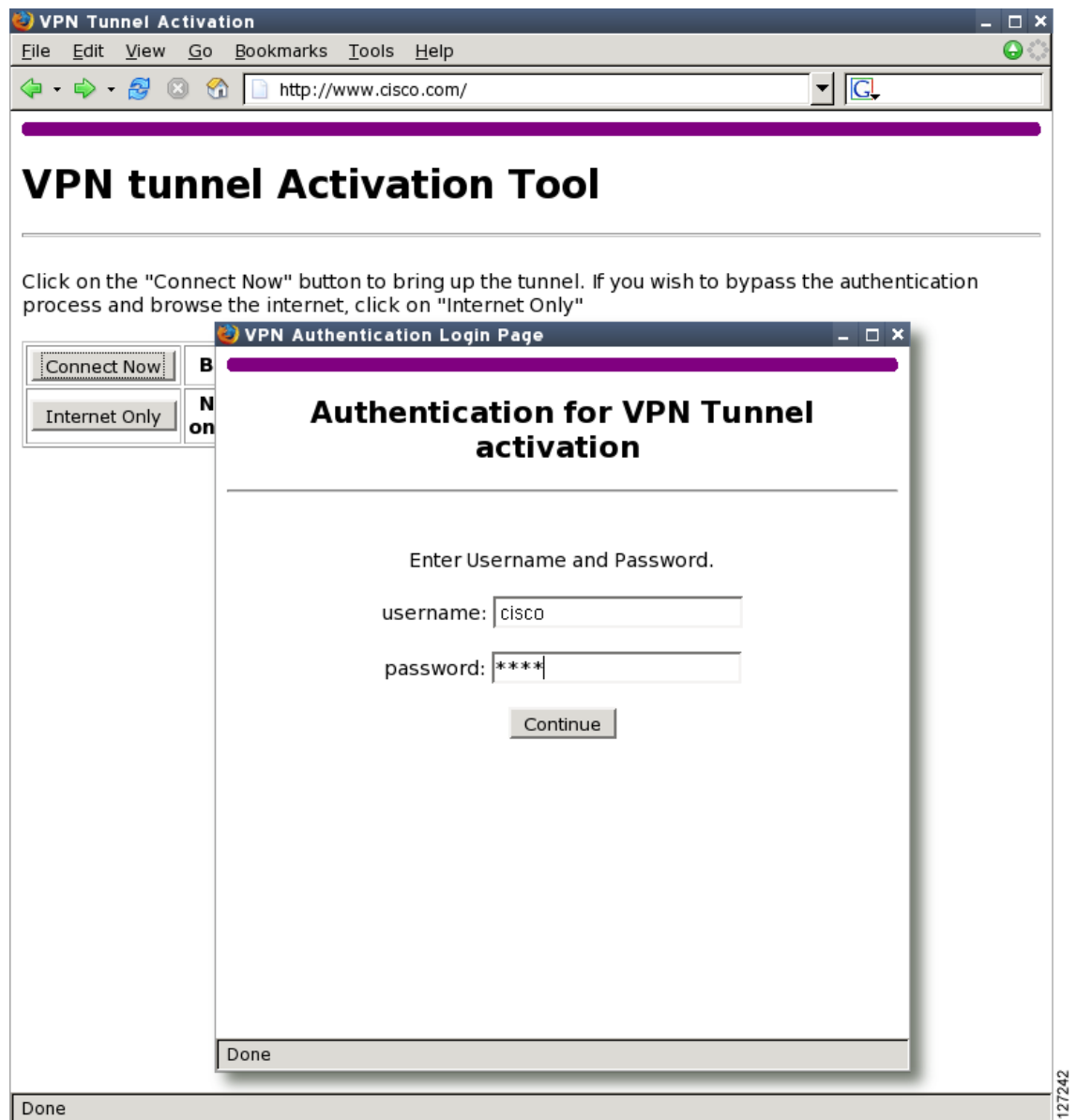
**Note**

If the Web-Based Activation window is mistakenly closed, to connect again, a user should follow this two-step process:

1. In a browser, type “http://routeripaddress/ezvpn/bypass” and try to connect to the URL. Entering this URL clears the bypass state that was created for your IP address (when the “Internet only” button was pressed). If you get a message saying that no such page is found, it does not matter because the only purpose of accessing the URL is to clear the bypass state.
2. After clearing the bypass state, you can browse to any external site. The Connect and Bypass page appears again. You can connect to VPN by pressing the Connect button.

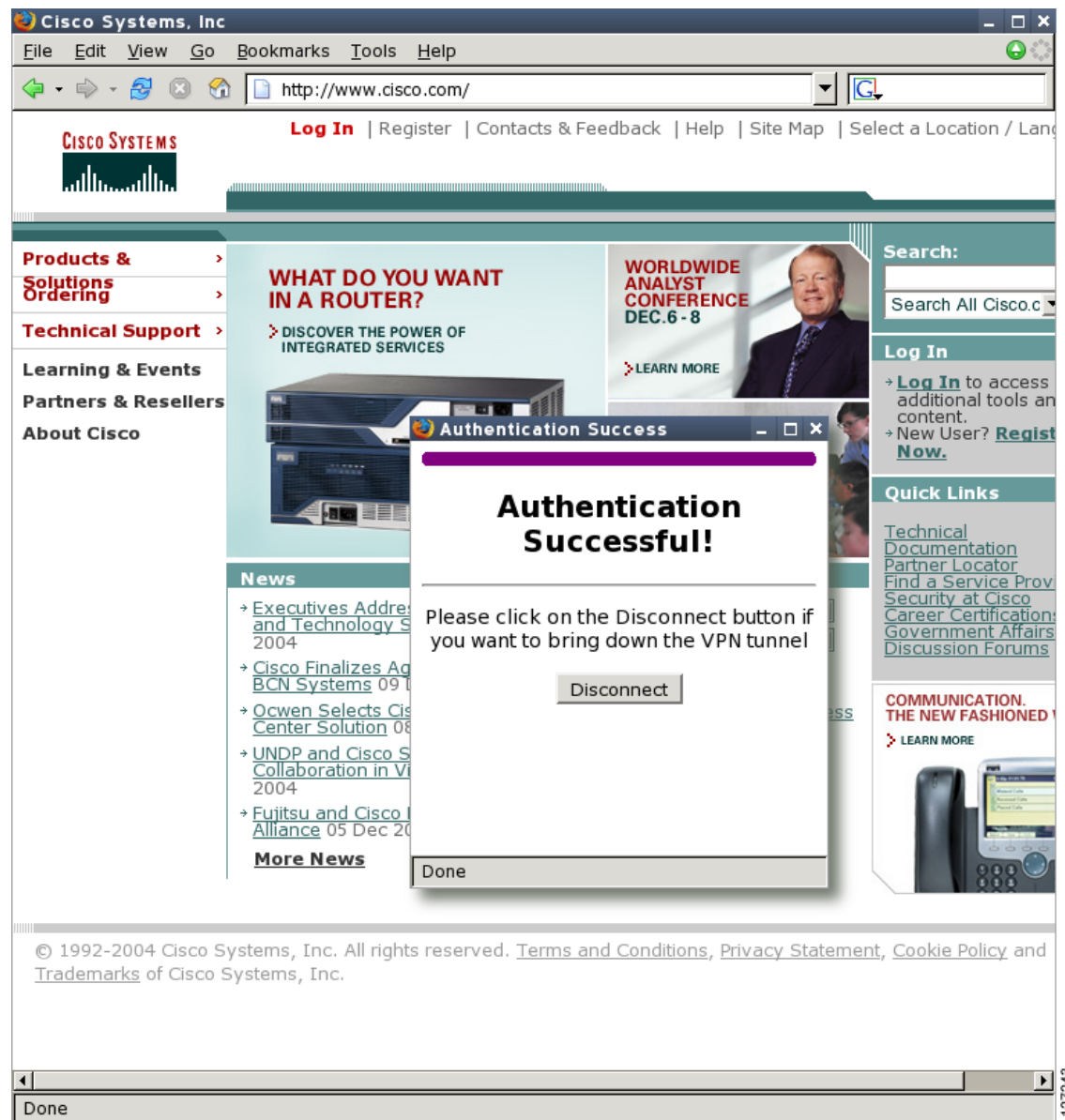
VPN Tunnel Authentication

[Figure 7](#) is an example of a web-based activation in which the user chose to connect to the corporate LAN by entering a username and password. After the user is successfully authenticated, the Easy VPN tunnel is brought up for this remote site. If there are multiple PCs behind this remote site, none of the additional users who are connecting to the corporate LAN will be requested for the Xauth credentials because the tunnel is already up.

Figure 7 VPN Tunnel Authentication

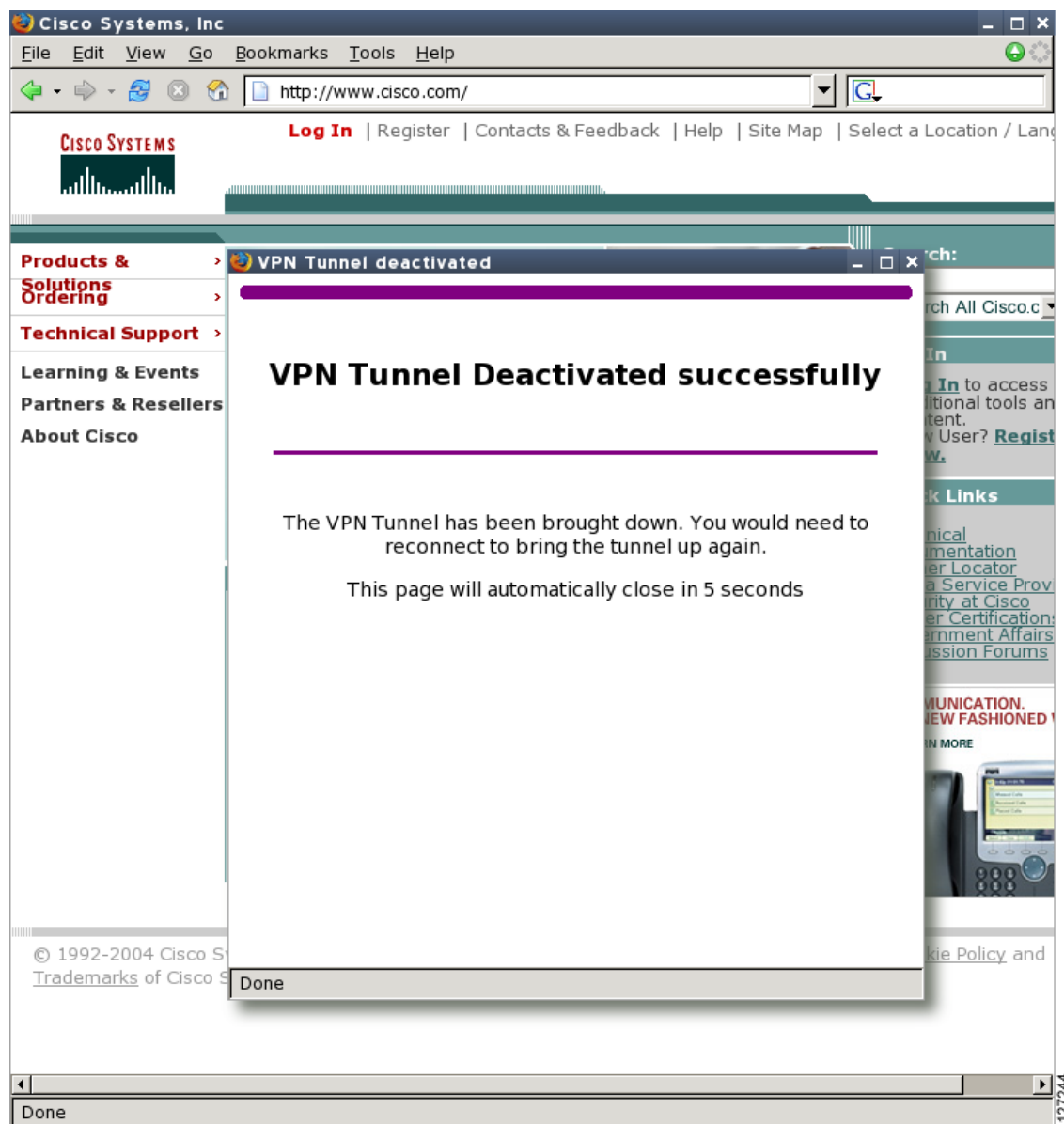
Successful Authentication

Figure 8 is an example of a successful activation. If the user chooses to deactivate the VPN tunnel, he or she should click the Disconnect button. After the IKE security association (SA) times out (the default value is 24 hours), the remote teleworker has to enter the Xauth credentials to bring up the tunnel.

Figure 8 Successful Activation

Deactivation

Figure 9 is an example of a VPN tunnel that has been deactivated successfully. The page automatically closes in 5 seconds.

Figure 9 *VPN Tunnel Deactivated Successfully*

802.1x Authentication

The 802.1x Authentication feature allows you to combine Easy VPN client mode operation with 802.1x authentication on Cisco IOS routers. For more information about this feature, see “802.1x Authentication” in the section “[Additional References](#).”

Tunnel Activation Options

There are three tunnel activation options:

- Automatic activation
- Manual activation
- Traffic-triggered activation (not available in Cisco IOS Release 12.3(11)T)

Tunnel connect and disconnect options are available with SDM.

Automatic Activation

The Cisco Easy VPN tunnel is automatically connected when the Cisco Easy VPN Remote feature is configured on an interface. If the tunnel times out or fails, the tunnel automatically reconnects and retries indefinitely.

To specify automatic tunnel control on a Cisco Easy VPN remote device, you need to configure the **crypto ipsec client ezvpn** command and then the **connect auto** subcommand. However, you do not need to use these two commands when you are creating a new Easy VPN remote configuration because the default is “automatic.”

To disconnect or reset a particular tunnel, you should use the **clear crypto ipsec client ezvpn** command, or you can use SDM.

Manual Activation

The Cisco Easy VPN Remote software implements manual control of the Cisco Easy VPN tunnels so that you can establish and terminate the tunnel on demand.

To specify manual tunnel control on a Cisco Easy VPN remote device, you need to input the **crypto ipsec client ezvpn** command and then the **connect manual** command.

The manual setting means that the Cisco Easy VPN remote will wait for a command before attempting to establish the Cisco Easy VPN Remote connection. When the tunnel times out or fails, subsequent connections will also have to wait for the command.

If the configuration is manual, the tunnel is connected only after you issue the command **crypto ipsec client ezvpn connect**.

To disconnect or reset a particular tunnel, you should use the **clear crypto ipsec client ezvpn** command, or you can use SDM.

See the “[Configuring Manual Tunnel Control](#)” section for specific information on how to configure manual control of a tunnel.

Traffic-Triggered Activation



Note

This feature is not available in Cisco IOS Release 12.3(11)T.

The Traffic-Triggered Activation feature is recommended for transactional-based VPN applications. It is also recommended for use with the Easy VPN dial backup feature for the backup Easy VPN configuration so that backup is activated only when there is traffic to send across the tunnel.

To use Access Control List (ACL) tunnel control, you must first describe the traffic that is considered “interesting.” For more information about ACLs, see the chapter “[Access Control Lists: Overview and Guidelines](#)” in the “Traffic Filtering and Firewalls” section of the *Cisco IOS Security Configuration Guide, Release 12.3*. To actually configure an ACL-triggered tunnel, use the **crypto ipsec client ezvpn** command with the **connect acl** subcommand.

Dead Peer Detection Stateless Failover Support

Two options are available for configuring Dead Peer Detection Stateless Failover Support:

- Backup Server List Local Configuration
- Backup Server List Auto Configuration

Backup Server List Local Configuration

Backup Server List Local Configuration allows users to enter multiple peer statements. With this feature configured, if the client is connecting to a peer and the negotiation fails, Easy VPN fails over to the next peer. This failover continues through the list of peers. When the last peer is reached, Easy VPN rolls over to the first peer. The IKE and IPsec SAs to the previous peer are deleted. Multiple peer statements work for both IP addresses as well as for hostnames. Setting or unsetting the peer statements will not affect the order of the peer statements.

To use this feature, use the **peer** subcommand of the **crypto ipsec client ezvpn** command.

Backup Server List Auto Configuration

Easy VPN remote that is based on Cisco IOS software can have up to 10 backup servers configured for redundancy. The Backup Server feature allows the Easy VPN server to “push” the backup server list to the Easy VPN remote.

The backup list allows the administrator to control the backup servers to which a specific Easy VPN remote will connect in case of failure, retransmissions, or dead peer detection (DPD) messages.

**Note**

Before the backup server feature can work, the backup server list has to be configured on the server.

How a Backup Server Works

If remote A goes to server A and the connection fails, remote A goes to server B. If server B has a backup list configured, that list will override the backup server list of server A. If the connection to server B fails, remote A will continue through the backup servers that have been configured.

**Note**

If you are in auto mode and you have a failure, you will transition automatically from server A to server B. However, if you are in manual mode, you have to configure the transition manually. To configure the transition manually, use the **crypto ipsec client ezvpn** command with the **connect** keyword.

No new configuration is required at the Easy VPN remote to enable this feature. If you want to display the current server, you can use the **show crypto ipsec client ezvpn** command. If you want to find out which peers were pushed by the Easy VPN server, you can use the same command.

To troubleshoot this feature, use the **debug crypto ipsec client ezvpn** command. If more information is needed for troubleshooting purposes, use the **debug crypto isakmp** command. The **show crypto ipsec client ezvpn** command may also be used for troubleshooting.

Cisco Easy VPN Remote Features

The Cisco Easy VPN Remote feature is a collection of features that improves the capabilities of the Cisco Easy VPN Remote feature introduced in Cisco IOS Release 12.2(4)YA. The Cisco Easy VPN Remote feature includes the following:

- [Default Inside Interface, page 20](#)—This feature supports the autoconfiguration of the default Easy VPN inside interface for Cisco 800 series routers.
- [Multiple Inside Interfaces, page 21](#)—This feature allows you to configure up to eight inside interfaces on the Cisco Easy VPN remote.
- [Multiple Outside Interfaces, page 21](#)—This feature allows you to configure up to four outside tunnels for outside interfaces.
- [VLAN Support, page 21](#)—This feature allows VLANs to be configured as valid Easy VPN inside interfaces.
- [Multiple Subnet Support, page 22](#)—This feature allows multiple subnets from the Easy VPN inside interface to be included in the Easy VPN tunnel.
- [NAT Interoperability Support, page 22](#)—This feature automatically restores the NAT configuration when the IPsec VPN tunnel is disconnected.
- [Local Address Support, page 22](#)—The Cisco Easy VPN Remote feature is enhanced to support an additional **local-address** attribute that specifies which interface is used to determine the IP address used to source the Easy VPN tunnel traffic.
- [Peer Hostname, page 23](#)—When a peer is defined as a hostname, the hostname is stored and the Domain Name System (DNS) lookup is done at the time of tunnel connection.
- [Proxy DNS Server Support, page 23](#)—This feature allows you to configure the router in a Cisco Easy VPN remote configuration to act as a proxy DNS server for LAN-connected users.
- [Cisco IOS Firewall Support, page 23](#)—This feature supports Cisco IOS Firewall configurations on all platforms.
- [Easy VPN Remote and Server on the Same Interface, page 23](#)—The Easy VPN remote and Easy VPN server are supported on the same interface, which makes it possible to establish a tunnel to another Easy VPN server and terminate the Easy VPN software client on the same interface simultaneously.
- [Easy VPN Remote and Site to Site on the Same Interface, page 23](#)—The Easy VPN Remote and site to site (crypto map) are supported on the same interface, which makes it possible to establish a tunnel to another Easy VPN server and have another site to site on the same interface simultaneously.
- [Cisco Easy VPN Remote Web Managers, page 24](#)—Users can manage the Cisco Easy VPN Remote feature on the Cisco uBR905 and Cisco uBR925 cable access routers using a built-in web interface.
- [Dead Peer Detection Periodic Message Option, page 24](#)—This feature allows you to configure your router to query the liveliness of its IKE peer at regular intervals.
- [Load Balancing, page 24](#)—If a remote device is loaded and unable to accept more traffic, the VPN 3000 will send a notify message that contains an IP address that represents the new IKE server to which the remote should connect.

- [Management Enhancements, page 25](#)—This feature allows for remote management of the VPN remote.
- [PFS Support, page 25](#)—The PFS configuration mode attribute is sent by the server if requested by the VPN remote device.
- [Dial Backup, page 25](#)—This feature allows you to configure a dial backup tunnel connection on your remote device.
- [Virtual IPsec Interface Support, page 27](#)—This feature allows you to selectively send traffic to different Easy VPN concentrators as well as to the Internet (includes a reference to the IPsec Virtual Tunnel Interface feature.)
- [Dual Tunnel Support, page 29](#)—This feature allows you to configure multiple Easy VPN tunnels that share common inside and outside interfaces to connect two peers to two different VPN servers simultaneously.
- [Banner, page 32](#)—The EasyVPN remote device can download a banner that has been pushed by the Easy VPN server. The banner can be used for Xauth and web-based activation. The banner is displayed when the Easy VPN tunnel is “up” on the Easy VPN remote console or as an HTML page in the case of web-based activation.
- [Configuration Management Enhancements \(Pushing a Configuration URL Through a Mode-Configuration Exchange\), page 33](#)—The Easy VPN remote device can download a URL that is pushed by the Easy VPN server, allowing the Easy VPN remote device to download configuration content and apply it to the running configuration.
- [Reactivate Primary Peer, page 33](#)—This feature allows you to designate a primary peer. When an Easy VPN device fails over from the primary peer to a backup peer and the primary peer is again available, connections with the backup peer are torn down and a connection is made with the primary peer.
- [Identical Addressing Support, page 33](#)—This feature integrates Network Address Translation (NAT) with Easy VPN to allow remotes with overlapping internal IP addressing to connect to the Easy VPN server.
- [cTCP Support on Easy VPN Clients, page 34](#)—When cTCP is enabled on a remote device (client) and headend device, IKE and ESP (Protocol 50) traffic is encapsulated in the TCP header so that the firewalls in between the client and the headend device permit this traffic (considering it the same as TCP traffic).

Default Inside Interface

Easy VPN Remote supports the autoconfiguration of the default Easy VPN inside interface for Cisco 800 series routers. The interface Ethernet 0 is the default inside interface.

If you want to disable the default inside interface and configure another inside interface on the Cisco 800 series router, you must configure the other inside interface first and then disable the default inside interface. You can use the following command to disable the default inside interface:

```
no crypto ipsec client ezvpn name inside
```

If you did not configure the other inside interface first before disabling the default inside interface, you will receive a message such as the following (see lines three and four):

```
Router (config)# interface ethernet0
Router (config-if)# no crypto ipsec client ezvpn hw-client inside
Cannot remove the single inside interface unless
one other inside interface is configured
```

Multiple Inside Interfaces

Inside interface support is enhanced in the Cisco Easy VPN Remote feature to support multiple inside interfaces for all platforms. Inside interfaces can be configured manually with the enhanced command and subcommand:

```
interface interface-name
  crypto ipsec client ezvpn name [outside | inside]
```

See the “[Configuring Multiple Inside Interfaces](#)” section for information on how to configure more than one inside interface.

Multiple inside interfaces offer the following capabilities:

- Up to eight inside interfaces are supported on the Cisco 800 and Cisco 1700 series routers.
- At least one inside interface must be configured for each outside interface; otherwise, the Cisco Easy VPN Remote feature does not establish a connection.
- Adding a new inside interface or removing an existing inside interface automatically resets the Cisco Easy VPN Remote connection (the currently established tunnel). You must reconnect a manually configured tunnel, and if Xauth is required by the Cisco Easy VPN server, the user is reprompted. If you have set the Cisco Easy VPN Remote configuration to connect automatically and no Xauth is required, no user input is required.
- Inside interfaces that are configured or the default setting can be shown by using the **show crypto ipsec client ezvpn** command.

Multiple Outside Interfaces

The Easy VPN Remote feature supports one Easy VPN tunnel per outside interface. You can configure up to four Easy VPN tunnels per Cisco router. Each Easy VPN tunnel can have multiple inside interfaces configured, but they cannot overlap with another Easy VPN tunnel unless dial backup is configured. For more information about dial backup, see the section “[Dial Backup](#).” To configure multiple outside interfaces, use the **crypto ipsec client ezvpn** command and **outside** keyword.

To disconnect or clear a specific tunnel, the **clear crypto ipsec client ezvpn** command specifies the IPsec VPN tunnel name. If there is no tunnel name specified, all existing tunnels are cleared.

See the “[Configuring Multiple Outside Interfaces](#)” section for more information on configuring more than one outside interface.

VLAN Support

Inside interface support on VLANs makes it possible to have valid Easy VPN inside interface support on a VLAN, which was not possible before Cisco IOS Release 12.3(7)XR. With this feature, SAs can be established at connection using the VLAN subnet address or mask as a source proxy.

For the inside interface support on VLANs to work, you must define each VLAN as an Easy VPN inside interface. In addition, IPsec SAs should be established for each inside interface in the same manner as for other inside interfaces. For more information about inside and outside interfaces, see the sections “[Multiple Inside Interfaces](#)” and “[Multiple Outside Interfaces](#).”

Inside interface support on VLANs is supported only on Cisco routers that support VLANs.

Multiple Subnet Support

For situations in which you have multiple subnets connected to an Easy VPN inside interface, you can optionally include these subnets in the Easy VPN tunnel. First, you must specify the subnets that should be included by defining them in an ACL. To configure an ACL, see “Access control lists, configuring” in the “[Additional References](#)” section. Next, you have to use the **acl** subcommand of the **crypto ipsec client ezvpn** (global) command to link your ACL to the Easy VPN configuration. Easy VPN Remote will automatically create the IPsec SAs for each subnet that is defined in the ACL as well as for the subnets that are defined on the Easy VPN inside interface.

**Note**

Multiple subnet support is not supported in client mode.

NAT Interoperability Support

Cisco Easy VPN Remote supports interoperability with NAT. You can have a NAT configuration and a Cisco Easy VPN Remote configuration that coexist. When an IPsec VPN tunnel is down, the NAT configuration works.

In the Cisco Easy VPN Remote feature, the router automatically restores the previous NAT configuration when the IPsec VPN tunnel is torn down. The user-defined access lists are not disturbed. Users can continue to access nontunnel areas of the Internet when the tunnel times out or disconnects.

**Note**

NAT interoperability is not supported in client mode with split tunneling.

Local Address Support

The Cisco Easy VPN Remote feature is enhanced to support an additional **local-address** attribute. This attribute specifies which interface is used to determine the IP address that is used to source the Easy VPN Remote tunnel traffic. After specifying the interface with the **local-address** subcommand, you can manually assign a static IP address to the interface or use the **cable-modem dhcp-proxy interface** command to automatically configure the specified interface with a public IP address. See the “[Configuring Proxy DNS Server Support](#)” section for configuration information.

Local Address Support is available for all platforms, but it is more applicable to the Cisco uBR905 and Cisco uBR925 cable access routers in conjunction with the **cable-modem dhcp-proxy interface** command. Typically, the loopback interface is the interface used to source tunnel traffic for the Cisco uBR905 and Cisco uBR925 cable access routers.

In a typical DOCSIS network, the Cisco uBR905 and Cisco uBR925 cable access routers are normally configured with a private IP address on the cable modem interface. In the initial Cisco Easy VPN Remote feature, a public IP address was required on the cable modem interface to support the Easy VPN remote.

In the Cisco Easy VPN Remote feature, cable providers can use the Cable DHCP Proxy feature to obtain a public IP address and assign it to the cable modem interface, which is usually the loopback interface.

For more information on the **cable-modem dhcp-proxy interface** command, see the “[Cable CPE Commands](#)” chapter in the *Cisco Broadband Cable Command Reference Guide*.

**Note**

The **cable-modem dhcp-proxy interface** command is supported only for the Cisco uBR905 and Cisco uBR925 cable access routers.

Peer Hostname

The peer in a Cisco Easy VPN Remote configuration can be defined as an IP address or a hostname. Typically, when a peer is defined as a hostname, a DNS lookup is done immediately to get an IP address. In the Cisco Easy VPN Remote feature, the peer hostname operation is enhanced to support DNS entry changes. The text string of the hostname is stored so that the DNS lookup is done at the time of the tunnel connection, not when the peer is defined as a hostname.

See the “[Configuring and Assigning the Easy VPN Remote Configuration](#)” section for information on enabling the peer hostname functionality.

Proxy DNS Server Support

When the Easy VPN tunnel is down, the DNS addresses of the ISP or cable provider should be used to resolve DNS requests. When the WAN connection is up, the DNS addresses of the enterprise should be used.

As a way of implementing use of the DNS addresses of the cable provider when the WAN connection is down, the router in a Cisco Easy VPN Remote configuration can be configured to act as a proxy DNS server. The router, acting as a proxy DNS server for LAN-connected users, receives DNS queries from local users on behalf of the real DNS server. The DHCP server then can send out the LAN address of the router as the IP address of the DNS server. After the WAN connection comes up, the router forwards the DNS queries to the real DNS server and caches the DNS query records.

See the “[Configuring Proxy DNS Server Support](#)” section for information on enabling the proxy DNS server functionality.

Cisco IOS Firewall Support

The Cisco Easy VPN Remote feature works in conjunction with Cisco IOS Firewall configurations on all platforms.

Easy VPN Remote and Server on the Same Interface

This feature allows the Easy VPN remote and Easy VPN server to be supported on the same interface, making it possible to both establish a tunnel to another Easy VPN server and terminate the Easy VPN software client on the same interface simultaneously. A typical application would be a geographically remote location for which Easy VPN Remote is being used to connect to a corporate Easy VPN server and also to terminate local software client users.

For more information about the Easy VPN Remote and Server on the Same Interface feature, see “Easy VPN Remote and Server on the Same Interface” in the section “[Additional References](#).”

Easy VPN Remote and Site to Site on the Same Interface

This feature allows the Easy VPN remote and site to site (crypto map) to be supported on the same interface, making it possible to both establish a tunnel to another Easy VPN server and have another site to site on the same interface simultaneously. A typical application would be a third-party VPN service provider that is managing a remote router via the site-to-site tunnel and using Easy VPN Remote to connect the remote site to a corporate Easy VPN server.

For more information about the Easy VPN Remote and Site to Site on the Same Interface feature, see “Easy VPN Remote and Site to Site on the Same Interface” in the section “[Additional References](#).”

Cisco Easy VPN Remote Web Managers

Web interface managers may be used to manage the Cisco Easy VPN Remote feature. One such web interface manager is SDM, which is supported on the Cisco 830 series, Cisco 1700 series, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. SDM enables you to connect or disconnect the tunnel and provides a web interface for Xauth. For more information about SDM, see [Cisco Security Device Manager](#).

A second web interface manager is the Cisco Router Web Setup (CRWS) tool, which is supported on the Cisco 806 router. The CRWS provides a similar web interface as SDM.

A third web interface manager, Cisco Easy VPN Remote Web Manager, is used to manage the Cisco Easy VPN Remote feature for Cisco uBR905 and Cisco uBR925 cable access routers. You do not need access to the CLI to manage the Cisco Easy VPN remote connection.

The web interface managers allow you to do the following:

- See the current status of the Cisco Easy VPN remote tunnel.
- Connect a tunnel that is configured for manual control.
- Disconnect a tunnel that is configured for manual control or reset a tunnel configured for automatic connection.
- Be prompted for Xauth information, if needed.

See the [“Troubleshooting the VPN Connection”](#) section for more information about Cisco Easy VPN Remote Web Manager.

Dead Peer Detection Periodic Message Option

The dead peer detection periodic message option allows you to configure your router to query the liveness of its IKE peer at regular intervals. The benefit of this approach over the default approach (on-demand dead peer detection) is earlier detection of dead peers. For more information about the dead peer detection periodic message option, see *“Dead peer detection”* in the section [“Additional References.”](#)

Load Balancing

When the Cisco VPN 3000 concentrator is configured for load balancing, the VPN 3000 will accept an incoming IKE request from the VPN remote on its virtual IP address. If the device is loaded and unable to accept more traffic, the VPN 3000 will send a notify message that contains an IP address that represents the new IKE server to which the remote should connect. The old connection will be torn down and a new connection established to the redirected VPN gateway.

There is no configuration required for load balancing to occur. If the VPN gateway is configured for load balancing, and it notifies the VPN remote that it is performing load balancing, the VPN remote has access to the load balancing feature.

To verify whether load balancing is occurring, use the **debug crypto isakmp**, **debug crypto ipsec client ezvpn**, and **show crypto ipsec** commands. To troubleshoot the load balancing process, use the **show crypto ipsec** command.

Management Enhancements

Management enhancements for Easy VPN remotes allow for the remote management of the VPN remote. The feature provides for the IPv4 address to be pushed by configuration mode to the VPN remote. The IPv4 address is assigned to the first available loopback interface on the VPN remote, and any existing statically defined loopbacks are not overridden. On disconnect, the address and loopback interface are removed from the list of active interfaces.

After the VPN remote is connected, the loopback interface should be accessible from the remote end of the tunnel. All PAT activities will be translated through this interface IP address.

If a loopback exists, and an IP address is associated with it and its state is unassigned, the interface is a good candidate for mode configuration address management.



Note

After you assign an address to the loopback interface, if you save the configuration to NVRAM and reboot the VPN remote, the configuration address is permanently contained in the configuration. If you saved the configuration to NVRAM and rebooted the VPN remote, you must enter configuration mode and remove the IP address from the loopback interface manually.

You can use the **show ip interface** command with the **brief** keyword to verify that a loopback has been removed. The output of this **show** command also displays the interface.

PFS Support

The PFS configuration mode attribute is sent by the server if requested by the VPN remote device. If any subsequent connection by the remote device shows that PFS is not received by the remote, PFS will not be sent in IPsec proposal suites.



Note

The PFS group that will be proposed in the IPsec proposal suites is the same as the group used for IKE.

You can use the **show crypto ipsec client ezvpn** command to display the PFS group and to verify that you are using PFS.

Dial Backup

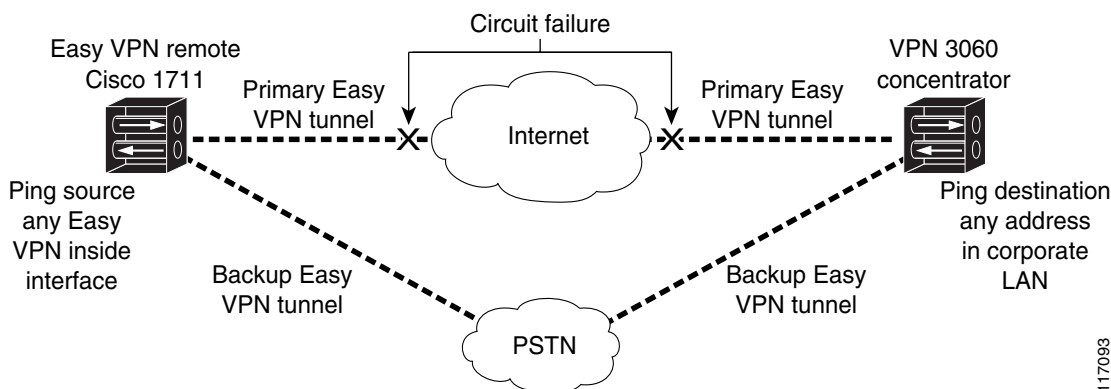


Note

The Dial Backup feature is not available in Cisco IOS Release 12.3(11)T.

Dial backup for Easy VPN remotes allows you to configure a dial backup tunnel connection on your remote device. The backup feature is “brought up” only when real data has to be sent, eliminating the need for expensive dialup or ISDN links that must be created and maintained even when there is no traffic.

[Figure 10](#) illustrates a typical Easy VPN remote-with-dial-backup scenario. In this scenario, a Cisco 1751 remote device is attempting to connect to another Cisco 1751 (acting as a server). There is a failure in the primary Easy VPN tunnel, and the connection is rerouted through the Easy VPN backup tunnel to the Cisco 1751 server.

Figure 10 *Dial Backup for Easy VPN Scenario*

Dial Backup Using a Dial-on-Demand Solution

IP static route tracking enable Cisco IOS software to identify when a Point-to-Point Protocol over Ethernet (PPPoE) or IPsec VPN tunnel “goes down” and initiates a Dial-on-Demand (DDR) connection to a preconfigured destination from any alternative WAN or LAN port (for example, a T1, ISDN, analog, or auxiliary port). The failure may be caused by several catastrophic events (for example, by Internet circuit failures or peer device failure). The remote route has only a static route to the corporate network. The IP static-route-tracking feature allows an object to be tracked (using an IP address or hostname) using Internet Control Message Protocol (ICMP), TCP, or other protocols, and it installs or removes the static route on the basis of the state of the tracked object. If the tracking feature determines that Internet connectivity is lost, the default route for the primary interface is removed, and the floating static route for the backup interface is enabled.

Dial Backup Using Object Tracking

IP static route tracking must be configured for dial backup on an Easy VPN remote device to work. The object tracking configuration is independent of the Easy VPN remote dial backup configuration. (For more information about object tracking, see the feature guide [Reliable Static Routing Backup Using Object Tracking](#).)

Easy VPN Remote Dial Backup Support Configuration

You can configure dial backup for your Easy VPN remote using two Easy VPN remote options that allow a connection to the backup Easy VPN configuration and a connection to the tracking system.

- To specify the Easy VPN configuration that will be activated when backup is triggered, use the **backup** subcommand of the **crypto ipsec client ezvpn** (global) command.
- The Easy VPN remote device registers to the tracking system to get the notifications for change in the state of the object. Use the **track** subcommand to inform the tracking process that the Easy VPN remote device is interested in tracking an object, which is identified by the object number. The tracking process, in turn, informs the Easy VPN remote device when the state of this object changes. This notification prompts the Easy VPN remote device when the state of this object changes. This notification prompts the Easy VPN remote device to bring up the backup connection when the tracked object state is DOWN. When the tracked object is UP again, the backup connection is torn down and the Easy VPN remote device will switch back to using the primary connection.

**Note**

Only one backup configuration is supported for each primary Easy VPN configuration. Each inside interface must specify the primary and backup Easy VPN configuration.

Dynamically Addressed Environments

To allow dial backup to be deployed in dynamically addressed environments, use the IP SLA Pre-Routed ICMP Echo Probe feature. (For more information about this feature, see [Cisco 1700 Series- Cisco IOS Release 12.3\(7\)XR](#) release notes. To use the IP SLA Pre-Routed ICMP Echo Probe feature, use the **icmp-echo** command with the **source-interface** keyword.

Dial Backup Examples

For examples of dial backup configurations, see the section “[Dial Backup: Examples](#).”

Virtual IPsec Interface Support

The Virtual IPsec Interface Support feature provides a routable interface to selectively send traffic to different Easy VPN concentrators as well as to the Internet.

Before Cisco IOS Release 12.4(4)T, at the tunnel-up/tunnel-down transition, attributes that were pushed during the mode configuration had to be parsed and applied. When such attributes resulted in the configurations being applied on the interface, the existing configuration had to be overridden. With the Virtual IPsec Interface Support feature, the tunnel-up configuration can be applied to separate interfaces, making it easier to support separate features at tunnel-up time. Features that are applied to the traffic going into the tunnel can be separate from the features that are applied to traffic that is not going through the tunnel (for example, split-tunnel traffic and traffic leaving the device when the tunnel is not up). When the Easy VPN negotiation is successful, the line protocol state of the virtual-access interface gets changed to up. When the Easy VPN tunnel goes down because the security association (SA) expires or is deleted, the line protocol state of the virtual-access interfaces changes to down.

Routes act as traffic selectors in an Easy VPN virtual interface, that is, the routes replace the access list on the crypto map. In a virtual-interface configuration, Easy VPN negotiates a single IPsec SA if the Easy VPN server has been configured with a dynamic virtual IPsec interface. This single SA is created irrespective of the Easy VPN mode that is configured.

After the SA is established, routes that point to the virtual-access interface are added to direct traffic to the corporate network. Easy VPN also adds a route to the VPN concentrator so that IPsec-encapsulated packets get routed to the corporate network. A default route that points to the virtual-access interface is added in the case of a nonsplit mode. When the Easy VPN server “pushes” the split tunnel, the split tunnel subnet becomes the destination to which the routes that point to the virtual access are added. In either case, if the peer (VPN concentrator) is not directly connected, Easy VPN adds a route to the peer.

**Note**

- Most routers that run the Cisco Easy VPN Client software have a default route configured. The default route that is configured should have a metric value greater than 1. The metric value must be greater than 1 because Easy VPN adds a default route that has a metric value of 1. The route points to the virtual-access interface so that all traffic is directed to the corporate network when the concentrator does not “push” the split tunnel attribute.

For more information about the IPsec Virtual Tunnel Interface feature, see the document *IPSec Virtual Tunnel Interface* (URL link provided in the “[Related Documents](#)” section of this document [General Information on IPsec and VPN]).

[Table 1](#) presents the different methods of configuring a remote device and the corresponding headend IPsec aggregator configurations. Each row represents a way to configure a remote device. The third column shows the different headend configurations that can be used with IPsec interfaces. See [Table 2](#) for a description of terms that are used in [Table 1](#) and [Table 3](#).

Table 1 **How Different Remote Device Configurations Interact with Various Headends and Configurations**

Remote Device Configurations	IOS Headend – Using Crypto Maps	IOS Headend – Using IPsec Interfaces	VPN3000/ASA
Crypto maps	<ul style="list-style-type: none"> Supported. 	—	—
Easy VPN virtual interface	<ul style="list-style-type: none"> Supported. Will create multiple SAs for a split tunnel. Because there is no interface on the headend, interface features cannot be supported. Limited quality of service (QoS) is supported. 	<ul style="list-style-type: none"> Supported. Creates only a single SA in split and no-split tunnels. Route injection is accomplished on the server. Routes are injected on the remote devices to direct traffic to the interface. 	<ul style="list-style-type: none"> Supported. Will create multiple SAs for a split tunnel.
Legacy Easy VPN	<ul style="list-style-type: none"> Creates a single IPsec SA on the headend when a default policy is pushed. Creates multiple SAs when a split-tunnel policy is pushed to the remote device. 	<ul style="list-style-type: none"> Not supported. Cannot be used with split tunnels because the headend interface does not support multiple SAs on a single interface. 	<ul style="list-style-type: none"> Supported. Creates multiple SAs for split tunnels.
Static virtual interface	<ul style="list-style-type: none"> Not supported. 	<ul style="list-style-type: none"> Supported. Can be used with a static interface or dynamic interface on the headend. Routing support is mandatory to reach the network. 	<ul style="list-style-type: none"> Not supported.

[Table 2](#) provides a description of the terms used in [Table 1](#) and [Table 3](#).

Table 2 **Terms Used in [Table 1](#) and [Table 3](#)**

Terms	Description
ASA	Cisco Adaptive Security Appliance, a threat-management security appliance.
Crypto maps	Commonly used for configuring IPsec tunnels. The crypto map is attached to an interface. For more information on crypto maps, see the section “Creating Crypto Map Sets” of the “Configuring Security for VPNs with IPsec” chapter of the <i>Cisco IOS Security Configuration Guide</i> . (URL link provided in the “ Related Documents ” section of this document.)
Easy VPN dual tunnel remote device	Two Easy VPN remote device configurations in which both are using a dynamic IPsec virtual tunnel interface.
Easy VPN virtual interface remote device (Easy VPN virtual interface)	Easy VPN remote configuration that configures the usage of a dynamic IPsec virtual tunnel interface.
IPsec interface	Consists of static and dynamic IPsec virtual interfaces.
IPsec Virtual Tunnel Interface	Tunnel interface that is created from a virtual template tunnel interface using mode IPsec. For more information on virtual tunnel interface configurations, see the document <i>IPSec Virtual Tunnel Interface</i> (URL link provided in the “ Related Documents ” section of this document [General Information on IPsec and VPN]).
Legacy Easy VPN	Easy VPN remote device configuration that uses crypto maps and does not use IPsec interfaces.
Static IPsec virtual tunnel interface (static virtual tunnel interface)	Tunnel interface used with mode IPsec that proposes and accepts only an “ipv4 any any” selector. For more information on static virtual tunnel interface configurations, see the document <i>IPSec Virtual Tunnel Interface</i> (URL link provided in the “ Related Documents ” section of this document [General Information on IPsec and VPN]).
VPN 3000	Cisco VPN 3000 series routers.

Dual Tunnel Support

Easy VPN now supports the ability to configure two easy VPN tunnels that have the same inside and outside interfaces. The feature is called the Easy VPN Dual Tunnel. Configuring multiple tunnels on a single remote device can be accomplished in a number of ways, which are listed below in [Table 3](#) along with their configuration and usage considerations. Further discussion in this section refers to only one such method of configuring dual tunnels using Easy VPN tunnels that have virtual interfaces. This method will be referred to as Dual Tunnel Support.

In a dual-tunnel Easy VPN setup, each Easy VPN tunnel is configured using virtual IPsec interface support, as shown in the section “[Virtual IPsec Interface Support](#).” Each Easy VPN tunnel has its unique virtual interface, which is created when the Easy VPN configuration is complete.

There are two possible combinations in which the dual tunnels can be used.

- Dual Easy VPN tunnels that have one tunnel using a nonsplit tunnel policy and the other tunnel using a split tunnel policy that has been pushed from the respective headend.

- Dual Easy VPN tunnel in which both tunnels are using an independent split tunnel policy that has been pushed from the respective headend.

**Note**

It is not permitted to have dual Easy VPN tunnels in which both tunnels are using a nonsplit tunnel policy.

The Easy VPN dual tunnel makes use of route injections to direct the appropriate traffic through the correct Easy VPN virtual tunnel interface. When the Easy VPN tunnel on the remote device “comes up,” it “learns” the split or nonsplit policy from the headend. The Easy VPN remote device injects routes in its routing table that correspond to the nonsplit networks that have been learned. If the headend pushes a nonsplit tunnel policy to the Easy VPN remote device, the Easy VPN remote device installs a default route in its routing table that directs all traffic out of the Easy VPN virtual interface that corresponds to this Easy VPN tunnel. If the headend pushes split-tunnel networks to the remote device, the remote device installs specific routes to the split networks in its routing table, directing the traffic to these networks out of the virtual tunnel interface.

**Note**

Dual Tunnel Easy VPN uses destination-based routing to send traffic to the respective tunnels.

Output features can be applied to this virtual interface. Examples of such output features are Cisco IOS Quality of Service and Cisco IOS Firewall. These features must be configured on the virtual template that is configured in the Easy VPN client configuration.

[Table 3](#) explains how this feature should be used. See [Table 2](#) for a description of terms that are used in [Table 1](#) and [Table 3](#).

Table 3 **Dual Tunnel Usage Guidelines**

Dual Tunnel Combinations	Headends Supported	Configuration and Usage Considerations on the Easy VPN Remote Device and Headend
Two legacy Easy VPN tunnels	IOS, ASA, and VPN 3000	<ul style="list-style-type: none"> Two tunnels cannot share a common outside interface. Two tunnels cannot share a common inside interface. The two tunnels should use separate inside and outside interfaces. Traffic from an inside interface that belongs to one Easy VPN tunnel cannot be pushed into another tunnel.
One legacy Easy VPN tunnel and one crypto map	IOS, ASA, and VPN 3000	The crypto map can share the same outside interface as the legacy Easy VPN client configuration. However, the behavior of the two remote devices depends on the mode of Easy VPN as well as the IPsec selectors of the crypto map and the Easy VPN remote device. This is not a recommended combination.
One legacy Easy VPN tunnel and one static virtual interface	IOS	Both tunnels cannot terminate on the same headend. The static virtual interface remote device tunnel has to be terminated on a static virtual interface on the headend router. The legacy Easy VPN remote device tunnel can terminate on the virtual tunnel interface or crypto map that is configured on the headend.

Table 3 *Dual Tunnel Usage Guidelines (continued)*

Dual Tunnel Combinations	Headends Supported	Configuration and Usage Considerations on the Easy VPN Remote Device and Headend
One legacy Easy VPN tunnel and one Easy VPN virtual interface	IOS, ASA, and VPN 3000	<ul style="list-style-type: none"> Both tunnels cannot terminate on the same headend. The legacy Easy VPN tunnel and the Easy VPN virtual interface can share a common inside and outside interface. An Easy VPN virtual interface should be used only with split tunneling. Legacy Easy VPN can use a split tunnel or no split tunnel. The Web-Based Activation feature cannot be applied on both Easy VPN tunnels. Using two Easy VPN virtual interfaces is preferable to using this combination.
One Easy VPN virtual interface and one static virtual interface	IOS	<ul style="list-style-type: none"> Both tunnels cannot terminate on the same peer. The static virtual interface and the Easy VPN virtual interface can use the same outside interface. The Easy VPN virtual interface should use split tunneling.
Two Easy VPN virtual interfaces	IOS, ASA, and VPN 3000	<ul style="list-style-type: none"> Both tunnels cannot terminate on the same peer. At least one of the tunnels should use split tunneling. Web-Based Activation cannot be applied to both Easy VPN tunnels.

Banner

The Easy VPN server pushes a banner to the Easy VPN remote device. The Easy VPN remote device can use the banner during Xauth and web-based activation. The Easy VPN remote device displays the banner the first time that the Easy VPN tunnel is brought up.

The banner is configured under group configuration on the Easy VPN server.

Configuration Management Enhancements (Pushing a Configuration URL Through a Mode-Configuration Exchange)

After this feature has been configured on the server using the commands **configuration url** and **configuration version** (subcommands under the **crypto isakmp client configuration group** command), the server can “push” the configuration URL and configuration version number to the Easy VPN remote device. With this information, the Easy VPN remote device can download the configuration content and apply it to its running configuration. For more information about this feature, see the section “Configuration Management Enhancements” in the *Easy VPN Server* feature module.

Reactivate Primary Peer

The Reactivate Primary Peer feature allows a default primary peer to be defined. The default primary peer (a server) is one that is considered better than other peers for reasons such as lower cost, shorter distance, or more bandwidth. With this feature configured, if Easy VPN fails over during Phase 1 SA negotiations from the primary peer to the next peer in its backup list, and if the primary peer is again available, the connections with the backup peer are torn down and the connection is again made with the primary peer.

Dead Peer Detection is one of the mechanisms that acts as a trigger for primary peer reactivation. Idle timers that are configured under Easy VPN is another triggering mechanism. When configured, the idle timer detects inactivity on the tunnel and tears it down. A subsequent connect (which is immediate in auto mode) is attempted with the primary preferred peer rather than with the peer last used.

**Note**

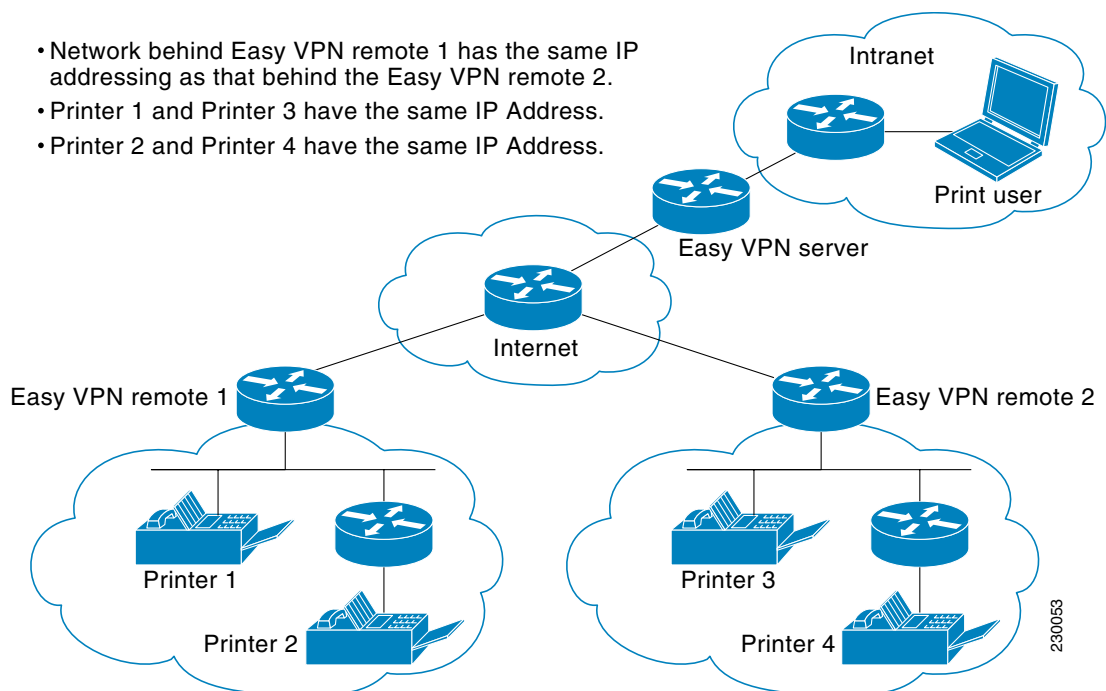
Only one primary peer can be defined.

Identical Addressing Support

The Identical Addressing Support feature supports identically addressed LANs on Easy VPN remotes. Network resources, such as printers and web servers on the LAN side of the EasyVPN remotes, that have overlapping addressing with other Easy VPN remotes are now reachable. The Easy VPN Remote feature was enhanced to work with NAT to provide this functionality.

- The Easy VPN server requires no changes to support the Identical Addressing Support feature.
- The Identical Addressing Support feature is supported only in network extension modes (network-extension and network-plus).
- Virtual tunnel interfaces must be configured on the Easy VPN remote before using the Identical Addressing Support feature.

Figure 11 shows an example of the Identical Addressing Support feature configuration.

Figure 11 Identical Addressing Support

The Identical Addressing Support feature can be configured with the following command and enhanced subcommands:

```
crypto ipsec client ezvpn <name>
```

Enhanced subcommands

- **nat acl** {*acl-name* | *acl-number*}—Enables split tunneling for the traffic specified by the ACL name or the ACL number.
 - The *acl-name* argument is the name of the ACL.
 - The *acl-number* argument is the number of the ACL.
- **nat allow**—Allows NAT to be integrated with Cisco Easy VPN.

For detailed steps on how to configure Identical Addressing Support, see “[Configuring Identical Addressing Support](#).”

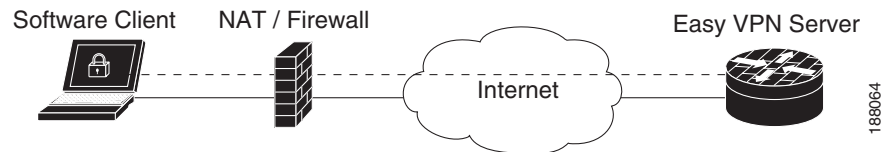
cTCP Support on Easy VPN Clients

The Cisco Tunneling Control Protocol (cTCP) feature can be used for situations in which an Easy VPN client (remote device) is operating in an environment in which standard IPsec does not function or in which it does not function transparently without modification to existing firewall rules. These situations include the following:

- Small office or home office router performing Network Address Translation (NAT) or Port Address Translation (PAT)
- PAT-provided IP address behind a larger router (for example, in a corporation)
- Non-NAT firewall (packet filtering or stateful)
- Proxy server

Figure 12 illustrates how IPsec traffic that is tunneled inside the cTCP traverses Network Address Translation (NAT) and the firewall (see the dashed line).

Figure 12 *cTCP on an Easy VPN Remote Device*



For detailed steps on how to configure cTCP on Easy VPN remote devices, see the section “[Configuring cTCP on an Easy VPN Client](#).”

For more information about cTCP support on Easy VPN remote devices, including configuration and troubleshooting examples, see “cTCP on Cisco Easy VPN remote devices” in the section “[Related Documents](#).”

How to Configure Cisco Easy VPN Remote

This section includes the following required and optional tasks.

Remote Tasks

- [Configuring and Assigning the Easy VPN Remote Configuration, page 36](#) (required)
- [Verifying the Cisco Easy VPN Configuration, page 38](#) (optional)
- [Configuring Save Password, page 39](#) (optional)
- [Configuring Manual Tunnel Control, page 40](#) (optional)
- [Configuring Automatic Tunnel Control, page 42](#) (optional)
- [Configuring Multiple Inside Interfaces, page 43](#) (optional)
- [Configuring Multiple Outside Interfaces, page 44](#) (optional)
- [Configuring Multiple Subnet Support, page 45](#) (optional)
- [Configuring Proxy DNS Server Support, page 47](#) (optional)
- [Configuring Dial Backup, page 47](#) (optional)
- [Configuring the DHCP Server Pool, page 48](#) (required)
- [Resetting a VPN Connection, page 48](#) (optional)
- [Monitoring and Maintaining VPN and IKE Events, page 49](#) (optional)
- [Configuring a Virtual Interface, page 50](#) (optional)
- [Troubleshooting Dual Tunnel Support, page 51](#) (optional)
- [Configuring Reactivate \(a Default\) Primary Peer, page 52](#) (optional)
- [Configuring Identical Addressing Support, page 53](#) (optional)
- [Configuring cTCP on an Easy VPN Client, page 56](#) (optional)

Easy VPN Server Tasks

- [Configuring a Cisco IOS Easy VPN Server, page 57](#) (required)
- [Configuring an Easy VPN Server on a VPN 3000 Series Concentrator, page 57](#) (optional)
- [Configuring an Easy VPN Server on a Cisco PIX Firewall, page 59](#) (optional)

Web Interface Tasks

- [Configuring Web-Based Activation, page 60](#) (optional)
- [Monitoring and Maintaining Web-Based Activation, page 60](#) (optional)
- [Using SDM As a Web Manager, page 64](#) (optional)

Troubleshooting the VPN Connection

- [Troubleshooting a VPN Connection Using the Cisco Easy VPN Remote Feature, page 64](#) (optional)
- [Troubleshooting the Client Mode of Operation, page 64](#) (optional)
- [Troubleshooting Remote Management, page 65](#) (optional)
- [Troubleshooting Dead Peer Detection, page 65](#) (optional)

Remote Tasks

Configuring and Assigning the Easy VPN Remote Configuration

The router acting as the Easy VPN remote must create a Cisco Easy VPN Remote configuration and assign it to the outgoing interface. To configure and assign the remote configuration, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec client ezvpn *name***
4. **group *group-name* key *group-key***
5. **peer [*ip-address* | *hostname*]**
6. **mode {**client** | **network-extension**}**
7. **exit**
8. **interface *interface***
9. **crypto ipsec client ezvpn *name* [**outside**]**
10. **exit**
11. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto ipsec client ezvpn name Example: Router (config)# crypto ipsec client ezvpn easy client remote	Creates a remote configuration and enters Cisco Easy VPN Remote configuration mode.
Step 4	group group-name key group-key Example: Router (config-crypto-ezvpn)# group easy-vpn-remote-groupname key easy-vpn-remote-password	Specifies the IPsec group and IPsec key value to be associated with this configuration. <p>Note The value of the <i>group-name</i> argument must match the group defined on the Easy VPN server. On Cisco IOS routers, use the crypto isakmp client configuration group and crypto map dynmap isakmp authorization list commands.</p> <p>Note The value of the <i>group-key</i> argument must match the key defined on the Easy VPN server. On Cisco IOS routers, use the crypto isakmp client configuration group command.</p>
Step 5	peer [ip-address hostname] Example: Router (config-crypto-ezvpn)# peer 192.185.0.5	Specifies the IP address or hostname for the destination peer (typically the IP address on the outside interface of the destination route). <ul style="list-style-type: none"> Multiple peers may be configured. <p>Note You must have a DNS server configured and available to use the <i>hostname</i> option.</p>
Step 6	mode {client network-extension} Example: Router (config-crypto-ezvpn)# mode client	Specifies the type of VPN connection that should be made. <ul style="list-style-type: none"> client—Specifies that the router is configured for VPN client operation, using NAT or PAT address translation. Client operation is the default if the type of VPN connection is not specified network-extension—Specifies that the router is to become a remote extension of the enterprise network at the destination of the VPN connection.
Step 7	exit Example: Router (config-crypto-ezvpn)# exit	Exits Cisco Easy VPN Remote configuration mode.

	Command	Purpose
Step 8	interface <i>interface</i> Example: Router (config)# interface Ethernet1	Enters interface configuration mode for the interface. <ul style="list-style-type: none">This interface will become the outside interface for the NAT or PAT translation.
Step 9	crypto ipsec client ezvpn <i>name</i> [outside] Example: Router (config-if)# crypto ipsec client ezvpn easy_vpn remotel outside	Assigns the Cisco Easy VPN Remote configuration to the interface. <ul style="list-style-type: none">This configuration automatically creates the necessary NAT or PAT translation parameters and initiates the VPN connection (if you are in client mode). Note The inside interface must be specified on Cisco 1700 and higher platforms.
Step 10	exit Example: Router (config-if)# exit	Exits interface configuration mode.
Step 11	exit Example: Router (config)# exit	Exits global configuration mode.

Verifying the Cisco Easy VPN Configuration

To verify that the Cisco Easy VPN Remote configuration has been correctly configured, that the configuration has been assigned to an interface, and that the IPsec VPN tunnel has been established, perform the following steps.

SUMMARY STEPS

1. **show crypto ipsec client ezvpn**
2. **show ip nat statistics**

DETAILED STEPS

- Step 1** Display the current state of the Cisco Easy VPN Remote connection using the **show crypto ipsec client ezvpn** command. The following is typical output for a Cisco 1700 series router using client mode:

```
Router# show crypto ipsec client ezvpn
```

```
Tunnel name : hw1
Inside interface list: FastEthernet0/0, Serial0/0,
Outside interface: Serial1/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 10.0.0.5
Mask: 255.255.255.255
Default Domain: cisco.com
Tunnel name : hw2
Inside interface list: Serial0/1,
Outside interface: Serial1/1
Current State: IPSEC_ACTIVE
```

```
Last Event: SOCKET_UP
Default Domain: cisco.com
```

- Step 2** Display the NAT or PAT configuration that was automatically created for the VPN connection using the **show ip nat statistics** command. The “Dynamic mappings” field of this display gives the details for the NAT or PAT translation that is occurring on the VPN tunnel.

```
Router# show ip nat statistics

Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  cable-modem0
Inside interfaces:
  Ethernet0
Hits: 1489 Misses: 1
Expired translations: 1
Dynamic mappings:
-- Inside Source
access-list 198 pool enterprise refcount 0
 pool enterprise: netmask 255.255.255.0
   start 192.168.1.90 end 192.168.1.90
   type generic, total addresses 1, allocated 0 (0%), misses 0\
```

If you are seeing IPSEC_ACTIVE in your output at this point, everything is operating as expected.

Configuring Save Password

To configure the Save Password feature, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **password encryption aes**
4. **crypto ipsec client ezvpn *name***
5. **username *name* password {0 | 6} {*password*}**
6. **exit**
7. **show running-config**

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	password encryption aes Example: Router (config)# password encryption aes	Enables a type 6 encrypted preshared key.
Step 4	crypto ipsec client ezvpn name Example: Router (config)# crypto ipsec client ezvpn ezvpn1	Creates a Cisco Easy VPN remote configuration and enters the Cisco Easy VPN remote configuration mode.
Step 5	username name password {0 6} {password} Example: Router (config-crypto-ezvpn)# username server_1 password 0 blue	Allows you to save your Xauth password locally on the PC. <ul style="list-style-type: none">The 0 keyword specifies that an unencrypted password will follow.The 6 keyword specifies that an encrypted password will follow.The <i>password</i> argument is the unencrypted (cleartext) user password.
Step 6	exit Example: Router (config-crypto-ezvpn)# exit	Exits the Cisco Easy VPN remote configuration mode.
Step 7	show running-config Example: Router (config)# show running-config	Displays the contents of the configuration file that is currently running.

Configuring Manual Tunnel Control

To configure control of IPsec VPN tunnels manually so that you can establish and terminate the IPsec VPN tunnels on demand, perform the following steps.



Note

CLI is one option for connecting the tunnel. The preferred method is via the web interface (using SDM).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec client ezvpn *name***
4. **connect [auto | manual]**
5. **exit**
6. **exit**
7. **crypto ipsec client ezvpn connect *name***

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto ipsec client ezvpn <i>name</i> Example: Router (config)# crypto ipsec client ezvpn easy vpn remotel	Assigns a Cisco Easy VPN remote configuration to an interface and enters Cisco Easy VPN Remote configuration mode. <ul style="list-style-type: none"> The <i>name</i> argument specifies the configuration name to be assigned to the interface.
Step 4	connect [auto manual] Example: Router (config-crypto-ezvpn)# connect manual	Connects the VPN tunnel. Specify manual to configure manual tunnel control. <ul style="list-style-type: none"> Automatic is the default; you do not need to use the manual keyword if your configuration is automatic.
Step 5	exit Example: Router (config-crypto-ezvpn)# exit	Exits Cisco Easy VPN Remote configuration mode.
Step 6	exit Example: Router (config)# exit	Exits global configuration mode and enters privileged EXEC mode.
Step 7	crypto ipsec client ezvpn connect <i>name</i> Example: Router# crypto ipsec client ezvpn connect easy vpn remotel	Connects a given Cisco Easy VPN remote configuration. <ul style="list-style-type: none"> The <i>name</i> argument specifies the IPsec VPN tunnel name. Note If the tunnel name is not specified, the active tunnel is connected. If there is more than one active tunnel, the command fails with an error requesting that you specify the tunnel name.

Configuring Automatic Tunnel Control

To configure automatic tunnel control, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec client ezvpn** *name*
4. **connect** [auto | manual]
5. **exit**
6. **exit**
7. **crypto ipsec client ezvpn connect** *name*

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto ipsec client ezvpn <i>name</i> Example: Router (config)# crypto ipsec client ezvpn easy vpn remotel	Assigns a Cisco Easy VPN remote configuration to an interface and enters Cisco Easy VPN Remote configuration mode. <ul style="list-style-type: none"> • Specify the configuration name to be assigned to the interface.
Step 4	connect [auto manual] Example: Router (config-crypto-ezvpn)# connect auto	Connects the VPN tunnel. <ul style="list-style-type: none"> • Specify auto to configure automatic tunnel control. Automatic is the default; you do not need to use this subcommand if your configuration is automatic.
Step 5	exit Example: Router (config-crypto-ezvpn)# exit	Exits Cisco Easy VPN Remote configuration mode.
Step 6	exit Example: Router (config)# exit	Exits global configuration mode and enters privileged EXEC mode.

	Command	Purpose
Step 7	crypto ipsec client ezvpn connect <i>name</i> Example: Router# crypto ipsec client ezvpn connect easy vpn remotel	Connects a given Cisco Easy VPN remote configuration. <ul style="list-style-type: none"> The <i>name</i> argument specifies the IPsec VPN tunnel name. Note If the tunnel name is not specified, the active tunnel is connected. If there is more than one active tunnel, the command fails with an error requesting that you specify the tunnel name.

Configuring Multiple Inside Interfaces

You can configure up to three inside interfaces for all platforms. You need to manually configure each inside interface using the following procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-name*
4. **exit**
5. **crypto ipsec client ezvpn** *name* [**outside** | **inside**]
6. **interface** *interface-name*
7. **exit**
8. **crypto ipsec client ezvpn** *name* [**outside** | **inside**]

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>interface-name</i> Example: Router (config)# interface Ethernet0	Selects the interface you want to configure by specifying the interface name and enters interface configuration mode.
Step 4	exit Example: Router (config-if)# exit	Exits interface configuration mode.

	Command	Purpose
Step 5	crypto ipsec client ezvpn <i>name</i> [outside inside] Example: Router (config)# crypto ipsec client ezvpn easy vpn remote 1 inside	Specifies the Cisco Easy VPN remote configuration name to be assigned to the first inside interface. <ul style="list-style-type: none"> You must specify inside for each inside interface.
Step 6	interface <i>interface-name</i> Example: Router (config)# interface Ethernet1	Selects the next interface you want to configure by specifying the next interface name and enters interface configuration mode.
Step 7	exit Example: Router (config-if)# exit	Exits interface configuration mode.
Step 8	crypto ipsec client ezvpn <i>name</i> [outside inside] Example: Router (config)# crypto ipsec client ezvpn easy vpn remote2 inside	Specifies the Cisco Easy VPN remote configuration name to be assigned to the next inside interface. <ul style="list-style-type: none"> You must specify inside for each inside interface. Repeat Step 3 through Step 4 to configure an additional tunnel if desired.

Configuring Multiple Outside Interfaces

You can configure multiple tunnels for outside interfaces, setting up a tunnel for each outside interface. You can configure a maximum of four tunnels using the following procedure for each outside interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface *interface-name***
4. **exit**
5. **crypto ipsec client ezvpn *name* [outside | inside]**
6. **interface *interface-name***
7. **exit**
8. **crypto ipsec client ezvpn *name* [outside | inside]**

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>interface-name</i> Example: Router (config)# interface Ethernet0	Selects the first outside interface you want to configure by specifying the interface name and enters interface configuration mode.
Step 4	exit Example: Router (config-if)# exit	Exits interface configuration mode.
Step 5	crypto ipsec client ezvpn <i>name</i> [outside inside] Example: Router (config)# crypto ipsec client ezvpn easy vpn remotel outside	Specifies the Cisco Easy VPN remote configuration name to be assigned to the first outside interface. <ul style="list-style-type: none">Specify outside (optional) for each outside interface. If neither outside nor inside is specified for the interface, the default is outside.
Step 6	interface <i>interface-name</i> Example: Router (config)# interface Ethernet1	Selects the next outside interface you want to configure by specifying the next interface name.
Step 7	exit Example: Router (config-if)# exit	Exits interface configuration mode.
Step 8	crypto ipsec client ezvpn <i>name</i> [outside inside] Example: Router (config)# crypto ipsec client ezvpn easy vpn remote2 outside	Specifies the Cisco Easy VPN remote configuration name to be assigned to the next outside interface. <ul style="list-style-type: none">Specify outside (optional) for each outside interface. If neither outside nor inside is specified for the interface, the default is outside. Repeat Step 3 through Step 4 to configure additional tunnels if desired.

Configuring Multiple Subnet Support

When configuring multiple subnet support, you must first configure an access list to define the actual subnets to be protected. Each source subnet or mask pair indicates that all traffic that is sourced from this network to any destination is protected by IPsec. For information about configuring ACLs, see “Access control lists, configuring” in the section “[Additional References](#).”

After you have defined the subnets, you must configure the crypto IPsec client EZVPN profile to use the ACLs.

**Note**

Multiple subnets are not supported in client mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-name*
4. **exit**
5. **crypto ipsec client ezvpn** *name*
6. **acl** {*acl-name* | *acl-number*}

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>interface-name</i> Example: Router (config)# interface Ethernet1	Selects the interface you want to configure by specifying the interface name and enters interface configuration mode.
Step 4	exit Example: Router (config-if)# exit	Exits interface configuration mode.
Step 5	crypto ipsec client ezvpn <i>name</i> Example: Router (config)# crypto ipsec client ezvpn ez1	Creates a Cisco Easy VPN remote configuration and enters crypto Easy VPN configuration mode.
Step 6	acl { <i>acl-name</i> <i>acl-number</i> } Example: Router (config-crypto-ezvpn)# acl acl-list1	Specifies multiple subnets in a VPN tunnel.

Configuring Proxy DNS Server Support

As a way of implementing the use of the DNS addresses of the ISP when the WAN connection is down, the router in a Cisco Easy VPN remote configuration can be configured to act as a proxy DNS server. To enable the proxy DNS server functionality with the **ip dns server** command, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dns server**

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip dns server Example: Router (config)# ip dns server	Enables the router to act as a proxy DNS server. Note This definition is IOS specific.

What to Do Next

After configuring the router, you configure the Cisco IOS Easy VPN server as follows:

- Under the **crypto isakmp client configuration group** command, configure the *dns* subcommand as in the following example:

```
dns A.B.C.D A1.B1.C1.D1
```

These DNS server addresses should be pushed from the server to the Cisco Easy VPN remote and dynamically added to or deleted from the running configuration of the router.

For information about general DNS server functionality in Cisco IOS software applications, see [Configuring DNS](#) and [Configuring DNS on Cisco Routers](#).

Configuring Dial Backup



Note

The Dial Backup feature is not available in Cisco IOS Release 12.3(11)T.

To configure dial backup, perform the following steps.

SUMMARY STEPS

1. Create the Easy VPN backup configuration.
2. Add the backup subcommand details to the primary configuration.
3. Apply the backup Easy VPN configuration to the dial backup outside interface.
4. Apply the Easy VPN profile to the inside interfaces.

DETAILED STEPS

	Command	Purpose
Step 1	Create the Easy VPN dial backup configuration.	For details about the backup configuration, see the section “ Dial Backup .”
Step 2	Add the backup subcommand details to the primary configuration.	Use the backup subcommand and track keyword of the crypto ipsec client ezvpn command.
Step 3	Apply the backup Easy VPN configuration to the dial backup outside interface (for example, serial, async, or dialer).	For details about applying the backup configuration to the dial backup outside interface, see the section “ Configuring Multiple Outside Interfaces .”
Step 4	Apply the Easy VPN profile to the inside interfaces (there can be more than one).	For details about applying the Easy VPN profile to the inside interfaces, see the section “ Configuring Multiple Inside Interfaces .”

Configuring the DHCP Server Pool

To configure the Dynamic Host Configuration Protocol (DHCP) server pool, see the chapter “[Configuring DHCP](#)” in the *Cisco IOS IP Configuration Guide*, Release 12.3.

Resetting a VPN Connection

To reset the VPN connection, perform the following steps. The **clear** commands can be configured in any order or independent of one another.

SUMMARY STEPS

1. **enable**
2. **clear crypto ipsec client ezvpn**
3. **clear crypto sa**
4. **clear crypto isakmp**

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	clear crypto ipsec client ezvpn Example: Router# clear crypto ipsec client ezvpn	Resets the Cisco Easy VPN remote state machine and brings down the Cisco Easy VPN remote connection on all interfaces or on a given interface (tunnel).
Step 3	clear crypto sa Example: Router# clear crypto sa	Deletes IPsec SAs.
Step 4	clear crypto isakmp Example: Router# clear crypto isakmp	Clears active IKE connections.

Monitoring and Maintaining VPN and IKE Events

To monitor and maintain VPN and IKE events, perform the following steps.

SUMMARY STEPS

1. enable
2. debug crypto ipsec client ezvpn
3. debug crypto ipsec
4. debug crypto isakmp

SUMMARY STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	debug crypto ipsec client ezvpn Example: Router# debug crypto ipsec client ezvpn	Displays information showing the configuration and implementation of the Cisco Easy VPN Remote feature.

	Command	Purpose
Step 3	debug crypto ipsec Example: Router# debug crypto ipsec	Displays IPsec events.
Step 4	debug crypto isakmp Example: Router# debug crypto isakmp	Displays messages about IKE events.

Configuring a Virtual Interface

To configure a virtual interface, perform the following steps.



Note

Before the virtual interface is configured, ensure that the Easy VPN profile is not applied on any outside interface. Remove the Easy VPN profile from the outside interface and then configure the virtual interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number* **type** *type-of-virtual-template*
4. **tunnel mode ipsec ipv4**
5. **exit**
6. **crypto ipsec client ezvpn** *name*
7. **virtual-interface** *virtual-template-number*

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface virtual-template <i>number</i> type <i>type-of-virtual-template</i> Example: Router (config)# interface virtual-template1 type tunnel	(Optional) Creates a virtual template of the type tunnel and enters interface configuration mode. <ul style="list-style-type: none"> • Steps 3, 4, and 5 are optional, but if one is configured, they must all be configured.

	Command	Purpose
Step 4	tunnel mode ipsec ipv4 Example: Router (if-config)# tunnel mode ipsec ipv4	(Optional) Configures the tunnel that does the IPsec tunneling.
Step 5	exit Example: Router (if-config)# exit	(Optional) Exits interface (virtual-tunnel) configuration mode.
Step 6	crypto ipsec client ezvpn name Example: Router (config)# crypto ipsec client ezvpn EasyVPN1	Creates a Cisco Easy VPN remote configuration and enters the Cisco Easy VPN remote configuration mode.
Step 7	virtual-interface virtual-template-number Example: Router (config-crypto-ezvpn)# virtual-interface 3	Instructs the Easy VPN remote to create a virtual interface to be used as an outside interface. If the virtual template number is specified, the virtual-access interface is derived from the virtual interface that was specified. If a virtual template number is not specified, a generic virtual-access interface is created.

Troubleshooting Dual Tunnel Support

The following **debug** and **show** commands may be used to troubleshoot your dual-tunnel configuration.

SUMMARY STEPS

1. **enable**
2. **debug crypto ipsec client ezvpn**
3. **debug ip policy**
4. **show crypto ipsec client ezvpn**
5. **show ip interface**

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	debug crypto ipsec client ezvpn Example: Router# debug crypto ipsec client ezvpn	Displays information about Cisco Easy VPN remote connections.

	Command	Purpose
Step 3	debug ip policy Example: Router# debug ip policy	Displays IP policy routing packet activity.
Step 4	show crypto ipsec client ezvpn Example: Router# show crypto ipsec client ezvpn	Displays the Cisco Easy VPN Remote configuration.
Step 5	show ip interface Example: Router# show ip interface	Displays the usability status of interfaces that are configured for IP.

Configuring Reactivate (a Default) Primary Peer

To configure a default primary peer, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec client ezvpn** *name*
4. **peer** {*ip-address* | *hostname*} [**default**]
5. **idle-time** *idle-time*

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto ipsec client ezvpn <i>name</i> Example: Router (config)# crypto ipsec client ezvpn ez1	Creates a Cisco Easy VPN remote configuration and enters crypto Easy VPN configuration mode.

	Command	Purpose
Step 4	peer { <i>ip-address</i> <i>hostname</i> } [default] Example: Router (config-crypto-ezvpn)# peer 10.2.2.2 default	Sets the peer IP address or hostname for the VPN connection. <ul style="list-style-type: none"> A hostname can be specified only when the router has a DNS server available for hostname resolution. The peer subcommand may be input multiple times. However, only one default or primary peer entry can exist at a time (for example, 10.2.2.2 default). The default keyword defines the peer as the primary peer.
Step 5	idle-time <i>idle-time</i> Example: Router (config-crypto-ezvpn)# idle-time 60	(Optional) Idle time in seconds after which an Easy VPN tunnel is brought down. <ul style="list-style-type: none"> Idle time=60 through 86400 seconds. Note If idle time is configured, the tunnel for the primary server is not brought down.

Configuring Identical Addressing Support

Configuring Identical Addressing Support comprises the following tasks:

- Defining the Easy VPN remote in network-extension mode and enabling **nat allow**.
- Assigning the Cisco Easy VPN Remote configuration to the Outside interface.
- Creating a loopback interface and assigning the Cisco Easy VPN Remote configuration to the Inside interface of the loopback interface.
- Configuring a one-to-one static NAT translation for each host that needs to be accessible from the EasyVPN server-side network or from other client locations.
- Configuring dynamic overloaded NAT or PAT using an access list for all the desired VPN traffic. The NAT or PAT traffic is mapped to the Easy VPN inside interface IP address.
- And, if split-tunneling is required, using the **nat acl** command to enable split-tunneling for the traffic specified by the *acl-name* or the *acl-number* argument. The ACL is the same as the ACL used by the NAT or PAT mapping in the preceding bullet item.

To configure Identical Addressing Support, perform the following steps on your router.

Prerequisites

Easy VPN Remote must be configured in network extension mode before you can configure the Identical Addressing Support feature.

SUMMARY STEPS

- enable**
- configure terminal**
- crypto ipsec client ezvpn** *name*
- mode network-extension**
- nat allow**
- exit**
- interface** *interface*

8. **crypto ipsec client ezvpn name** *outside*
9. **exit**
10. **interface** *interface*
11. **ip address** *ip mask*
12. **crypto ipsec client ezvpn name** *inside*
13. **exit**
14. **ip nat inside source static** *local-ip global-ip*
15. **ip nat inside source list** {*acl-name* | *acl-number*} **interface** *interface* **overload**
16. **crypto ipsec client ezvpn name**
17. **nat acl** {*acl-name* | *acl-number*}
18. **exit**
19. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto ipsec client ezvpn name Example: Router (config)# crypto ipsec client ezvpn easyclient	Creates a remote configuration and enters Cisco Easy VPN Remote configuration mode.
Step 4	mode network-extension Example: Router (config-crypto-ezvpn)# mode network-extension	Configures Easy VPN client in network-extension mode.
Step 5	nat allow Example: Router (config-crypto-ezvpn)# nat allow	Allows NAT to be integrated with Easy VPN and enables the Identical Addressing feature.
Step 6	exit Example: Router (config-crypto-ezvpn)# exit	Exits Cisco Easy VPN Remote configuration mode.

	Command	Purpose
Step 7	interface <i>interface</i> Example: Router (config)# interface Ethernet1	Enters interface configuration mode for the interface. <ul style="list-style-type: none"> This interface will become the outside interface for the NAT or PAT translation.
Step 8	crypto ipsec client ezvpn name outside Example: Router (config-if)# crypto ipsec client ezvpn easyclient outside	Assigns the Cisco Easy VPN Remote configuration to the outside interface. <ul style="list-style-type: none"> This configuration automatically creates the necessary NAT or PAT translation parameters and initiates the VPN connection (if you are in client mode).
Step 9	exit Example: Router (config-if)# exit	Exits interface configuration mode.
Step 10	interface <i>interface</i> Example: Router (config)# interface Loopback0	Enters interface configuration mode for the loopback interface. <ul style="list-style-type: none"> This interface will become the inside interface for the NAT or PAT translation.
Step 11	ip address ip mask Example: Router (config-if)# ip address 10.1.1.1 255.255.255.252	Assigns the IP address and mask to the loopback interface.
Step 12	crypto ipsec client ezvpn name inside Example: Router (config-if)# crypto ipsec client ezvpn easyclient inside	Assigns the Cisco Easy VPN Remote configuration to the inside interface.
Step 13	exit Example: Router (config-if)# exit	Exits interface configuration mode.
Step 14	ip nat inside source static local-ip global-ip Example: Router (config)# ip nat inside source static 10.10.10.10 5.5.5.5	Configure a one-to-one static NAT translation for each host that needs to be accessible from the Easy VPN server side network, or from other client locations.
Step 15	ip nat inside source list {acl-name acl-number} interface interface overload Example: Router (config)# ip nat inside source list 100 interface Loopback0 overload	Configure dynamic overloaded NAT or PAT, which uses an ACL for all the desired VPN traffic. The NAT and PAT traffic is mapped to the Easy VPN inside interface IP address. <ul style="list-style-type: none"> The <i>acl-name</i> argument is the name of the ACL. The <i>acl-number</i> argument is the number of the ACL.

	Command	Purpose
Step 16	crypto ipsec client ezvpn <i>name</i> Example: Router (config)# crypto ipsec client ezvpn easyclient	(Optional, if using split tunneling) Enters Cisco Easy VPN Remote configuration mode.
Step 17	nat acl { <i>acl-name</i> <i>acl-number</i> } Example: Router (config-crypto-ezvpn)# nat acl 100	(Optional, if using split tunneling) Enables split-tunneling for the traffic specified by the <i>acl-name</i> or the <i>acl-number</i> argument. The ACL is the same as the ACL used by the NAT or PAT mapping in the Step 15. <ul style="list-style-type: none">• The <i>acl-name</i> argument is the name of the ACL.• The <i>acl-number</i> argument is the number of the ACL.
Step 18	exit Example: Router (config-crypto-ezvpn)# exit	Exits Cisco Easy VPN Remote configuration mode.
Step 19	exit Example: Router (config)# exit	Exits global configuration mode.

Configuring cTCP on an Easy VPN Client

To configure cTCP on an Easy VPN client (remote device), perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ctcp** [*keepalive number-of-seconds* | **port** *port-number*]
4. **crypto ipsec client ezvpn** *name*
5. **ctcp port** *port-number*

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command	Purpose
Step 3	crypto ctcp [keepalive <i>number-of-seconds</i> port <i>port-number</i>] Example: Router (config)# crypto ctcp keepalive 15	Sets cTCP keepalive interval for the remote device. <ul style="list-style-type: none"> <i>number-of-seconds</i>—Number of seconds between keepalives. Value = 5 through 3600. port <i>port-number</i>—Port number that cTCP listens to. Up to 10 numbers can be configured. Note The cTCP client has to send periodic keepalives to the server to keep NAT or firewall sessions alive.
Step 4	crypto ipsec client ezvpn <i>name</i> Example: Router (config)# crypto ipsec client ezvpn ezvpn1	Creates a Cisco Easy VPN remote configuration and enters Cisco Easy VPN remote configuration mode.
Step 5	ctcp port <i>port-number</i> Example: Router (config-crypto-ezvpn)# ctcp port 200	Sets the port number for cTCP encapsulation for Easy VPN. <ul style="list-style-type: none"> <i>port-number</i>—Port number on the hub. Value = 1 through 65535.

Easy VPN Server Tasks

Configuring a Cisco IOS Easy VPN Server

For information about configuring the Easy VPN Server, see the following document:

- [Easy VPN Server](#)

Configuring an Easy VPN Server on a VPN 3000 Series Concentrator

This section describes the guidelines required to configure the Cisco VPN 3000 series concentrator for use with the Cisco Easy VPN Remote feature. As a general rule, you can use the default configuration except for IP addresses, server addresses, routing configurations, and for the following parameters and options:

- [Peer Configuration on a Cisco Easy VPN Remote Using the Hostname](#), page 58
- [Interactive Hardware Client Authentication Version 3.5](#), page 58
- [IPsec Tunnel Protocol](#), page 58
- [IPsec Group](#), page 58
- [Group Lock](#), page 58
- [Xauth](#), page 59
- [Split Tunneling](#), page 59
- [IKE Proposals](#), page 59
- [New IPsec SA](#), page 59

**Note**

You must be using Cisco VPN 3000 series concentrator software Release 3.11 or later to support Cisco Easy VPN software clients and remotes.

Peer Configuration on a Cisco Easy VPN Remote Using the Hostname

After you have configured the Cisco Easy VPN server on the VPN 3000 concentrator to use hostname as its identity, you must configure the peer on the Cisco Easy VPN remote using the hostname. You can either configure DNS on the client to resolve the peer hostname or configure the peer hostname locally on the client using the **ip host** command. As an example, you can configure the peer hostname locally on an Easy VPN remote as follows:

```
ip host crypto-gw.cisco.com 10.0.0.1
```

Or you can configure the Easy VPN remote to use the hostname with the **peer** command and *hostname* argument, as follows:

```
peer crypto-gw.cisco.com.
```

Interactive Hardware Client Authentication Version 3.5

The Cisco Easy VPN Remote feature does not support the Interactive Hardware Client Authentication Version 3.5 feature. This feature must be disabled. You can disable the feature on the VPN 3000 series concentrator by clicking the **HW Client** tab on the **Configuration | User Management | Base Group** screen.

IPsec Tunnel Protocol

IPsec Tunnel Protocol enables the IPsec tunnel protocol so that it is available for users. The IPsec Tunnel Protocol is configured on the Cisco VPN 3000 series concentrator by clicking the **General** tab on the **Configuration | User Management | Base Group** screen.

IPsec Group

IPsec group configures the Cisco VPN 3000 series concentrator with a group name and password that match the values configured for the Cisco Easy VPN remote configuration on the router. These values are configured on the router with the **group group-name key group-key** subcommand and arguments. The values are configured on the Cisco VPN 3000 series concentrator using the **Configuration | User Management | Groups** screen.

Group Lock

If you are defining multiple users in multiple groups on the VPN 3000 series concentrator, you must check the **Group Lock** box in the IPsec tab to prevent users in one group from logging in with the parameters of another group. For example, if you have configured one group for split tunneling access and another group without split tunneling access, clicking the **Group Lock** box prevents users in the second group from gaining access to the split tunneling features. The Group Lock checkbox appears in the **IPsec** tab in the **Configuration | User Management | Base Group** screen and in the **IPsec** tab in the **Configuration | User Management | Groups | Add/Modify** screens.

Xauth

To use Xauth, set the **Authentication** parameter to **None**. The Authentication parameter appears in the **IPsec** tab in the **Configuration | User Management | Base Group** screen and in the **IPsec** tab in the **Configuration | User Management | Groups | Add/Modify** screens.

Split Tunneling

The **Configuration | User Management | Base Group, Mode Configuration Parameters Tab** screen includes a **Split Tunnel** option with a checkbox that says “Allow the networks in the list to bypass the tunnel.”

IKE Proposals

The Cisco VPN 3000 series concentrator is preconfigured with a default IKE proposal, CiscoVPNClient-3DES-MD5, that can be used with Cisco Easy VPN remotes. This IKE proposal supports preshared keys with Xauth using the MD5/HMAC-128 algorithm and Diffie-Hellman Group 2.

This IKE proposal is active by default, but you should verify that it is still an active proposal using the **Configuration | System | Tunneling Protocols | IPsec | IKE Proposals** screen.

In addition, as part of configuring the Cisco VPN 3000 series concentrator—for the Cisco Easy VPN Remote image, you do not need to create a new IPsec SA. Use the default IKE and Easy VPN remote lifetime configured on the Cisco VPN 3000 series concentrator.



Note

You can also use the default IKE proposals IKE-DES-MD5 and IKE-3DES-MD5, but they do not enable Xauth support by default.

New IPsec SA

You can create a new IPsec SA. Cisco Easy VPN clients use a SA having the following parameters:

- Authentication Algorithm=ESP/MD5/HMAC-128
- Encryption Algorithm=DES-56 or 3DES-168 (recommended)
- Encapsulation Mode=Tunnel
- IKE Proposal=CiscoVPNClient-3DES-MD5 (preferred)

The Cisco VPN 3000 series concentrator is preconfigured with several default security associations (SAs), but they do not meet the IKE proposal requirements. To use an IKE proposal of CiscoVPNClient-3DES-MD5, copy the ESP/IKE-3DES-MD5 SA and modify it to use CiscoVPNClient-3DES-MD5 as its IKE proposal. An IKE proposal is configured on the VPN 3000 series concentrator using the **Configuration | Policy Management | Traffic Management | Security Associations** screen.

Configuring an Easy VPN Server on a Cisco PIX Firewall

For information about configuring an Easy VPN Server on a Cisco PIX Firewall, see the following document:

- [Easy VPN Server](#)

Web Interface Tasks

Configuring Web-Based Activation

To configure a LAN so that any HTTP requests coming from any of the PCs on the private LAN are intercepted, providing corporate users with access to the corporate Web page, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec client ezvpn *name***
4. **xauth userid mode {http-intercept | interactive | local}**

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto ipsec client ezvpn <i>name</i> Example: Router (config)# crypto ipsec client ezvpn easy vpn remotel	Assigns a Cisco Easy VPN remote configuration to an interface and enters Cisco Easy VPN Remote configuration mode. <ul style="list-style-type: none">• The <i>name</i> argument specifies the configuration name to be assigned to the interface.
Step 4	xauth userid mode {http-intercept interactive local} Example: Router (config-crypto-ezvpn)# xauth userid mode http-intercept	Specifies how the VPN device handles Xauth requests or prompts from the server.

Monitoring and Maintaining Web-Based Activation

To monitor and maintain web-based activation, perform the following steps. (The **debug** and **show** commands may be used independently, or they may all be configured.)

SUMMARY STEPS

1. **enable**
2. **debug crypto ipsec client ezvpn**

3. **debug ip auth-proxy ezvpn**
4. **show crypto ipsec client ezvpn**
5. **show ip auth-proxy config**

DETAILED STEPS

	Command	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	debug crypto ipsec client ezvpn Example: Router# debug crypto ipsec client ezvpn	Displays information about the Cisco Easy VPN connection.
Step 3	debug ip auth-proxy ezvpn Example: Router# debug ip auth-proxy ezvpn	Displays information related to proxy authentication behavior for web-based activation.
Step 4	show crypto ipsec client ezvpn Example: Router# show crypto ipsec client ezvpn	Shows that the username and password used for user credentials during Xauth negotiations will be obtained by intercepting HTTP connections from the user.
Step 5	show ip auth-proxy config Example: Router# show ip auth-proxy config	Displays the auth-proxy rule that has been created and applied by Easy VPN.

Examples

Debug Output

The following is sample **debug** output for a typical situation in which a user has opened a browser and connected to the corporate website:

```
Router# debug ip auth-proxy ezvpn
```

```
Dec 10 12:41:13.335: AUTH-PROXY: New request received by EzVPN WebIntercept
! The following line shows the ip address of the user.
from 10.4.205.205
Dec 10 12:41:13.335: AUTH-PROXY:GET request received
Dec 10 12:41:13.335: AUTH-PROXY:Normal auth scheme in operation
Dec 10 12:41:13.335: AUTH-PROXY:Ezvpn is NOT active. Sending connect-bypass page to user
```

At this point, the user chooses “connect” on his or her browser:

```
Dec 10 12:42:43.427: AUTH-PROXY: New request received by EzVPN WebIntercept
from 10.4.205.205
Dec 10 12:42:43.427: AUTH-PROXY:POST request received
Dec 10 12:42:43.639: AUTH-PROXY:Found attribute <connect> in form
Dec 10 12:42:43.639: AUTH-PROXY:Sending POST data to EzVPN
Dec 10 12:42:43.639: EZVPN(tunnel22): Communication from Interceptor
application.
```

```
Request/Response from 10.4.205.205, via Ethernet0
Dec 10 12:42:43.639:          connect: Connect Now
Dec 10 12:42:43.639: EZVPN(tunnel22): Received CONNECT from 10.4.205.205!
Dec 10 12:42:43.643: EZVPN(tunnel22): Current State: CONNECT_REQUIRED
Dec 10 12:42:43.643: EZVPN(tunnel22): Event: CONNECT
Dec 10 12:42:43.643: EZVPN(tunnel22): ezvpn_connect_request
```

Easy VPN contacts the server:

```
Dec 10 12:42:43.643: EZVPN(tunnel22): Found valid peer 192.168.0.1
Dec 10 12:42:43.643: EZVPN(tunnel22): Added PSK for address 192.168.0.1

Dec 10 12:42:43.643: EZVPN(tunnel22): New State: READY
Dec 10 12:42:44.815: EZVPN(tunnel22): Current State: READY
Dec 10 12:42:44.815: EZVPN(tunnel22): Event: IKE_PFS
Dec 10 12:42:44.815: EZVPN(tunnel22): No state change
Dec 10 12:42:44.819: EZVPN(tunnel22): Current State: READY
Dec 10 12:42:44.819: EZVPN(tunnel22): Event: CONN_UP
Dec 10 12:42:44.819: EZVPN(tunnel22): ezvpn_conn_up B8E86EC7 E88A8A18 D0D51422
8AFF32B7
```

The server requests Xauth information:

```
Dec 10 12:42:44.823: EZVPN(tunnel22): No state change
Dec 10 12:42:44.827: EZVPN(tunnel22): Current State: READY
Dec 10 12:42:44.831: EZVPN(tunnel22): Event: XAUTH_REQUEST
Dec 10 12:42:44.831: EZVPN(tunnel22): ezvpn_xauth_request
Dec 10 12:42:44.831: EZVPN(tunnel22): ezvpn_parse_xauth_msg
Dec 10 12:42:44.831: EZVPN: Attributes sent in xauth request message:
Dec 10 12:42:44.831:          XAUTH_TYPE_V2(tunnel22): 0
Dec 10 12:42:44.831:          XAUTH_USER_NAME_V2(tunnel22):
Dec 10 12:42:44.831:          XAUTH_USER_PASSWORD_V2(tunnel22):
Dec 10 12:42:44.831:          XAUTH_MESSAGE_V2(tunnel22) <Enter Username and
Password.>
Dec 10 12:42:44.831: EZVPN(tunnel22): Requesting following info for xauth
Dec 10 12:42:44.831:          username:(Null)
Dec 10 12:42:44.835:          password:(Null)
Dec 10 12:42:44.835:          message:Enter Username and Password.
Dec 10 12:42:44.835: EZVPN(tunnel22): New State: XAUTH_REQ
```

The username and password prompt are displayed in the browser of the user:

```
Dec 10 12:42:44.835: AUTH-PROXY: Response to POST is CONTINUE
Dec 10 12:42:44.839: AUTH-PROXY: Displayed POST response successfully
Dec 10 12:42:44.843: AUTH-PROXY:Served POST response to the user
```

When the user enters his or her username and password, the following is sent to the server:

```
Dec 10 12:42:55.343: AUTH-PROXY: New request received by EzVPN WebIntercept
from 10.4.205.205
Dec 10 12:42:55.347: AUTH-PROXY:POST request received
Dec 10 12:42:55.559: AUTH-PROXY:No of POST parameters is 3
Dec 10 12:42:55.559: AUTH-PROXY:Found attribute <username> in form
Dec 10 12:42:55.559: AUTH-PROXY:Found attribute <password> in form
Dec 10 12:42:55.559: AUTH-PROXY:Found attribute <ok> in form
Dec 10 12:42:55.563: AUTH-PROXY:Sending POST data to EzVPN
Dec 10 12:42:55.563: EZVPN(tunnel22): Communication from Interceptor application.
Request/Response from 10.4.205.205, via Ethernet0
Dec 10 12:42:55.563:          username:http
Dec 10 12:42:55.563:          password:<omitted>
Dec 10 12:42:55.563:          ok:Continue
Dec 10 12:42:55.563: EZVPN(tunnel22): Received username|password from 10.4.205.205!
Dec 10 12:42:55.567: EZVPN(tunnel22): Current State: XAUTH_PROMPT
Dec 10 12:42:55.567: EZVPN(tunnel22): Event: XAUTH_REQ_INFO_READY
Dec 10 12:42:55.567: EZVPN(tunnel22): ezvpn_xauth_reply
```

```
Dec 10 12:42:55.567:          XAUTH_TYPE_V2(tunnel22): 0
Dec 10 12:42:55.567:          XAUTH_USER_NAME_V2(tunnel22): http
Dec 10 12:42:55.567:          XAUTH_USER_PASSWORD_V2(tunnel22): <omitted>
Dec 10 12:42:55.567: EZVPN(tunnel22): New State: XAUTH_REPLIED
Dec 10 12:42:55.891: EZVPN(tunnel22): Current State: XAUTH_REPLIED
Dec 10 12:42:55.891: EZVPN(tunnel22): Event: XAUTH_STATUS
Dec 10 12:42:55.891: EZVPN(tunnel22): xauth status received: Success
```

After using the tunnel, the user chooses “Disconnect”:

```
Dec 10 12:48:17.267: EZVPN(tunnel22): Received authentic disconnect credential
Dec 10 12:48:17.275: EZVPN(): Received an HTTP request: disconnect
Dec 10 12:48:17.275: %CRYPTO-6-EZVPN_CONNECTION_DOWN: (Client) User=
    Group=tunnel22 Client_public_addr=192.168.0.13 Server_public_addr=192.168.0.1
    Assigned_client_addr=10.3.4.5
```

Show Output Before the User Is Connected to the Tunnel

The following output from the two **show** commands (**show crypto ipsec client ezvpn** and **show ip auth-proxy config**) displays what you might see before a user is connected to a VPN tunnel:

```
Router# show crypto ipsec client ezvpn tunnel22
```

```
Tunnel name : tunnel22
Inside interface list: Ethernet0
Outside interface: Ethernet1
Current State: CONNECT_REQUIRED
Last Event: RESET
Save Password: Disallowed
! Note the next line.
    XAuth credentials: HTTP intercepted
    HTTP return code : 200
    IP addr being prompted: 0.0.0.0
Current EzVPN Peer: 192.168.0.1
```

```
Router# show ip auth-proxy config
```

```
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Rule Configuration
! Note that the next line is the Easy VPN-defined internal rule.
    Auth-proxy name ezvpn401***
    Applied on Ethernet0
    http list not specified inactivity-timer 60 minutes
```

Show Output After the User Is Connected to the Tunnel

The following output from the two **show** commands (**show crypto ipsec client ezvpn** and **show ip auth-proxy config**) displays what you might see after the user has been connected to the tunnel:

```
Router# show crypto ipsec client ezvpn tunnel22
```

```
Tunnel name : tunnel22
Inside interface list: Ethernet0
Outside interface: Ethernet1
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 10.3.4.5
Mask: 255.255.255.255
Save Password: Disallowed
    XAuth credentials: HTTP intercepted
    HTTP return code : 200
    IP addr being prompted: 192.168.0.0
```

```
Current EzVPN Peer: 192.168.0.1

Router# show ip auth-proxy config

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication Proxy Watch-list is disabled

Auth-proxy name ezvpnWeb*** (EzVPN-defined internal rule)
http list not specified inactivity-timer 60 minutes
```

Using SDM As a Web Manager

For information about the SDM web manager, see the following document:

- [Cisco Security Device Manager](#)

Troubleshooting the VPN Connection

Troubleshooting a VPN Connection Using the Cisco Easy VPN Remote Feature

To troubleshoot a VPN connection created using the Cisco Easy VPN Remote feature, use the following suggested techniques.

- Be aware that any changes to an active Cisco Easy VPN remote configuration or IP address changes to the involved interfaces, such as adding or removing an inside interface, result in a reset of the Cisco Easy VPN Remote connection.
- Enable debugging of the Cisco Easy VPN Remote feature using the **debug crypto ipsec client ezvpn** command.
- Enable debugging of IKE events using the **debug crypto ipsec** and **debug crypto isakmp** commands.
- Display the active IPsec VPN connections using the **show crypto engine connections active** command.
- To reset the VPN connection, use the **clear crypto ipsec client ezvpn** command. If you have debugging enabled, you might prefer to use the **clear crypto sa** and **clear crypto isakmp** commands.

Troubleshooting the Client Mode of Operation

The following information may be used to troubleshoot the Easy VPN Remote configuration for the client mode of operation.

In client mode, the Cisco Easy VPN Remote feature automatically configures the NAT or PAT translation and access lists that are needed to implement the VPN tunnel. These configurations are automatically created when the IPsec VPN connection is initiated. When the tunnel is torn down, the NAT or PAT and access list configurations are automatically deleted.

The NAT or PAT configuration is created with the following assumptions:

- The **ip nat inside** command is applied to all inside interfaces, including default inside interfaces. The default inside interface is the Ethernet 0 interface (for the Cisco 806, Cisco 826, Cisco 827, Cisco 828, Cisco 831, Cisco 836, and Cisco 837 routers).

- The **ip nat outside** command is applied to the interface that is configured with the Cisco Easy VPN Remote configuration. On the Cisco 800 series and Cisco 1700 series routers, the outside interface is configured with the Cisco Easy VPN Remote configuration. On the Cisco 1700 series routers, Cisco 2600 series routers, Cisco 3600 series routers, and Cisco 3700 series routers, multiple outside interfaces can be configured.

**Tip**

The NAT or PAT translation and access list configurations that are created by the Cisco Easy VPN Remote feature are not written to either the startup configuration or running configuration files. These configurations, however, can be displayed using the **show ip nat statistics** and **show access-list** commands.

Troubleshooting Remote Management

To troubleshoot remote management of the VPN remote, use the **show ip interface** command. Using the **brief** keyword, you can verify that the loopback has been removed and that the interface is shown correctly.

Examples

Following is a typical example of output from the **show ip interface** command.

```
Router# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0	unassigned	YES	NVRAM	administratively down	down
Ethernet1	10.0.0.11	YES	NVRAM	up	up
Loopback0	192.168.6.1	YES	manual	up	up
Loopback1	10.12.12.12	YES	NVRAM	up	up

```
Router# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0	unassigned	YES	NVRAM	administratively down	down
Ethernet1	10.0.0.11	YES	NVRAM	up	up
Loopback1	10.12.12.12	YES	NVRAM	up	up

Troubleshooting Dead Peer Detection

To troubleshoot dead peer detection, use the **show crypto ipsec client ezvpn** command.

Examples

The following typical output displays the current server and the peers that have been pushed by the Easy VPN server:

```
Router# show crypto ipsec client ezvpn
```

```
Easy VPN Remote Phase: 4
Tunnel name : ez1
Inside interface list: Loopback1,
Outside interface: Ethernet1
```

```
Current State: IPSEC_ACTIVE
Last Event: CONNECT
Address: 192.168.6.5
Mask: 255.255.255.255
DNS Primary: 10.2.2.2
DNS Secondary: 10.2.2.3
NBMS/WINS Primary: 10.6.6.6
Default Domain: cisco.com
Save Password: Allowed
Current EzVPN Peer:10.0.0.110
Backup Gateways
(0): green.cisco.com
(1): blue
```

Configuration Examples for Cisco Easy VPN Remote

This section provides the following configuration examples.

Easy VPN Remote Configuration Examples

- [Client Mode Configuration: Examples, page 67](#)
- [Local Address Support for Easy VPN Remote: Example, page 72](#)
- [Network Extension Mode Configuration: Examples, page 73](#)
- [Save Password Configuration: Example, page 77](#)
- [PFS Support: Examples, page 78](#)
- [Dial Backup: Examples, page 78](#)
- [Web-Based Activation: Example, page 84](#)
- [Easy VPN Remote with Virtual IPsec Interface Support Configuration: Examples, page 84](#)
- [Dual Tunnel Configuration: Example, page 89](#)
- [Dual Tunnel Show Output: Examples, page 91](#)
- [Reactivate Primary Peer: Example, page 94](#)
- [Identical Addressing Support Configuration: Example, page 95](#)
- [cTCP on an Easy VPN Client \(Remote Device\): Examples, page 95](#)

Easy VPN Server Configuration Examples

- [Cisco Easy VPN Server Without Split Tunneling: Example, page 96](#)
- [Cisco Easy VPN Server Configuration with Split Tunneling: Example, page 97](#)
- [Cisco Easy VPN Server Configuration with Xauth: Example, page 99](#)
- [Easy VPN Server Interoperability Support: Example, page 101](#)

Easy VPN Remote Configuration Examples

Client Mode Configuration: Examples

The examples in this section show configurations for the Cisco Easy VPN Remote feature in client mode. Also shown are the Cisco IOS Easy VPN server configurations that correspond to these client configurations.

- [Cisco Easy VPN Client in Client Mode \(Cisco 831\): Example, page 67](#)
- [Cisco Easy VPN Client in Client Mode \(Cisco 837\): Example, page 68](#)
- [Cisco Easy VPN Client in Client Mode \(Cisco 1700 Series\): Example, page 70](#)

For more client-mode configuration examples, see [IPSec VPN](#) (under the “Technical Documents” and “Cisco IOS IPSec Configuration Documents” sections) and to [Cisco Easy VPN Solutions](#).



Note

Typically, users configure the Cisco 800 series routers with the SDM or CRWS web interface, not by entering CLI commands. However, the configurations shown here for the Cisco 800 series routers display typical configurations that can be used if manual configuration is desired.

Cisco Easy VPN Client in Client Mode (Cisco 831): Example

In the following example, a Cisco 831 router is configured as an Easy VPN remote using the Cisco Easy VPN Remote feature in client mode. This example shows the following components of the Cisco Easy VPN Remote configuration:

- DHCP server pool—The **ip dhcp pool** command creates a pool of IP addresses to be assigned to the PCs connected to the Ethernet 0 interface of the router. The pool assigns addresses in the class C private address space (192.168.100.0) and configures each PC so that its default route is 192.168.100.1, which is the IP address assigned to the Ethernet interface of the router. The DHCP lease period is one day.
- Cisco Easy VPN remote configuration—The first **crypto ipsec client ezvpn easy vpn remote** command (global configuration mode) creates a Cisco Easy VPN remote configuration named “easy vpn remote.” This configuration specifies the group name “easy vpn remote-groupname” and the shared key value “easy vpn remote-password,” and it sets the peer destination to the IP address **192.185.0.5** (which is the address assigned to the interface connected to the Internet on the destination peer router). The Cisco Easy VPN Remote configuration is configured for the default **client** mode.



Note

If DNS is also configured on the router, the **peer** keyword option also supports a hostname instead of an IP address.

- The second **crypto ipsec client ezvpn easy vpn remote** command (interface configuration mode) assigns the Cisco Easy VPN Remote configuration to the Ethernet 1 interface so that all traffic that is received and transmitted on that interface is sent through the VPN tunnel.

```
! Cisco Router Web Setup Template
!
no service pad
no service tcp-small-servers
no service udp-small-servers
service timestamps debug uptime
service timestamps log uptime
```

```

service password-encryption
!
hostname 806Router
!
!
ip subnet-zero
ip domain-lookup
ip dhcp excluded-address 10.10.10.1
!
ip dhcp pool CLIENT
    import all
    network 10.10.10.0 255.255.255.255
    default-router 10.10.10.1
    lease 1 0 0
!
!
crypto ipsec client ezvpn easy_vpn_remote
    peer 192.168.0.5
    group easy_vpn_remote_groupname key easy_vpn_remote_password
    mode client
!
!
interface Ethernet0
    ip address 10.10.10.1 255.255.255.255
    no cdp enable
    hold-queue 32 in
!
interface Ethernet1
    ip address dhcp
    no cdp enable
    crypto ipsec client ezvpn easy_vpn_remote
!
ip classless
ip http server
!
!
ip route 10.0.0.0 10.0.0.0 Ethernet1
!
line con 0
    exec-timeout 120 0
    stopbits 1
line vty 0 4
    exec-timeout 0 0
    login local

```

Cisco Easy VPN Client in Client Mode (Cisco 837): Example

In the following example, a Cisco 837 router is configured as an Easy VPN remote using the Cisco Easy VPN Remote feature in the client mode of operation. This example shows the following components of the Cisco Easy VPN remote configuration:

- PPPoE configuration—The ATM 0 interface is configured to support PPPoE connections over the Dialer 1 virtual interface. Because the interfaces use PPPoE, a DHCP IP address pool is not required to provide IP addresses to the connected PCs.
- Cisco Easy VPN Remote configuration—The first **crypto ipsec client ezvpn** command (global configuration mode) creates a Cisco Easy VPN remote configuration named “easy vpn remote.” This configuration specifies the group name “easy vpn remote-groupname” and the shared key value of “easy vpn remote-password,” and it sets the peer destination to the IP address 10.0.0.5 (which is the address assigned to the interface connected to the Internet on the destination peer router). The Cisco Easy VPN remote configuration is configured for the default client mode.



Note If DNS is also configured on the router, the **peer** keyword option also supports a hostname instead of an IP address.

- The second **crypto ipsec client ezvpn** command (interface configuration mode) assigns the Cisco Easy VPN remote configuration to the Dialer 1 interface so that all traffic received and transmitted on that interface is sent through the VPN tunnel.

```

version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname c827
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
vpdn enable
!
vpdn-group pppoe
 request-dialin
  protocol pppoe
  ip mtu adjust
!!
!
crypto ipsec client ezvpn easy_vpn_remote
 group easy_vpn_remote_groupname key easy_vpn_remote_password
 mode client
 peer 10.0.0.5
!!
!
interface Ethernet0
 ip address 10.0.0.117 255.0.0.0
 hold-queue 100 out
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 1/40
  pppoe-client dial-pool-number 1
!
 dsl operating-mode auto
!
interface Dialer1
 ip address 10.0.0.3 255.0.0.0
 ip mtu 1492
 encapsulation ppp
 dialer pool 1
 crypto ipsec client ezvpn easy_vpn_remote
!
ip classless
ip route 0.0.0.0 0.0.0.0 ATM0
ip route 0.0.0.0 0.0.0.0 Dialer1 permanent
ip route 10.0.0.0 255.0.0.0 10.0.0.13

```

```

ip http server
ip pim bidir-enable
!
line con 0
  stopbits 1
line vty 0 4
  login
!
scheduler max-task-time 5000
end

```

Cisco Easy VPN Client in Client Mode (Cisco 1700 Series): Example

In the following example, a Cisco 1753 router is configured as an Easy VPN remote using the Cisco Easy VPN Remote feature in the client mode of operation. This example shows a running configuration of a Cisco 1753 that has two inside interfaces and one outside interface on one tunnel. The **connect auto** subcommand manually establishes the IPsec VPN tunnel.

Router# **show running-config**

```

Building configuration...
Current configuration : 881 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mma-1753
!
!
memory-size iomem 15
ip subnet-zero
!!
!
ip ssh time-out 120
ip ssh authentication-retries 3
! !
!
crypto ipsec client ezvpn easy_vpn_remote
connect auto
group ezvpn key ezvpn
mode client
peer 10.6.6.1
! !
!
interface FastEthernet0/0
ip address 10.4.4.2 255.255.255.0
speed auto
crypto ipsec client ezvpn easy_vpn_remote inside
!
interface Serial0/0
ip address 10.6.6.2 255.255.255.0
no fair-queue
crypto ipsec client ezvpn easy_vpn_remote
!
interface Serial1/0
ip address 10.5.5.2 255.255.255.0
clock rate 4000000
crypto ipsec client ezvpn easy_vpn_remote inside
!
ip classless
no ip http server

```

```

ip pim bidir-enable
!
!
line con 0
line aux 0
line vty 0 4
login
!
end

```

The following example shows a running configuration of a Cisco 1760 router that has two active, automatically connected tunnels, easy vpn remote1 and easy vpn remote2. Tunnel easy vpn remote1 has two configured inside interfaces and one configured outside interface. Tunnel easy vpn remote2 has one configured inside interface and one configured outside interface. The example also shows the output for the **show crypto ipsec client ezvpn** command that lists the tunnel names and the outside and inside interfaces.

Router# **show running-config**

```

Building configuration...
Current configuration : 1246 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 1760
!
aaa new-model
!
!
aaa session-id common
!
ip subnet-zero
!!
!
crypto ipsec client ezvpn easy_vpn_remote2
connect auto
group ez key ez
mode network-extension
peer 10.7.7.1
crypto ipsec client ezvpn easy_vpn_remote1
connect auto
group ezvpn key ezvpn
mode client
peer 10.6.6.1
!
!
!
interface FastEthernet0/0
ip address 10.5.5.2 255.255.255.0
speed auto
no cdp enable
crypto ipsec client ezvpn easy_vpn_remote1 inside
!
interface Serial10/0
ip address 10.4.4.2 255.255.255.0
no ip route-cache
no ip mroute-cache
no fair-queue
no cdp enable
crypto ipsec client ezvpn easy_vpn_remote1 inside
!

```

```

interface Serial0/1
ip address 10.3.3.2 255.255.255.0
no cdp enable
crypto ipsec client ezvpn easy_vpn_remote2 inside
!
interface Serial1/0
ip address 10.6.6.2 255.255.255.0
clockrate 4000000
no cdp enable
crypto ipsec client ezvpn easy_vpn_remotel
!
interface Serial1/1
ip address 10.7.7.2 255.255.255.0
no keepalive
no cdp enable
crypto ipsec client ezvpn easy_vpn_remote2
!
ip classless
no ip http server
ip pim bidir-enable
!
!
radius-server retransmit 3
radius-server authorization permit missing Service-Type
!
line con 0
line aux 0
line vty 0 4
!
no scheduler allocate
end

```

```
Router# show crypto ipsec client ezvpn
```

```

Tunnel name : easy_vpn_remotel
Inside interface list: FastEthernet0/0, Serial0/0,
Outside interface: Serial1/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 10.0.0.5
Mask: 255.255.255.255
Default Domain: cisco.com
Tunnel name : easy_vpn_remote2
Inside interface list: Serial0/1,
Outside interface: Serial1/1
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Default Domain: cisco.com

```

Local Address Support for Easy VPN Remote: Example

The following example shows that the **local-address** command is used to specify the loopback 0 interface for sourcing tunnel traffic:

```

Router# configure terminal
Router(config)# crypto ipsec client ezvpn telecommuter-client
Router(config-crypto-ezvpn)# local-address loopback0

```


Network Extension Mode Configuration: Examples

In this section, the following examples demonstrate how to configure the Cisco Easy VPN Remote feature in the network extension mode of operation. Also shown are the Cisco IOS Easy VPN server configurations that correspond to these client configurations.

- [Cisco Easy VPN Client in Network Extension Mode \(Cisco 831\): Example, page 73](#)
- [Cisco Easy VPN Client in Network Extension Mode \(Cisco 837\): Example, page 74](#)
- [Cisco Easy VPN Client in Network Extension Mode \(Cisco 1700 Series\): Example, page 76](#)

For more network extension mode configuration examples, see *IPSec VPN* (under the “Technical Documents” and “Cisco IOS IPSec Configuration Documents” sections) and to *Cisco Easy VPN Solutions*.

Cisco Easy VPN Client in Network Extension Mode (Cisco 831): Example

In the following example, a Cisco 831 router is configured as an Easy VPN remote using the Cisco Easy VPN Remote feature. This example shows the following components of the Cisco Easy VPN remote configuration:

- The Ethernet 0 interface is assigned an address in the network address space of the Cisco IOS Easy VPN server. The **ip route** command directs all traffic for this network space from the Ethernet 1 interface to the destination server.
- Cisco Easy VPN Remote configuration—The first **crypto ipsec client ezvpn** command (global configuration mode) creates a Cisco Easy VPN remote configuration named “easy vpn remote.” This configuration specifies the group name “easy vpn remote-groupname” and the shared key value “easy vpn remote-password,” and it sets the peer destination to the IP address 192.185.0.5 (which is the address assigned to the interface connected to the Internet on the destination peer router). The Cisco Easy VPN remote configuration is configured for network extension mode.



Note If DNS is also configured on the router, the **peer** keyword option also supports a hostname instead of an IP address.

- The second **crypto ipsec client ezvpn** command (interface configuration mode) assigns the Cisco Easy VPN Remote configuration to the Ethernet 1 interface so that all traffic that is received and transmitted on that interface is sent through the VPN tunnel.

```
! Cisco Router Web Setup Template
!
no service pad
no service tcp-small-servers
no service udp-small-servers
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname Router
!
!
ip subnet-zero
ip domain-lookup
!
!
ip dhcp excluded-address 172.31.1.1
!
ip dhcp pool localpool
```

```

import all
network 172.31.1.0 255.255.255.255
default-router 172.31.1.1
lease 1 0 0
!
!
crypto ipsec client ezvpn easy_vpn_remote
peer 192.168.0.5
group easy_vpn_remote_groupname key easy_vpn_remote_password
mode network-extension
!
!
interface Ethernet0
ip address 172.31.1.1 255.255.255.255
no cdp enable
hold-queue 32 in
!
interface Ethernet1
ip address dhcp
no cdp enable
crypto ipsec client ezvpn easy_vpn_remote
!
ip classless
ip route 172.31.0.0 255.255.255.255 Ethernet1
ip http server
!
!
line con 0
exec-timeout 120 0
stopbits 1
line vty 0 4
exec-timeout 0 0
login local

```

Cisco Easy VPN Client in Network Extension Mode (Cisco 837): Example

In the following example, a Cisco 837 router is configured as an Easy VPN remote using the Cisco Easy VPN Remote feature in client mode. This example shows the following components of the Cisco Easy VPN remote configuration:

- PPPoE configuration—The ATM 0 interface is configured to support PPPoE connections over the Dialer 1 virtual interface. Because the interfaces use PPPoE, a DHCP IP address pool is not required to provide IP addresses to the connected PCs.
- The Ethernet 0 interface is assigned an address in the network address space of the Cisco IOS Easy VPN server. The **ip route** command directs all traffic for this network space from the Dialer 1 interface to the destination server.
- Cisco Easy VPN Remote configuration—The first **crypto ipsec client ezvpn** command (global configuration mode) creates a Cisco Easy VPN remote configuration named “easy vpn remote.” This configuration specifies the group name “easy vpn remote-groupname” and the shared key value “easy vpn remote-password,” and it sets the peer destination to the IP address 10.0.0.5 (which is the address assigned to the interface connected to the Internet on the destination peer router). The Cisco Easy VPN remote configuration is configured for the default network extension mode.



Note

If DNS is also configured on the router, the **peer** keyword option also supports a hostname instead of an IP address.

- The second **crypto ipsec client ezvpn** command (interface configuration mode) assigns the Cisco Easy VPN remote configuration to the Dialer1 interface so that all traffic that is received and transmitted on that interface is sent through the VPN tunnel.

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname c827
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
vpdn enable
!
vpdn-group pppoe
 request-dialin
  protocol pppoe
  ip mtu adjust
!
!
crypto ipsec client ezvpn easy_vpn_remote
 group easy_vpn_remote_groupname key easy_vpn_remote_password
 mode network-extension
 peer 10.0.0.5
!
!
interface Ethernet0
 ip address 172.16.0.30 255.255.255.192
 hold-queue 100 out
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 1/40
  pppoe-client dial-pool-number 1
!
dsl operating-mode auto
!
interface Dialer1
 ip address 10.0.0.3 255.0.0.0
 ip mtu 1492
 encapsulation ppp
 dialer pool 1
 crypto ipsec client ezvpn easy_vpn_remote
!
ip classless
ip route 172.16.0.0 255.255.255.128 Dialer1
ip route 0.0.0.0 0.0.0.0 ATM0
ip route 0.0.0.0 0.0.0.0 Dialer1 permanent
ip route 10.0.0.0 255.0.0.0 10.0.0.13
ip http server
ip pim bidir-enable
!
line con 0
 stopbits 1
```

```

line vty 0 4
 login
!
scheduler max-task-time 5000

```

Cisco Easy VPN Client in Network Extension Mode (Cisco 1700 Series): Example

In the following example, a Cisco 1700 series router is configured as an Easy VPN remote using the Cisco Easy VPN Remote feature in the network extension mode of operation. This example shows the following components of the Cisco Easy VPN remote configuration:

- Cisco Easy VPN Remote configuration—The first **crypto ipsec client ezvpn** command (global configuration mode) creates a Cisco Easy VPN remote configuration that is named “easy vpn remote.” This configuration specifies the group name “easy vpn remote-groupname” and the shared key value “easy vpn remote-password,” and it sets the peer destination to the IP address 10.0.0.2 (which is the address assigned to the interface connected to the Internet on the destination peer router). The Cisco Easy VPN remote configuration is configured for network extension mode.



Note If DNS is also configured on the router, the **peer** keyword option also supports a hostname instead of an IP address.

- The second **crypto ipsec client ezvpn easy vpn remote** command (interface configuration mode) assigns the Cisco Easy VPN remote configuration to the Ethernet 0 interface so that all traffic that is received and transmitted on that interface is sent through the VPN tunnel.

```

!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 1710
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
!
ip dhcp excluded-address 10.0.0.10
!
ip dhcp pool localpool
 import all
 network 10.70.0.0 255.255.255.248
 default-router 10.70.0.10
 lease 1 0 0
!
!
crypto ipsec client ezvpn easy_vpn_remote
 group easy_vpn_remote_groupname key easy_vpn_remote_password
 mode network-extension
 peer 10.0.0.2
!
!

```

```

interface Ethernet0
 ip address 10.50.0.10 255.0.0.0
 half-duplex
 crypto ipsec client ezvpn easy_vpn_remote
 !
interface FastEthernet0
 ip address 10.10.0.10 255.0.0.0
 speed auto
 !
ip classless
ip route 10.20.0.0 255.0.0.0 Ethernet0
ip route 10.20.0.0 255.0.0.0 Ethernet0
no ip http server
ip pim bidir-enable
!!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login

```

Save Password Configuration: Example

The following sample **show running-config** output shows that the Save Password feature has been configured (note the **password encryption aes** command and **username** keywords in the output):

Router# **show running-config**

```

133.CABLEMODEM.CISCO: Oct 28 18:42:07.115: %SYS-5-CONFIG_I: Configured from console by
consolen
Building configuration...

```

```

Current configuration : 1269 bytes
!
! Last configuration change at 14:42:07 UTC Tue Oct 28 2003
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
clock timezone UTC -4
no aaa new-model
ip subnet-zero
no ip routing
!
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
password encryption aes
!
!

```

```

no crypto isakmp enable
!
!
crypto ipsec client ezvpn remote_vpn_client
  connect auto
  mode client
  username greentree password 6 ARiFgh`SOJfMHLK[MHMQJZagR\M
!
!
interface Ethernet0
  ip address 10.3.66.4 255.255.255.0
  no ip route-cache
  bridge-group 59

```

PFS Support: Examples

The following **show crypto ipsec client ezvpn** command output shows the group name (“2”) and that PFS is being used:

```
Router# show crypto ipsec client ezvpn
```

```
Easy VPN Remote Phase: 4
```

```

Tunnel name : ez1
Inside interface list: Loopback1,
Outside interface: Ethernet1
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 192.168.6.6
Mask: 255.255.255.255
Using PFS Group: 2
Save Password: Allowed
Current EzVPN Peer:10.0.0.110

```

Note that on a Cisco IOS EasyVPN server, PFS must be included in IPsec proposals by adding to the crypto map, as in the following example:

```

crypto dynamic-map mode 1
  set security-association lifetime seconds 180
  set transform-set client
  set pfs group2
  set isakmp-profile fred
reverse-route

```

Dial Backup: Examples

Static IP Addressing

The following example shows that static IP addressing has been configured for a Cisco 1711 router:

```
Router# show running-config
```

```
Building configuration...
```

```

Current configuration : 3427 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ph4_R5

```

```
!
boot-start-marker
boot-end-marker
!
no logging buffered
!
username ph4_R8 password 0 cisco
username ph4_R7 password 0 lab
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
aaa new-model
!
!
aaa session-id common
ip subnet-zero
!
!
no ip domain lookup
ip cef
ip ids po max-events 100
ip dhcp-client default-router distance 1
no ftp-server write-enable
!
!
track 123 rtr 3 reachability
!
crypto isakmp keepalive 10 periodic
!
!
crypto ipsec client ezvpn backup_profile_vpn3k
connect auto
group hw_client_groupname key password123
mode client
peer 10.0.0.5
username rchu password password123
crypto ipsec client ezvpn hw_client_vpn3k
connect auto
group hw_client_groupname key password123
backup backup_profile_vpn3k track 123
mode client
peer 10.0.0.5
username rchu password password123
!
!
interface Loopback0
 ip address 10.40.40.50 255.255.255.255
!
interface Loopback1
 ip address 10.40.40.51 255.255.255.255
!
interface Loopback2
 no ip address
!
interface FastEthernet0
 description Primary Link to 10.0.0.2
 ip address 10.0.0.10 255.255.255.0
 duplex auto
 speed auto
 no cdp enable
 crypto ipsec client ezvpn hw_client_vpn3k
!
interface FastEthernet1
```

```

no ip address
duplex full
speed 100
no cdp enable
!
interface FastEthernet2
no ip address
no cdp enable
!
interface FastEthernet3
no ip address
no cdp enable
!
interface FastEthernet4
no ip address
no cdp enable
!
interface Vlan1
ip address 10.0.0.1 255.255.255.0
crypto ipsec client ezvpn backup_profile_vpn3k inside
crypto ipsec client ezvpn hw_client_vpn3k inside
!
interface Async1
description Backup Link
no ip address
ip nat outside
ip virtual-reassembly
encapsulation ppp
no ip route-cache cef
dialer in-band
dialer pool-member 1
dialer-group 1
async default routing
async mode dedicated
!
interface Dialer1
ip address 10.30.0.1 255.255.255.0
encapsulation ppp
no ip route-cache cef
dialer pool 1
dialer idle-timeout 60
dialer string 102
dialer hold-queue 100
dialer-group 1
crypto ipsec client ezvpn backup_profile_vpn3k
!
ip local policy route-map policy_for_rtr
ip classless

ip route 0.0.0.0 0.0.0.0 faste0 track 123

ip route 0.0.0.0 0.0.0.0 Dialer1 240
no ip http server
no ip http secure-server
!
!
ip access-list extended dummy1
permit ip host 10.0.0.2 host 10.3.0.1
ip access-list extended important_traffic
permit ip 10.0.0.0 0.0.0.255 10.0.0.2 0.0.0.255
permit ip 10.0.0.0 0.0.0.255 10.0.0.3 0.0.0.255
ip access-list extended important_traffic_2
permit ip 10.0.0.0 0.0.0.255 10.0.0.3 0.0.0.255

```



```
access-list 112 permit icmp any host 10.0.10.2 echo
dialer-list 1 protocol ip permit
no cdp run
!
route-map policy_for_rtr permit 10
  match ip address 112
  set interface Null0
  set ip next-hop 10.0.10.2
!
!
control-plane
!
rtr 2
  type echo protocol ipIcmpEcho 10.0.0.2 source-ipaddr 10.0.0.3
  timeout 10000
  threshold 1000
  frequency 11
rtr schedule 2 life forever start-time now
rtr 3
  type echo protocol ipIcmpEcho 10.0.0.2 source-interface FastEthernet0
  timeout 10000
  threshold 1000
  frequency 11
rtr schedule 3 life forever start-time now
!
line con 0
  exec-timeout 0 0
line 1
  modem InOut
  modem autoconfigure discovery
  transport input all
  autoselect ppp
  stopbits 1
  speed 115200
  flowcontrol hardware
line aux 0
line vty 0 4
  password lab
!
```

DHCP Configured on Primary Interface and PPP Async As Backup

The following example shows that a Cisco 1711 router has been configured so that DHCP is configured on the primary interface and PPP asynchronous mode is configured as the backup:

Router# **show running-config**

Building configuration...

```
Current configuration : 3427 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ph4_R5
!
boot-start-marker
boot-end-marker
!
no logging buffered
!
username ph4_R8 password 0 cisco
```

```

username ph4_R7 password 0 lab
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
aaa new-model
!
!
aaa session-id common
ip subnet-zero
!
!
no ip domain lookup
ip cef
ip ids po max-events 100
ip dhcp-client default-router distance 1
no ftp-server write-enable
!
!
track 123 rtr 3 reachability
!
crypto isakmp keepalive 10 periodic
!
!
crypto ipsec client ezvpn backup_profile_vpn3k
connect auto
group hw_client_groupname key password123
mode client
peer 10.0.0.5
username rchu password password123
crypto ipsec client ezvpn hw_client_vpn3k
connect auto
group hw_client_groupname key password123
backup backup_profile_vpn3k track 123
mode client
peer 10.0.0.5
username rchu password password123
!
!
interface Loopback0
ip address 10.40.40.50 255.255.255.255
!
interface Loopback1
ip address 10.40.40.51 255.255.255.255
!
interface Loopback2
no ip address
!
interface FastEthernet0
description Primary Link to 10.0.0.2
ip dhcp client route track 123
ip address dhcp
duplex auto
speed auto
no cdp enable
crypto ipsec client ezvpn hw_client_vpn3k
!
interface FastEthernet1
no ip address
duplex full
speed 100
no cdp enable
!
interface FastEthernet2

```

```
no ip address
no cdp enable
!
interface FastEthernet3
no ip address
no cdp enable
!
interface FastEthernet4
no ip address
no cdp enable
!
interface Vlan1
ip address 10.0.0.1 255.255.255.0
crypto ipsec client ezvpn backup_profile_vpn3k inside
crypto ipsec client ezvpn hw_client_vpn3k inside
!
interface Async1
description Backup Link
no ip address
ip nat outside
ip virtual-reassembly
encapsulation ppp
no ip route-cache cef
dialer in-band
dialer pool-member 1
dialer-group 1
async default routing
async mode dedicated
!
interface Dialer1
ip address 10.0.0.3 255.255.255.0
encapsulation ppp
no ip route-cache cef
dialer pool 1
dialer idle-timeout 60
dialer string 102
dialer hold-queue 100
dialer-group 1
crypto ipsec client ezvpn backup_profile_vpn3k
!
ip local policy route-map policy_for_rtr
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1 240
no ip http server
no ip http secure-server
!
!
ip access-list extended dummy1
permit ip host 10.10.0.2 host 10.0.0.1
ip access-list extended important_traffic
permit ip 10.0.0.0 0.0.0.255 10.0.0.2 0.0.0.255
permit ip 10.0.0.0 0.0.0.255 10.0.0.3 0.0.0.255
ip access-list extended important_traffic_2
permit ip 10.0.0.0 0.0.0.255 10.0.0.3 0.0.0.255
access-list 112 permit icmp any host 10.0.0.2 echo
dialer-list 1 protocol ip permit
no cdp run
!
route-map policy_for_rtr permit 10
match ip address 112
set interface Null0
set ip next-hop 10.0.0.2
!
!
```

```

control-plane
!
rtr 2
 type echo protocol ipIcmpEcho 10.0.0.2 source-ipaddr 10.0.0.3
 timeout 10000
 threshold 1000
 frequency 11
rtr schedule 2 life forever start-time now
rtr 3
 type echo protocol ipIcmpEcho 10.0.0.2 source-interface FastEthernet0
 timeout 10000
 threshold 1000
 frequency 11
rtr schedule 3 life forever start-time now
!
line con 0
 exec-timeout 0 0
line 1
 modem InOut
 modem autoconfigure discovery
 transport input all
 autoselect ppp
 stopbits 1
 speed 115200
 flowcontrol hardware
line aux 0
line vty 0 4
 password lab
!

```

Web-Based Activation: Example

The following example shows that HTTP connections from the user are to be intercepted and that the user can do web-based authentication (192.0.0.13 is the VPN client device and 192.0.0.1 is the server device):

```

crypto ipsec client ezvpn tunnel22
 connect manual
 group tunnel22 key 22tunnel
 mode client
 peer 192.168.0.1
 xauth userid mode http-intercept
!
!
interface Ethernet0
 ip address 10.4.23.15 255.0.0.0
 crypto ipsec client ezvpn tunnel22 inside!
interface Ethernet1
 ip address 192.168.0.13 255.255.255.128
 duplex auto
 crypto ipsec client ezvpn tunnel22
!

```

Easy VPN Remote with Virtual IPsec Interface Support Configuration: Examples

The following examples indicate that Virtual IPsec Interface Support has been configured on the Easy VPN remote devices.

Virtual IPsec Interface: Generic Virtual Access

The following example shows an Easy VPN remote device with virtual-interface support using a generic virtual-access IPsec interface.

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone IST 0
ip subnet-zero
no ip dhcp use vrf connected
!
!
crypto ipsec client ezvpn ez
  connect manual
  group easy key cisco
  mode client
  peer 10.3.0.2
  virtual-interface
  xauth userid mode interactive
!
!
interface Ethernet0/0
  ip address 10.1.0.2 255.255.255.0
  no keepalive
  no cdp enable
  crypto ipsec client ezvpn ez inside
!
interface Ethernet1/0
  ip address 10.2.0.1 255.255.255.0
  no keepalive
  no cdp enable
  crypto ipsec client ezvpn ez
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.2.0.2 2
no ip http server
no ip http secure-server
!
!
line con 0
line aux 0
line vty 0 4
  login
!
end
```

Virtual IPsec Interface: Virtual Access Derived from Virtual Template

The following example shows an Easy VPN remote device with virtual-interface support using a virtual-template-derived virtual-access IPsec interface:

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone IST 0
ip subnet-zero
no ip dhcp use vrf connected
!
!
crypto ipsec client ezvpn ez
  connect manual
  group easy key cisco
  mode client
  peer 10.3.0.2
  virtual-interface 1
  xauth userid mode interactive
!
!
interface Ethernet0/0
  ip address 10.1.0.2 255.255.255.0
  no keepalive
  no cdp enable
  crypto ipsec client ezvpn ez inside
!
interface Ethernet1/0
  ip address 10.2.0.1 255.255.255.0
  no keepalive
  no cdp enable
  crypto ipsec client ezvpn ez
!
interface Virtual-Template1 type tunnel
  no ip address
  tunnel mode ipsec ipv4
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.2.0.2 2
no ip http server
no ip http secure-server
!
!
line con 0
line aux 0
line vty 0 4
  login
!
end

```

When the Tunnel Is Down

The result of a virtual-interface configuration on an Easy VPN profile is the creation of a virtual-access interface. This interface provides IPsec encapsulation. The output below shows the configuration of a virtual-access interface when Easy VPN is “down.”

```
Router# show running-config interface virtual-access 2
```

```
Building configuration...
```

```
Current configuration : 99 bytes
!
interface Virtual-Access2
 no ip address
 tunnel source Ethernet1/0
 tunnel mode ipsec ipv4
end
```

A virtual-interface configuration results in the creation of a virtual-access interface. This virtual-access interface is made automatically outside the interface of the Easy VPN profile. The routes that are added later when the Easy VPN tunnels come up point to this virtual interface for sending the packets to the corporate network. If **crypto ipsec client ezvpn name outside (crypto ipsec client ezvpn name command and outside keyword)** is applied on a real interface, that interface is used as the IKE (IPsec) endpoint (that is, IKE and IPsec packets use the address on the interface as the source address).

```
Router# show crypto ipsec client ezvpn
```

```
Easy VPN Remote Phase: 5

Tunnel name : ez
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access2 (bound to Ethernet1/0)
Current State: CONNECT_REQUIRED
Last Event: TRACKED OBJECT UP
Save Password: Disallowed
Current EzVPN Peer: 10.3.0.2
```

Because a virtual interface, or for that matter any interface, is routable, routes act like traffic selectors. When the Easy VPN tunnel is “down,” there are no routes pointing to the virtual interface, as shown in the following example:

```
Router# show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.2.0.2 to network 0.0.0.0

    10.0.0.0/24 is subnetted, 2 subnets
C       10.2.0.0 is directly connected, Ethernet1/0
C       10.1.0.0 is directly connected, Ethernet0/0
S*    0.0.0.0/0 [2/0] via 10.2.0.2
```

When the Tunnel Is Up

In the case of client or network plus mode, Easy VPN creates a loopback interface and assigns the address that is pushed in mode configuration. To assign the address of the loopback to the interface, use the **ip unnumbered** command (**ip unnumbered loopback**). In the case of network extension mode, the virtual access will be configured as **ip unnumbered ethernet0** (the bound interface).

```
Router# show running-config interface virtual-access 2
```

```
Building configuration...
```

```
Current configuration : 138 bytes
```

```
!
interface Virtual-Access2
 ip unnumbered Loopback0
 tunnel source Ethernet1/0
 tunnel destination 10.3.0.2
 tunnel mode ipsec ipv4
end
```

```
Router# show crypto ipsec client ezvpn
```

```
Easy VPN Remote Phase: 5
```

```
Tunnel name : ez
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access2 (bound to Ethernet1/0)
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 10.5.0.2
Mask: 255.255.255.255
DNS Primary: 10.6.0.2
NBMS/WINS Primary: 10.7.0.1
Default Domain: cisco.com
Using PFS Group: 2
Save Password: Disallowed
Split Tunnel List: 1
    Address      : 10.4.0.0
    Mask         : 255.255.255.0
    Protocol     : 0x0
    Source Port  : 0
    Dest Port    : 0
Current EzVPN Peer: 10.3.0.2
```

When the tunnels come up, Easy VPN adds either a default route that points to the virtual-access interface or adds routes for all the split attributes of the subnets that point to the virtual-access interface. Easy VPN also adds a route to the peer (destination or concentrator) if the peer is not directly connected to the Easy VPN device.

The following **show ip route** command output examples are for virtual IPsec interface situations in which a split tunnel attribute was sent by the server and a split tunnel attribute was not sent, respectively.

Split Tunnel Attribute Has Been Sent by the Server

```
Router# show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
```


o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.2.0.2 to network 0.0.0.0

```

10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C    10.2.0.0/24 is directly connected, Ethernet1/0
S    10.3.0.2/32 [1/0] via 10.2.0.2, Ethernet1/0 <<< Route to
peer (EzVPN server)
C    10.1.0.0/24 is directly connected, Ethernet0/0
C    10.5.0.2/32 is directly connected, Loopback0
S    10.4.0.0/24 [1/0] via 0.0.0.0, Virtual-Access2 <<< Split
tunnel attr sent by the server
S*   10.0.0.0/0 [2/0] via 10.2.0.2

```

Split Tunnel Attribute Has Not Been Sent by the Server

All networks in the split attribute should be shown, as in the following example:

Router# **show ip route**

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

```

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

```

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C    10.2.0.0/24 is directly connected, Ethernet1/0
! The following line is the route to the peer (the Easy VPN server).
S    10.3.0.2/32 [1/0] via 10.2.0.2, Ethernet1/0
C    10.1.0.0/24 is directly connected, Ethernet0/0
C    10.5.0.3/32 is directly connected, Loopback0
! The following line is the default route.
S*   10.0.0.0/0 [1/0] via 10.0.0.0, Virtual-Access2

```

Dual Tunnel Configuration: Example

The following is an example of a typical dual-tunnel configuration:

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable password lab
!
no aaa new-model
!
resource policy
!
clock timezone IST 0
ip subnet-zero
!
!

```

```

username lab password 0 lab
!
!
crypto ipsec client ezvpn ezvpn1
  connect manual
  group easy key cisco
  mode network-extension
  peer 10.75.1.2
  virtual-interface 1
  xauth userid mode interactive
crypto ipsec client ezvpn ezvpn2
  connect manual
  group easy key cisco
  mode network-extension
  peer 10.75.2.2
  virtual-interface 1
  xauth userid mode interactive
!
!
interface Ethernet0/0
  ip address 192.168.1.1 255.255.255.255
  no keepalive
  crypto ipsec client ezvpn ezvpn1 inside
  crypto ipsec client ezvpn ezvpn2 inside
!
interface Ethernet0/1
  no ip address
  shutdown
!
interface Ethernet0/2
  no ip address
  shutdown
!
interface Ethernet0/3
  no ip address
  shutdown
!
interface Ethernet1/0
  ip address 10.76.1.2 255.255.255.0
  no keepalive
  crypto ipsec client ezvpn ezvpn1
  crypto ipsec client ezvpn ezvpn2
!
interface Serial2/0
  ip address 10.76.2.2 255.255.255.0
  no keepalive
  serial restart-delay 0
!
interface Virtual-Template1 type tunnel
  no ip address
  tunnel mode ipsec ipv4
!
!
ip classless
ip route 10.0.0.0 10.0.0.0 10.76.1.1 2
no ip http server
no ip http secure-server
!
!
no cdp run
!
!
line con 0
  exec-timeout 0 0

```

```

line aux 0
line vty 0 4
  login local
!
end

```

Dual Tunnel Show Output: Examples

The following **show** command examples display information about three phases of a dual tunnel that is coming up:

- First Easy VPN tunnel is up
- Second Easy VPN tunnel is initiated
- Both of the Easy VPN tunnels are up

Before the EzVPN Tunnels Are Up

```
Router# show crypto ipsec client ezvpn
```

```
Easy VPN Remote Phase: 6
```

```

Tunnel name : ezvpn1
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access2 (bound to Ethernet1/0)
Current State: CONNECT_REQUIRED
Last Event: TRACKED OBJECT UP
Save Password: Disallowed
Current EzVPN Peer: 10.75.1.2

```

```

Tunnel name : ezvpn2
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access3 (bound to Serial2/0)
Current State: CONNECT_REQUIRED
Last Event: TRACKED OBJECT UP
Save Password: Disallowed
Current EzVPN Peer: 10.75.2.2

```

```
Router# show ip route
```

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

```

The gateway of last resort is 10.76.1.1 to network 0.0.0.0.

```

10.0.0.0/24 is subnetted, 2 subnets
C      10.76.2.0 is directly connected, Serial2/0
C      10.76.1.0 is directly connected, Ethernet1/0
C      192.168.1.0/24 is directly connected, Ethernet0/0
S*    0.0.0.0/0 [2/0] via 10.76.1.1

```



Note

The metric of the default route should be greater than 1 so that the default route that is added later by Easy VPN takes precedence and the traffic goes through the Easy VPN virtual-access interface.

Easy VPN “ezvpn2” Tunnel Is Up

```
Router# show crypto ipsec client ezvpn
```

```
Easy VPN Remote Phase: 6
```

```
Tunnel name : ezvpn1
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access2 (bound to Ethernet1/0)
Current State: CONNECT_REQUIRED
Last Event: TRACKED_OBJECT_UP
Save Password: Disallowed
Current EzVPN Peer: 10.75.1.2
```

```
Tunnel name : ezvpn2
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access3 (bound to Serial2/0)
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
DNS Ezvpn1: 10.6.0.2
NBMS/WINS Ezvpn1: 10.7.0.1
Default Domain: cisco.com
Save Password: Disallowed
Current EzVPN Peer: 10.75.2.2
```

```
Router# show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route
```

The gateway of last resort is 0.0.0.0 to network 0.0.0.0.

```
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
! The next line is the Easy VPN route.
S      10.75.2.2/32 [1/0] via 10.76.1.1
C      10.76.2.0/24 is directly connected, Serial2/0
C      10.76.1.0/24 is directly connected, Ethernet1/0
C      192.168.1.0/24 is directly connected, Ethernet0/0
! The next line is the Easy VPN route.
S*     0.0.0.0/0 [1/0] via 0.0.0.0, Virtual-Access3
```

One default route and one route to the peer is added as shown above.

Easy VPN “ezvpn2” Is Up and Easy VPN “ezvpn1” Is Initiated

```
Router# crypto ipsec client ezvpn connect ezvpn1
```

```
Router# show crypto ipsec cli ent ezvpn
```

```
Easy VPN Remote Phase: 6
```

```
Tunnel name : ezvpn1
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access2 (bound to Ethernet1/0)
Current State: READY
```

```
Last Event: CONNECT
Save Password: Disallowed
Current EzVPN Peer: 10.75.1.2
```

```
Tunnel name : ezvpn2
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access3 (bound to Serial2/0)
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
DNS Ezvpn1: 10.6.0.2
NBMS/WINS Ezvpn1: 10.7.0.1
Default Domain: cisco.com
Save Password: Disallowed
Current EzVPN Peer: 10.75.2.2
```

```
Router# show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route
```

The gateway of last resort is 10.0.0.0 to network 10.0.0.0.

```
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
S      10.75.2.2/32 [1/0] via 10.76.1.1
! The next line is the Easy VPN router.
S      10.75.1.2/32 [1/0] via 10.76.1.1
C      10.76.2.0/24 is directly connected, Serial2/0
C      10.76.1.0/24 is directly connected, Ethernet1/0
C      192.168.1.0/24 is directly connected, Ethernet0/0
S*    10.0.0.0/0 [1/0] via 10.0.0.0, Virtual-Access3
```

The route to 10.75.1.2 is added before the Easy VPN “ezvpn1” tunnel has come up. This route is for reaching the Easy VPN “ezvpn1” peer 10.75.1.2.

Both Tunnels Are Up

```
Router# show crypto ipsec client ezvpn
```

```
Easy VPN Remote Phase: 6
```

```
Tunnel name : ezvpn1
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access2 (bound to Ethernet1/0)
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
DNS Ezvpn1: 10.6.0.2
NBMS/WINS Ezvpn1: 10.7.0.1
Default Domain: cisco.com
Save Password: Disallowed
Split Tunnel List: 1
    Address      : 192.168.3.0
    Mask         : 255.255.255.255
    Protocol     : 0x0
    Source Port  : 0
    Dest Port    : 0
Current EzVPN Peer: 10.75.1.2
```

```
Tunnel name : ezvpn2
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access3 (bound to Serial2/0)
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
DNS Ezvpn1: 10.6.0.2
NBMS/WINS Ezvpn1: 10.7.0.1
Default Domain: cisco.com
Save Password: Disallowed
Current EzVPN Peer: 10.75.2.2
```

Router# **show ip route**

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

The gateway of last resort is 10.0.0.0 to network 10.0.0.0.

```
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
! The next line is the Easy VPN router (ezvpn2).
S    10.75.2.2/32 [1/0] via 10.76.1.1
! The next line is the Easy VPN router (ezvpn1).
S    10.75.1.2/32 [1/0] via 10.76.1.1
C    10.76.2.0/24 is directly connected, Serial2/0
C    10.76.1.0/24 is directly connected, Ethernet1/0
C    192.168.1.0/24 is directly connected, Ethernet0/0
! The next line is the Easy VPN route (ezvpn1).
S    192.168.3.0/24 [1/0] via 0.0.0.0, Virtual-Access2
! The next line is the Easy VPN (ezvpn2).
S*   10.0.0.0/0 [1/0] via 10.0.0.0, Virtual-Access3
```

The route to split tunnel “192.168.3.0/24” that points to Virtual-Access2 is added for the Easy VPN “ezvpn” tunnel as shown in the above **show** output.

Reactivate Primary Peer: Example

The following show output illustrates that the default primary peer feature has been activated. The primary default peer is 10.3.3.2.

Router# **show crypto ipsec client ezvpn**

```
Easy VPN Remote Phase: 6

Tunnel name : ezc
Inside interface list: Loopback0
Outside interface: Ethernet0/0
Current State: IPSEC_ACTIVE
Primary EzVPN Peer: 10.3.3.2, Last Tried: Dec 30 07:21:23.071
Last Event: CONN_UP
Address: 10.7.7.1
Mask: 255.255.255.255
DNS Primary: 10.1.1.1
NBMS/WINS Primary: 10.5.254.22
```

```

Save Password: Disallowed
Current EzVPN Peer: 10.4.4.2

23:52:44: %CRYPTO-6-EZVPN_CONNECTION_UP(Primary peer):
      User: lab, Group: hw-client-g
      Client_public_addr=10.4.22.103, Server_public_addr=10.4.23.112
      Assigned_client_addr=10.7.7.1

```

Identical Addressing Support Configuration: Example

In the following example, a Cisco router is configured for the Identical Addressing Support feature:

```

interface Virtual-Templat1 type tunnel
    no ip address
    ip nat outside
!
crypto ipsec client ezvpn easy
    connect manual
    group easy key work4cisco
    mode network-extension
    peer 10.2.2.2
    virtual-interface 1
    nat allow
    nat acl 100
!
interface Ethernet1
    ip address 10.0.0.1 255.255.255.0
    ip nat outside
    crypto ipsec client ezvpn easy
!
interface Ethernet0
    ip address 10.0.0.2 255.255.255.0
    ip nat inside
!
interface Loopback0
    ip address 10.1.1.1 255.255.255.252
    ip nat enable
crypto ipsec client ezvpn easy inside
!
ip access-list 100 permit ip 10.0.0.0 0.0.0.255 any
!
ip nat inside source list 100 interface Loopback0 overload
!
ip nat inside source static 10.5.5.5 1.1.1.101

```

cTCP on an Easy VPN Client (Remote Device): Examples

For configuration and troubleshooting examples, see the topic “cTCP on Cisco Easy VPN remote devices” in the [“Related Documents” section on page 101](#).

Easy VPN Server Configuration Examples

This section describes basic Cisco Easy VPN server configurations that support the Cisco Easy VPN remote configurations given in the previous sections. For complete information on configuring these servers, see [Easy VPN Server](#) for Cisco IOS Release 12.3(7)T, available on Cisco.com.

- [Cisco Easy VPN Server Without Split Tunneling: Example, page 96](#)
- [Cisco Easy VPN Server Configuration with Split Tunneling: Example, page 97](#)
- [Cisco Easy VPN Server Configuration with Xauth: Example, page 99](#)
- [Easy VPN Server Interoperability Support: Example, page 101](#)

Cisco Easy VPN Server Without Split Tunneling: Example

The following example shows the Cisco Easy VPN server that is the destination peer router for the Cisco Easy VPN remote network extension mode configurations shown earlier in this section. In addition to the other IPsec configuration commands, the **crypto isakmp client configuration group** command defines the attributes for the VPN group that was assigned to the Easy VPN remote router. This includes a matching key value (easy vpn remote password), and the appropriate routing parameters, such as DNS server, for the Easy VPN remotes.

To support the network extension mode of operation, the **ip route** command instructs that incoming packets for the 172.168.0.0 network be directed from the cable modem interface to the Cisco Easy VPN remote. Other **ip route** commands might be needed, depending on the topology of your network.



Note

This example shows a Cisco uBR925 cable access router, but typically the destination Easy VPN remote is a router, such as a Cisco VPN 3000 concentrator or a Cisco IOS router, that supports the Easy VPN Server feature.

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname uBR925Server
!
aaa new-model
!
!
aaa authorization network easy vpn remote-groupname local
aaa session-id common
!
!
clock timezone - 0 6
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 1
 authentication pre-share
 group 2
crypto isakmp client configuration address-pool local dynpool
!
crypto isakmp client configuration group easy vpn remote-groupname
 key easy vpn remote-password
 dns 172.16.0.250 172.16.0.251
 wins 172.16.0.252 172.16.0.253
 domain cisco.com
 pool dynpool
!
```



```

!
crypto ipsec transform-set transform-1 esp-des esp-sha-hmac
!
crypto dynamic-map dynmap 1
  set transform-set transform-1
  reverse-route
!
!
crypto map dynmap isakmp authorization list easy vpn remote-groupname
crypto map dynmap client configuration address respond
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!
!
interface Ethernet0
  ip address 172.16.0.129 255.255.255.128
!
interface cable-modem0
  no cable-modem compliant bridge
  crypto map dynmap
!
interface usb0
  no ip address
  arp timeout 0
!
ip local pool dynpool 172.16.0.65 172.16.0.127
ip classless
! Add the appropriate ip route commands for network-extension mode
ip route 172.16.1.0 255.255.255.248 cable-modem0
no ip http server
no ip http cable-monitor
!
snmp-server manager
!
line con 0
  exec-timeout 0 0
line vty 0 4
!
scheduler max-task-time 5000

```

Cisco Easy VPN Server Configuration with Split Tunneling: Example

The following example shows a Cisco Easy VPN server that is configured for a split tunneling configuration with a Cisco Easy VPN remote. This example is identical to that shown in the “[Cisco Easy VPN Server Without Split Tunneling: Example](#)” except for access list 150, which is assigned as part of the **crypto isakmp client configuration group** command. This access list allows the Cisco Easy VPN remote to use the server to access one additional subnet that is not part of the VPN tunnel without compromising the security of the IPsec connection.

To support network extension mode, the **ip route** command instructs that incoming packets for the 172.168.0.0 network be directed from the cable modem interface to the Cisco Easy VPN remote. Other **ip route** commands might be necessary, depending on the topology of your network.



Note

This example shows a Cisco uBR925 cable access router, but typically the destination Easy VPN remote will be a router, such as a VPN 3000 concentrator or a Cisco IOS router, that supports the Easy VPN Server feature.

```

version 12.2
no service pad
service timestamps debug uptime

```

```

service timestamps log uptime
no service password-encryption
service internal
!
hostname uBR925Server
!
aaa new-model
!
!
aaa authorization network easy vpn remote-groupname local
aaa session-id common
!
!
clock timezone - 0 6
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 1
  authentication pre-share
  group 2
crypto isakmp client configuration address-pool local dynpool
!
crypto isakmp client configuration group easy vpn remote-groupname
  key easy vpn remote-password
  dns 172.16.0.250 172.16.0.251
  wins 172.16.0.252 172.16.0.253
  domain cisco.com
  pool dynpool
acl 150
!
!
crypto ipsec transform-set transform-1 esp-des esp-sha-hmac
!
crypto dynamic-map dynmap 1
  set transform-set transform-1
  reverse-route
!
!
crypto map dynmap isakmp authorization list easy vpn remote-groupname
crypto map dynmap client configuration address respond
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!
!
interface Ethernet0
  ip address 172.16.0.129 255.255.255.255
!
interface cable-modem0
  no cable-modem compliant bridge
  crypto map dynmap
!
interface usb0
  no ip address
  arp timeout 0
!
ip local pool dynpool 172.16.0.65 172.16.0.127
ip classless
! Add the appropriate ip route commands for network-extension mode
ip route 172.16.1.0 255.255.255.255 cable-modem0
no ip http server
no ip http cable-monitor
!
access-list 150 permit ip 172.16.0.128 10.0.0.127 any

```

```
snmp-server manager
!
line con 0
  exec-timeout 0 0
line vty 0 4
!
scheduler max-task-time 5000
end
```

Cisco Easy VPN Server Configuration with Xauth: Example

The following example shows a Cisco Easy VPN server configured to support Xauth with the Cisco Easy VPN Remote feature. This example is identical to that shown in the “[Cisco Easy VPN Server Configuration with Split Tunneling: Example](#)” except for the following commands that enable and configure Xauth:

- **aaa authentication login userlist local**—Specifies the local username database for authentication at login time. You could also specify the use of RADIUS servers by first using the **aaa authentication login userlist group radius** command and then by specifying the RADIUS servers using the **aaa group server radius** command.
- **crypto isakmp xauth timeout**—Specifies the amount of time, in seconds, that the user has to enter the appropriate username and password to authenticate the session.
- **crypto map dynmap client authentication list userlist**—Creates a crypto map named “**dynmap**” that enables Xauth.
- **username cisco password 7 cisco**—Creates an entry in the local username database for a user with the username of “**cisco**” and an encrypted password of “**cisco**.” This command should be repeated for each separate user that accesses the server.

The following commands, which are also present in the non-Xauth configurations, are also required for Xauth use:

- **aaa authorization network easy vpn remote-groupname local**—Requires authorization for all network-related service requests for users in the group named “**easy vpn remote-groupname**” using the local username database.
- **aaa new-model**—Specifies that the router should use the new AAA authentication commands.
- **aaa session-id common**—Specifies that a unique and common session ID should be used for AAA sessions.
- **crypto map dynmap 1 ipsec-isakmp dynamic dynmap**—Specifies that IKE should be used to establish the IPsec SAs, using the crypt map named “**dynmap**” as the policy template.
- **crypto map dynmap client configuration address respond**—Enables IKE negotiation, accepting requests from any requesting peers.
- **crypto map dynmap isakmp authorization list easy vpn remote-groupname**—Configures the crypto map named “**dynmap**” to use IKE Shared Secret using the group named “**easy vpn remote-groupname**.”



Tip

This configuration shows the server configured for split tunneling, but Xauth can also be used with nonsplit tunnel configurations as well.

**Note**

This example shows a Cisco uBR925 cable access router, but typically the destination Easy VPN server is a router such as a VPN 3000 concentrator or a Cisco IOS router that supports the Easy VPN Server feature.

```

version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname uBR925Server
!
aaa new-model
!
!
aaa authentication login userlist local
aaa authorization network easy vpn remote-groupname local
aaa session-id common
!
username cisco password 7 cisco
!
!
clock timezone - 0 6
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 1
  authentication pre-share
  group 2
crypto isakmp client configuration address-pool local dynpool
crypto isakmp xauth timeout 60
!
crypto isakmp client configuration group easy vpn remote-groupname
  key easy vpn remote-password
  dns 172.16.0.250 172.16.0.251
  wins 172.16.0.252 172.16.0.253
  domain cisco.com
  pool dynpool
  acl 150
!
!
crypto ipsec transform-set transform-1 esp-des esp-sha-hmac
!
crypto dynamic-map dynmap 1
  set transform-set transform-1
  reverse-route
!
!
crypto map dynmap client authentication list userlist
crypto map dynmap isakmp authorization list easy vpn remote-groupname
crypto map dynmap client configuration address respond
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!!
!
interface Ethernet0
  ip address 172.16.0.129 255.255.255.128
!
interface cable-modem0

```

```

no cable-modem compliant bridge
crypto map dynmap
!
interface usb0
no ip address
arp timeout 0
!
ip local pool dynpool 172.16.0.65 172.16.0.127
ip classless
ip route 172.16.1.0 255.255.255.248 cable-modem0
no ip http server
no ip http cable-monitor
!
access-list 150 permit ip 172.16.0.128 0.0.0.127 any
snmp-server manager
!
line con 0
exec-timeout 0 0
line vty 0 4
!
scheduler max-task-time 5000
end

```

Easy VPN Server Interoperability Support: Example

For information about this feature, see “General information on IPSec and VPN” in the section “[Additional References](#)” (*Managing VPN Remote Access*).

Additional References

The following sections provide references related to Cisco Easy VPN Remote.

Related Documents

Related Topic	Document Title
Platform-specific documentation	
Cisco 800 series routers	<ul style="list-style-type: none"> • Cisco 800 Series Routers • Cisco 806 Router and SOHO 71 Router Hardware Installation Guide • Cisco 806 Router Software Configuration Guide • Cisco 826, 827, 828, 831, 836, and 837 and SOHO 76, 77, 78, 91, 96, and 97 Routers Software Configuration Guide • Cisco 826 and SOHO 76 Router Hardware Installation Guide • Cisco 827 and SOHO 77 Routers Hardware Installation Guide • Cisco 828 and SOHO 78 Routers Hardware Installation Guide • Cisco 837 ADSL Broadband Router

Related Topic	Document Title
Cisco uBR905 and Cisco uBR925 cable access routers	<ul style="list-style-type: none"> • Cisco uBR925 Cable Access Router Hardware Installation Guide • Cisco uBR905 Hardware Installation Guide • Cisco uBR905/uBR925 Cable Access Router Software Configuration Guide • Cisco uBR905 Cable Access Router Subscriber Setup Quick Start Card • Cisco uBR925 Cable Access Router Subscriber Setup Quick Start Card • Cisco uBR925 Cable Access Router Quick Start User Guide
Cisco 1700 series routers	<ul style="list-style-type: none"> • Cisco 1700 Series Router Software Configuration Guide • Cisco 1710 Security Router Hardware Installation Guide • Cisco 1710 Security Router Software Configuration Guide • Cisco 1711 Security Access Router • Cisco 1720 Series Router Hardware Installation Guide • Cisco 1721 Access Router Hardware Installation Guide • Cisco 1750 Series Router Hardware Installation Guide • Cisco 1751 Router Hardware Installation Guide • Cisco 1751 Router Software Configuration Guide • Cisco 1760 Modular Access Router Hardware Installation Guide <p>Also see the Cisco IOS release notes for Cisco IOS Release 12.2(4)YA:</p> <ul style="list-style-type: none"> • SOHO 70 and Cisco 800 Series—Release Notes for Release 12.2(4)YA • Release Notes for Cisco uBR905 and Cisco uBR925 Cable Access Routers for Cisco IOS Release 12.2 YA • Cisco 1700 Series—Release Notes for Release 12.2(4)YA
Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers	<ul style="list-style-type: none"> • Cisco 2600 Series Multiservice Platforms • Cisco 2600 Series Routers Hardware Installation Guide • Cisco 3600 Series Multiservice Platforms • Cisco 3600 Series Hardware Installation Guide • Cisco 3700 Series Multiservice Access Routers • Cisco 3700 Series Routers Hardware Installation Guide • Cisco 2600 Series, 3600 Series, and 3700 Series Regulatory Compliance and Safety Information on Cisco.com
IPsec and VPN documentation	

Related Topic	Document Title
802.1x authentication	<ul style="list-style-type: none"> • Configuring Cisco IOS Easy VPN Remote with 802.1X Authentication (white paper) • VPN Access Control Using 802.1X Local Authentication
Access control lists, configuring	<ul style="list-style-type: none"> • Access Control Lists: Overview and Guidelines
Configuration information (additional in-depth)	<ul style="list-style-type: none"> • Cisco Easy VPN Solutions—Provides white papers and examples for configuring Cisco IOS Easy VPN in network extension mode. • Cisco IOS Security Command Reference—Provides a reference for each of the Cisco IOS commands used to configure IPsec encryption and related security features. • SSL VPN—Provides information about SSL VPN.
cTCP on Cisco Easy VPN remote devices	<ul style="list-style-type: none"> • EFT Deployment Guide for Cisco Tunnel Control Protocol on Cisco EasyVPN
Dead peer detection	<ul style="list-style-type: none"> • IPSec Dead Peer Detection Periodic Message Option
DHCP, configuring	<ul style="list-style-type: none"> • Configuring DHCP • “Configuring the Cisco IOS DHCP Client” in the Cisco IOS IP Configuration Guide
Digital certificates (RSA signature support)	<ul style="list-style-type: none"> • Easy VPN Remote RSA Signature Support
DNS, configuring	<ul style="list-style-type: none"> • Configuring DNS and Configuring DNS on Cisco Routers
Easy VPN Server feature, which provides Cisco Unity client support for the Cisco Easy VPN Remote feature	<ul style="list-style-type: none"> • Easy VPN Server • Cisco Easy VPN • Configuring NAC with IPsec Dynamic Virtual Tunnel Interface
Encrypted Preshared Key feature	<ul style="list-style-type: none"> • Encrypted Preshared Key

Related Topic	Document Title
IPsec and VPN, general information	<ul style="list-style-type: none"> • <i>Deploying IPsec</i>—Provides an overview of IPsec encryption and its key concepts, along with sample configurations. Also provides a link to many other documents on related topics. • <i>Configuring Authorization and Revocation of Certificates in a PKI</i>—Describes the concept of digital certificates and how they are used to authenticate IPsec users. • <i>Configuring Authentication Proxy</i> • <i>An Introduction to IP Security (IPsec) Encryption</i>—Provides a step-by-step description of how to configure IPsec encryption. • <i>Managing VPN Remote Access</i>—Describes how to configure the Cisco PIX firewall as an Easy VPN server and how to configure Easy VPN remote software clients. • <i>Configuring VPN Settings</i>—Provides information about configuring a PIX firewall to operate as a Cisco Secure VPN client. • <i>Configuring Security for VPNs with IPSec</i>—Provides information about configuring crypto maps. • <i>IPSec Virtual Tunnel Interface</i>—Provides information about IPsec virtual tunnel interfaces. • IP technical tips sections on Cisco.com.
Object tracking	<ul style="list-style-type: none"> • <i>Reliable Static Routing Backup Using Object Tracking</i>
Note Additional documentation on IPsec becomes available on Cisco.com as new features and platforms are added. Cisco Press also publishes several books on IPsec—go to http://www.ciscopress.com for more information on Cisco Press books.	

Standards

Standards	Title
No new or modified standards are supported by this feature.	—

MIBs

MIBs	MIBs Link
<ul style="list-style-type: none">CISCO-IPSEC-FLOW-MONITOR-MIB—Contains attributes describing IPsec-based VPNs (Internet Engineering Task Force (IETF) IPsec Working Group Draft).CISCO-IPSEC-MIB—Describes Cisco implementation-specific attributes for Cisco routers implementing IPsec VPNs.CISCO-IPSEC-POLICY-MAP-MIB—Extends the CISCO-IPSEC-FLOW-MONITOR-MIB to map dynamically created structures to the policies, transforms, cryptomaps, and other structures that created or are using them.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html

For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html.

- **ctcp port**
- **clear crypto ipsec client ezvpn**
- **crypto ctp**
- **crypto ipsec client ezvpn (global)**
- **crypto ipsec client ezvpn (interface)**
- **crypto ipsec client ezvpn connect**
- **crypto ipsec client ezvpn xauth**
- **debug crypto ipsec client ezvpn**
- **debug ip auth-proxy ezvpn**
- **icmp-echo**
- **ip http ezvpn**
- **show crypto ipsec client ezvpn**
- **show tech-support**
- **type echo protocol ipIcmpEcho**
- **xauth userid mode**

Feature Information for Easy VPN Remote

Table 4 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Note

Table 4 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 4 Feature Information for Easy VPN Remote

Feature Name	Releases	Feature Information
Easy VPN Remote	12.2(4)YA Cisco IOS XE Release 2.1	Support for Cisco Easy VPN Remote (Phase I) of this feature was introduced for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers. In Cisco IOS XE Release 2.1, support for this feature was introduced on Cisco ASR 1000 Series Routers.
	12.2(13)T	Cisco Easy VPN Remote was integrated into Cisco IOS Release 12.2(13)T.
	12.2(8)YJ	Support for Cisco Easy VPN Remote (Phase II) of this feature was introduced for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
	12.2(15)T	The Cisco Easy VPN Remote (Phase II) feature was integrated into Cisco IOS Release 12.2(15)T. Support for the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers was added.
	12.3(2)T	The Type 6 Password in the IOS Configuration feature was added.
	12.3(4)T	The Save Password and Multiple Peer Backup features were added. The following sections provide information about the Save Password feature: <ul style="list-style-type: none"> • Using Xauth, page 9 • Configuring Save Password, page 39 • Save Password Configuration: Example, page 77

Table 4 *Feature Information for Easy VPN Remote (continued)*

Feature Name	Releases	Feature Information
	12.3(7)T	<p>The following feature was introduced in this release:</p> <ul style="list-style-type: none"> • Dead Peer Detection Periodic Message Option, page 24
	12.3(7)XR	<p>The following features were introduced: Dead Peer Detection with Stateless Failover (Object Tracking with Easy VPN)—Backup Server List Local Configuration and Backup Server List Auto Configuration, Management Enhancements, Load Balancing, VLAN Support, Multiple Subnet Support, Traffic-Triggered Activation, Perfect Forward Secrecy (PFS) Via Policy Push, 802.1x Authentication, Certificate (PKI) Support, Easy VPN Remote and Server on the Same Interface, and Easy VPN Remote and Site to Site on the Same Interface.</p> <p>The following sections provide information about these features:</p> <ul style="list-style-type: none"> • 802.1x Authentication, page 16 • Traffic-Triggered Activation, page 17 • Backup Server List Local Configuration, page 18 • Backup Server List Auto Configuration, page 18 • VLAN Support, page 21 • Easy VPN Remote and Server on the Same Interface, page 23 • Easy VPN Remote and Site to Site on the Same Interface, page 23 • Load Balancing, page 24 • Management Enhancements, page 25 • PFS Support, page 25 <p>Note Cisco 800 series routers are not supported in Cisco IOS Release 12.3(7)XR.</p> <p>Note These features are available only in Cisco Release 12.3(7)XR2.</p>
	12.3(7)XR2	<p>The features in Cisco IOS Release 12.3(7)XR were introduced on Cisco 800 series routers.</p>
	12.3(8)YH	<p>The Dial Backup, Traffic-Triggered Activation, and Web-Based Activation features were introduced on the Cisco 1812 router.</p> <p>The following sections provide information about these features:</p> <ul style="list-style-type: none"> • Dial Backup, page 25 • Dial Backup: Examples, page 78

Table 4 *Feature Information for Easy VPN Remote (continued)*

Feature Name	Releases	Feature Information
	12.3(11)T	Except for the Dial Backup and Traffic-Triggered Activation features, all features introduced in Cisco IOS Releases 12.3(7)XR and 12.3(7)XR2 were integrated into Cisco IOS Release 12.3(11)T.
	12.3(14)T	Dial Backup and Traffic-Triggered Activation features were integrated into Cisco IOS Release 12.3(14)T. In addition, the Web-Based Activation feature was integrated into this release.
	12.3(8)YI	The Dial Backup, Traffic-Triggered Activation, and Web-Based Activation features were introduced on the Cisco 1800 series fixed configuration routers.
	12.3(8)YI1	The Dial Backup, Traffic-Triggered Activation, and Web-Based Activation features were introduced on the Cisco 870 series routers.
	12.4(2)T 12.2(33)SXH	<p>The following features were added in this release: Banner, Auto-Update, and Browser-Proxy Enhancements.</p> <p>The following section provides information about these features:</p> <ul style="list-style-type: none"> • Banner, page 32
	12.4(4)T 12.2(33)SXH	<p>The following features were added in this release: Dual Tunnel Support, Configuration Management Enhancements (Pushing a Configuration URL Through a Mode-Configuration Exchange), Reactivate Primary Peer, and Virtual IPsec Interface Support.</p> <p>The following sections provide information about these features:</p> <ul style="list-style-type: none"> • Virtual IPsec Interface Support, page 27 • Dual Tunnel Support, page 29 • Configuration Management Enhancements (Pushing a Configuration URL Through a Mode-Configuration Exchange), page 33 • Reactivate Primary Peer, page 33
	12.2(33)SRA	Cisco Easy VPN Remote was integrated into Cisco IOS Release 12.2(33)SRA.
	12.4(11)T	<p>The following feature was added in this release:</p> <ul style="list-style-type: none"> • Identical Addressing Support <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> – Identical Addressing Support, page 33

Table 4 *Feature Information for Easy VPN Remote (continued)*

Feature Name	Releases	Feature Information
	12.4(20)T	<p>The following features were added in this release:</p> <ul style="list-style-type: none"> • cTCP Support on Easy VPN Clients <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> – cTCP Support on Easy VPN Clients, page 34 – Configuring cTCP on an Easy VPN Client, page 56 – cTCP on an Easy VPN Client (Remote Device): Examples, page 95 <p>The following commands were introduced or modified for this feature: crypto ctcp, ctcp port</p>

Glossary

AAA—authentication, authorization, and accounting. Framework of security services that provide the method for identifying users (authentication); for remote access control (authorization); and for collecting and sending security server information used for billing, auditing, and reporting (accounting).

aggressive mode—Mode that eliminates several steps during Internet Key Exchange (IKE) authentication negotiation between two or more IPsec peers. Aggressive mode is faster than main mode but is not as secure.

authorization—Method for remote access control, including one-time authorization or authorization for each service; per-user account list and profile; user group support; and support of IP, IPX, ARA, and Telnet. AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared to the information contained in a database for a given user and the result is returned to AAA to determine the actual capabilities and restrictions of the user. The database can be located locally on the access server or router, or it can be hosted remotely on a RADIUS or TACACS+ security server. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights, with the appropriate user. All authorization methods must be defined through AAA.

CA—certificate authority. An entity in a network that issues and manages security credentials and public keys (in the form of X509v3 certificates) for message encryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the information of the requestor, the CA can then issue a certificate. Certificates generally include the public key of the owner, the expiration date of the certificate, the name of the owner, and other information about the public key owner.

CRWS—Cisco Router Web Setup Tool. Tool that provides web interface capabilities.

cTCP—Cisco Tunneling Control Protocol. When cTCP is enabled on a remote device (client) and headend device, IKE and ESP (Protocol 50) traffic is encapsulated in the TCP header so that the firewalls in between the client and the headend device permits this traffic (considering it the same as TCP traffic).

DPD—dead peer detection. Queries the liveliness of the Internet Key Exchange (IKE) peer of a router at regular intervals.

DSLAM—digital subscriber line access multiplexer. A device that connects many digital subscriber lines to a network by multiplexing the DSL traffic onto one or more network trunk lines.

IKE—Internet Key Exchange. Key management protocol standard that is used in conjunction with the IP Security (IPsec) standard. IPsec is an IP security feature that provides robust authentication and encryption of IP packets. IPsec can be configured without IKE, but IKE enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard. IKE is a hybrid protocol that implements the Oakley key exchange and Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.

IPsec—IP Security Protocol. Framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer. IPsec uses IKE to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPsec. IPsec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

main mode—Mode that ensures the highest level of security when two or more IPsec peers are negotiating IKE authentication. It requires more processing time than aggressive mode.

MIB—Management Information Base. Database of network management information that is used and maintained by a network management protocol, such as Simple Network Management Protocol (SNMP) or Common Management Information Protocol (CMIP). The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a graphical user interface (GUI) network management system (NMS). MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

peer—Router or device that participates as an endpoint in IPsec and IKE.

preshared key—Shared, secret key that uses IKE for authentication.

QoS—quality of service. Capability of a network to provide better service to selected network traffic over various technologies, including Frame Relay; Asynchronous Transfer Mode (ATM); Ethernet; and 802.1 networks, SONET, and IP-routed networks that may use any or all of these underlying technologies.

RADIUS—Remote Authentication Dial-In User Service. Distributed client or server system that secures networks against unauthorized access. RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

SA—security association. Instance of security policy and keying material applied to a data flow. Both IKE and IPsec use SAs, although SAs are independent of one another. IPsec SAs are unidirectional, and they are unique in each security protocol. An IKE SA is used by IKE only, and unlike the IPsec SA, it is bi-directional. IKE negotiates and establishes SAs on behalf of IPsec. A user can also establish IPsec SAs manually.

A set of SAs are needed for a protected data pipe, one per direction per protocol. For example, if you have a pipe that supports encapsulating security payload (ESP) between peers, one ESP SA is required for each direction. SAs are uniquely identified by destination (IPsec endpoint) address, security protocol (AH or ESP), and security parameter index (SPI).

SDM—Security Device Manager. Web interface manager that enables you to connect or disconnect a VPN tunnel and that provides a web interface for extended authentication (Xauth).

SNMP—Simple Network Management Protocol. Application-layer protocol that provides a message format for communication between SNMP managers and agents.

trap—Message sent by an SNMP agent to a network management system, console, or terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached.

VPN—virtual private network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses tunnels to encrypt all information at the IP level.

**Note**

See [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0805).

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.



Cisco Group Encrypted Transport VPN

First Published: November 17, 2006

Last Updated: August 20, 2008



Note

Effective with Cisco IOS 12.4(11)T, the Multicast Rekeying feature information (originally published as Cisco IOS Release 12.4(6)T [titled [Secure Multicast](#)]) has been integrated into this document.

Today's networked applications, such as voice and video, are accelerating the need for instantaneous, branch-interconnected, and Quality of Service- (QoS-) enabled WANs. The distributed nature of these applications results in increased demands for scale. At the same time, enterprise WAN technologies force businesses to trade off between QoS-enabled branch interconnectivity and transport security. As network security risks increase and regulatory compliance becomes essential, Cisco Group Encrypted Transport VPN (GET VPN) eliminates the need to compromise between network intelligence and data privacy.

GET VPN eliminates the need for tunnels. By removing the need for point-to-point tunnels, meshed networks are able to scale higher while maintaining network-intelligence features that are critical to voice and video quality, such as QoS, routing, and multicast. GET VPN offers a new standards-based IP security (IPsec) security model that is based on the concept of "trusted" group members. Trusted member routers use a common security methodology that is independent of any point-to-point IPsec tunnel relationship.

GET VPN is a set of features that are necessary to secure IP multicast group traffic or unicast traffic over a private WAN that originates on or flows through a Cisco IOS device. GET VPN combines the keying protocol Group Domain of Interpretation (GDOI) with IPsec encryption to provide users with an efficient method to secure IP multicast traffic or unicast traffic. GET VPN enables the router to apply encryption to nontunneled (that is, "native") IP multicast and unicast packets and eliminates the requirement to configure tunnels to protect multicast and unicast traffic.

Cisco Group Encrypted Transport VPN provides the following benefits:

- Provides data security and transport authentication, helping to meet security compliance and internal regulation by encrypting all WAN traffic
- Enables high-scale network meshes and eliminates complex peer-to-peer key management with group encryption keys
- For Multiprotocol Label Switching (MPLS) networks, maintains network intelligence (such as full-mesh connectivity, natural routing path, and QoS)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008 Cisco Systems, Inc. All rights reserved.

- Grants easy membership control with a centralized key server
- Helps ensure low latency and jitter by enabling full-time, direct communications between sites, without requiring transport through a central hub
- Reduces traffic loads on customer premises equipment (CPE) and provider-edge (PE) encryption devices by using the core network for replication of multicast traffic, avoiding packet replication at each individual peer site

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Information About Cisco Group Encrypted Transport VPN](#)” section on [page 3](#).

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Cisco Group Encrypted Transport VPN, page 2](#)
- [Restrictions for Cisco Group Encrypted Transport VPN, page 3](#)
- [Information About Cisco Group Encrypted Transport VPN, page 3](#)
- [How to Configure Cisco Group Encrypted Transport VPN, page 20](#)
- [Configuration Examples for Cisco Group Encrypted Transport VPN, page 40](#)
- [Additional References, page 47](#)
- [Command Reference, page 48](#)
- [Feature Information for Cisco Group Encrypted Transport VPN, page 49](#)
- [Glossary, page 50](#)
- [Appendix I: System Messages, page 51](#)

Prerequisites for Cisco Group Encrypted Transport VPN

- You must be using Cisco IOS Release 12.4(11)T.
- The following Cisco VPN acceleration modules are supported:
 - Cisco AIM-VPN/SSL Module for Cisco integrated services routers
 - Cisco VPN acceleration Module 2+ for Cisco 7200 series routers and 7301 routers
 - Cisco VSA (high-performance crypto engine) for Cisco 7200VXR/NPE-G2 routers
- You should be knowledgeable about IPsec and Internet Key Exchange (IKE).
- You should know how to configure multicast and unicast routing on a Cisco IOS global router.

- When configuring the IKE policy, the IKE lifetime should be set to the minimum of 5 minutes so that unnecessary resources are not wasted on the maintenance of the IKE security association (SA). After the registration IKE SA is established, the registration SAs no longer have to be maintained because the rekey SA has been created and will be used to accept future rekeys.

Restrictions for Cisco Group Encrypted Transport VPN

- The following platforms can be configured only as shown:
 - Cisco 870 series routers: as a group member only.
 - Cisco VSA does not support time-based anti-replay in 12.4(15)T5.
- If you are encrypting high packet rates for counter-based anti-replay, ensure that you do not make the lifetime too long or it can take several hours for the sequence number to wrap. For example, if the packet rate is 100 kilopackets per second, the lifetime should be configured as less than 11.93 hours so that the SA is used before the sequence number wraps.
- For unicast traffic and counter-based anti-replay, the sequence numbers may be out of sync between the group members if one of the group members goes down and comes back up (for example: There is traffic from Group Member 1 to Group Member 2, and the last sequence number is x. Group Member 1 goes down and comes back up. The sequence number of the Security Association (SA) at Group Member 1 now starts with 1, but Group Member 2 is expecting continuation from the previous sequence number (x+1). This situation causes subsequent traffic from Group Member 1 to be dropped until the sequence number on Group Member 1 reaches x or the next rekey.
- The Cisco VSA feature introduced in Cisco IOS Release 12.4(15)T5 does not support time-based anti-replay.
- If you are overriding the don't fragment bit (df-bit) setting in the IP header of encapsulated packets, you must configure the override commands in global configuration mode. GET VPN does not honor the interface configuration.

**Note**

This restriction is limited only to GET VPN. IPsec still honors both global configuration- and interface-specific override commands.

Because Path MTU Discovery (PMTUD) does not work for GET VPN, there is a possibility that encapsulated packets could be dropped when the df-bit is set and the MTU of an intermediate link is less than the size of the encapsulated packet. In such an event, the router that drops the packet sends a notification to the source IP address on the packet, indicating that the packet has been dropped because the router could not fragment the packet due to the df-bit setting. In GET VPN, this message goes past the encapsulating endpoint directly to the source of the data due to the header preservation feature of GET VPN. Thus, the encapsulating router never knows that it has to fragment the packet to a smaller size before setting the df-bit after encapsulation. It continues to set the df-bit on the packets and they continue to be dropped at the intermediate router. (This is known as blackholing the traffic.)

Information About Cisco Group Encrypted Transport VPN

To configure GET VPN, you should understand the following concepts:

- [Cisco Group Encrypted Transport VPN Overview, page 4](#)

- [Cisco Group Encrypted Transport VPN Architecture, page 4](#)
- [Cisco Group Encrypted Transport VPN Features, page 11](#)
- [End-User Considerations, page 19](#)
- [System Error Messages, page 20](#)

Cisco Group Encrypted Transport VPN Overview

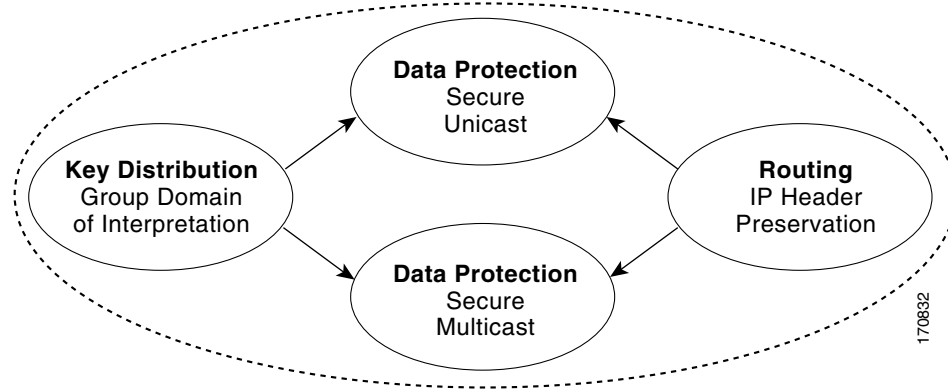
Today's networked applications, such as voice and video, are accelerating the necessity for instantaneous, branch-interconnected, and QoS-enabled WANs. And the distributed nature of these applications results in increased demands for scale. At the same time, enterprise WAN technologies force businesses to trade off between QoS-enabled branch interconnectivity and transport security. As network security risks increase and regulatory compliance becomes essential, GET VPN, a next-generation WAN encryption technology, eliminates the need to compromise between network intelligence and data privacy.

With the introduction of GET, Cisco now delivers a new category—tunnel-less VPN—that eliminates the need for tunnels. By removing the need for point-to-point tunnels, meshed networks can scale higher while maintaining network-intelligence features critical to voice and video quality. GET offers a new standards-based security model that is based on the concept of “trusted” group members. Trusted member routers use a common security methodology that is independent of any point-to-point IPsec tunnel relationship. By using trusted groups instead of point-to-point tunnels, “any-any” networks can scale higher while maintaining network-intelligence features (such as QoS, routing, and multicast), which are critical to voice and video quality.

GET-based networks can be used in a variety of WAN environments, including IP and Multiprotocol Label Switching (MPLS). MPLS VPNs that use this encryption technology are highly scalable, manageable, and cost-effective, and they meet government-mandated encryption requirements. The flexible nature of GET allows security-conscious enterprises either to manage their own network security over a service provider WAN service or to offload encryption services to their providers. GET simplifies securing large Layer 2 or MPLS networks that require partial or full-mesh connectivity.

Cisco Group Encrypted Transport VPN Architecture

GET VPN is an enhanced solution that encompasses Multicast Rekeying, a Cisco solution for enabling encryption for “native” multicast packets, and unicast rekeying over a private WAN. Multicast Rekeying and GET VPN is based on GDOI as defined in Internet Engineering Task Force (IETF) RFC 3547. In addition, there are similarities to IPsec in the area of header preservation and SA lookup. Dynamic distribution of IPsec SAs has been added, and tunnel overlay properties of IPsec have been removed. [Figure 1](#) further illustrates the concepts of GET VPN and their relationships among one another.

Figure 1 GET VPN Concepts and Relationships

This section includes the following subsections:

- [Key Distribution: Group Domain of Interpretation, page 5](#)
- [Routing, page 9](#)
- [Secure Data Plane Multicast, page 9](#)
- [Secure Data Plane Unicast, page 10](#)

Key Distribution: Group Domain of Interpretation

GDOI

GDOI is defined as the Internet Security Association Key Management Protocol (ISAKMP) Domain of Interpretation (DOI) for group key management. In a group management model, the GDOI protocol operates between a group member and a group controller or key server (GCKS), which establishes security associations (SAs) among authorized group members. The ISAKMP defines two phases of negotiation. GDOI is protected by a Phase 1 ISAKMP security association. The Phase 2 exchange is defined in IETF RFC 3547. The topology shown in [Figure 2](#) and the corresponding explanation show how this protocol works.

Group Member

The group member registers with the key server to get the IPsec SA or SAs that are necessary to communicate with the group. The group member provides the group ID to the key server to get the respective policy and keys for this group. These keys are refreshed periodically, and before the current IPsec SAs expire, so that there is no loss of traffic.

Key Server

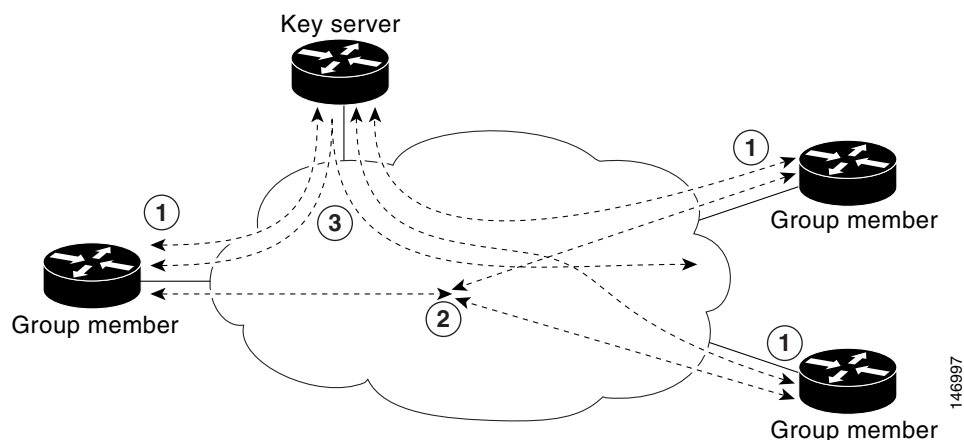
The responsibilities of the key server include maintaining the policy and creating and maintaining the keys for the group. When a group member registers, the key server downloads this policy and the keys to the group member. The key server also rekeys the group before existing keys expire.

The key server has two modes: servicing registration requests and sending rekeys. A group member can register at any time and receive the most current policy and keys. When a group member registers with the key server, the key server verifies the group ID that the group member is attempting to join. If this ID is a valid group ID, the key server sends the SA policy to the group member. After the group member acknowledges that it can handle the downloaded policy, the key server downloads the respective keys.

There are two types of keys that the key server can download: the key encryption key (KEK) and the traffic encryption key (TEK). The TEK becomes the IPsec SA with which the group members within the same group communicate. The KEK encrypts the rekey message.

The GDOI server sends out rekey messages either because of an impending IPsec SA expiration or because the policy has changed on the key server (using command-line interface [CLI]). The rekey messages may also be retransmitted periodically to account for possible packet loss. Packet loss can occur because rekey messages are sent without the use of any reliable transport. There is no efficient feedback mechanism by which receivers can indicate that they did not receive a rekey message, so retransmission seeks to bring all receivers up to date.

Figure 2 *Protocol Flows That Are Necessary for Group Members to Participate in a Group*



The above topology shows the protocol flows that are necessary for group members to participate in a group, which are as follows:

1. Group members register with the key server. The key server authenticates and authorizes the group members and downloads the IPsec policy and keys that are necessary for them to encrypt and decrypt IP multicast packets.
2. Group members exchange IP multicast packets that are encrypted using IPsec.
3. As needed, the key server “pushes” a rekey message to the group members. The rekey message contains new IPsec policy and keys to use when old IPsec SAs expire. Rekey messages are sent in advance of the SA expiration time to ensure that valid group keys are always available.

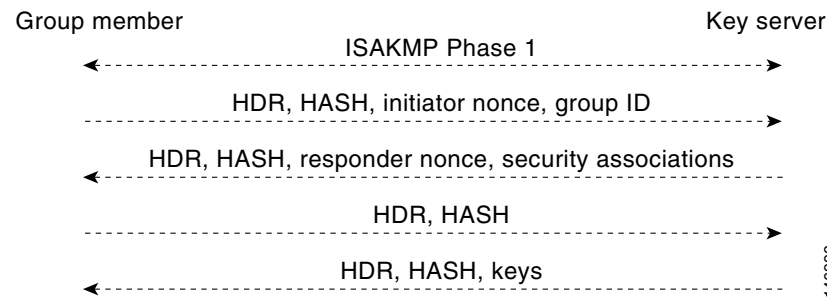
How Protocol Messages Work with the Cisco IOS

Multicast Rekeying uses the GDOI protocol (IETF RFC 3547) to distribute the policy and keys for the group. The GDOI protocol is between a key server and a group member. The key server creates and maintains the policy and keys, and it downloads the policy and keys to the authenticated group members. The group members are authenticated by the key server and communicate with other authenticated group members that are in the same group using the IPsec SAs that the group members have received from the key server.

The GDOI protocol is protected by an ISAKMP Phase 1 exchange. The GDOI key server and the GDOI group member must have the same ISAKMP policy. This Phase 1 ISAKMP policy should be strong enough to protect the GDOI protocol that follows. The GDOI protocol is a four-message exchange that follows the Phase 1 ISAKMP policy. The Phase 1 ISAKMP exchange can occur in main mode or aggressive mode.

Figure 3 shows the ISAKMP Phase 1 exchange.

Figure 3 ISAKMP Phase 1 Exchange and GDOI Registration



The above messages (the ISAKMP Phase 1 messages and the four GDOI protocol messages) are referred to as the GDOI registration, and the entire exchange that is shown above is a unicast exchange between the group member and the key server.

After the registration is successful, the key server sends a multicast rekey to all the group members that have registered within a group. During the registration, the group member receives the address of the multicast group and registers with the multicast group that is required to receive the multicast rekeys.



Note

The GDOI protocol uses User Datagram Protocol (UDP) port 848 (with Network Address Translation-Traversal (NAT-T), it floats to 4500).

IPsec

IPsec is a well-known RFC that defines an architecture to provide various security services for traffic at the IP layer. The components and how they fit together with each other and into the IP environment are described in IETF RFC 2401.

Communication Flow Between Key Servers and Group Members to Update IPsec SAs

Key servers and group members are the two components of the GET VPN architecture. The key server holds and supplies group authentication keys and IPsec SAs to the group members.

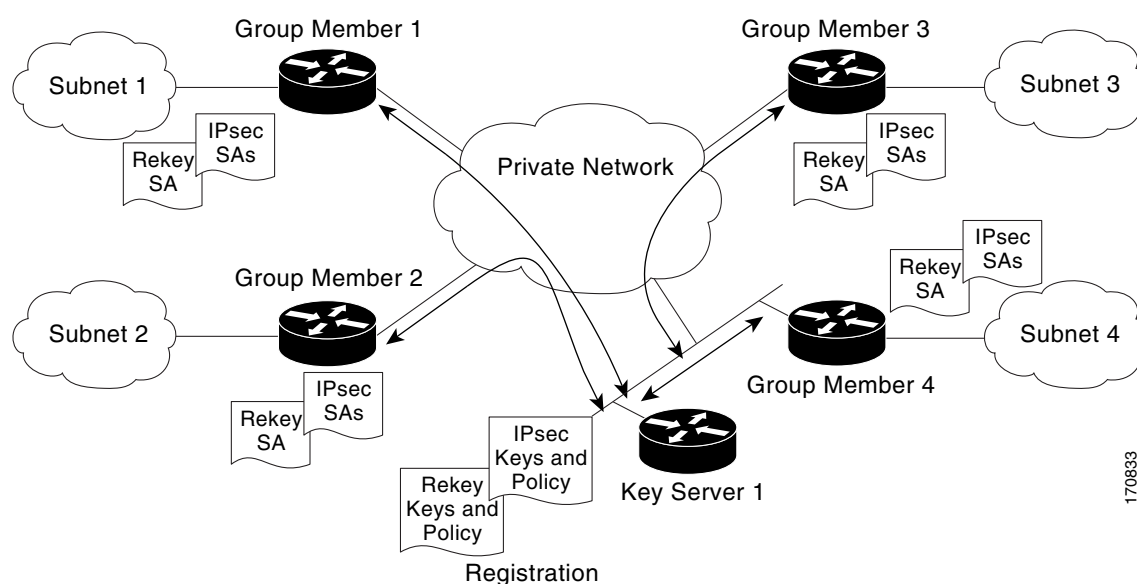
Group members provide encryption service to the interesting traffic (traffic that is worthy of being encrypted and secured by IPsec).

Communication among the key server and group members is encrypted and secured. GDOI supports the use of two keys: The TEK and the KEK. The TEK is downloaded by the key server to all the group members. The downloaded TEK is used by all the group members to communicate securely among each other. This key is essentially the group key that is shared by all the group members. The group policies and IPsec SAs are refreshed by the key server using periodic rekey messages to the group members. The KEK is also downloaded by the key server and is used by the group members to decrypt the incoming rekey messages from the key server.

The key server generates the group policy and IPsec SAs for the GDOI group. The information generated by the key server includes multiple TEK attributes, traffic encryption policy, lifetime, source and destination, a Security Parameter Index (SPI) ID that is associated with each TEK, and the rekey policy (one KEK).

Figure 4 illustrates the communication flow between group members and the key server. The key server, after receiving registration messages from a group member, generates the information that contains the group policy and new IPsec SAs. The new IPsec SA is then downloaded to the group member. The key server maintains a table that contains the IP address of each group member per group. When a group member registers, the key server adds its IP address in its associated group table, thus allowing the key server to monitor an active group member. A key server can support multiple groups. A group member can be part of multiple groups.

Figure 4 Communication Flow Between Group Members and the Key Server



IPsec and ISAKMP Timers

IPsec and ISAKMP SAs are maintained by the following timers:

- **TEK lifetime**—Determines the lifetime of the IPsec SA. Before the end of the TEK lifetime, the key server sends a rekey message, which includes a new TEK encryption key and transforms as well as the existing KEK encryption keys and transforms. The TEK lifetime is configured only on the key server, and the lifetime is "pushed down" to the group members using the GDOI protocol. The TEK lifetime value depends on the security policy of the network. If the **set security-association lifetime** command is not configured, the default value of 86400 seconds takes effect. To configure a TEK lifetime, see the [“Setting up an IPsec Lifetime Timer” section on page 28](#).
- **KEK lifetime**—Determines the lifetime of the GET VPN rekey SAs. Before the end of the lifetime, the key server sends a rekey message, which includes a new KEK encryption key and transforms as well as new TEK encryption keys and transforms. The KEK lifetime is configured only on the key server, and the lifetime is pushed down to group members dynamically using the GDOI protocol. The KEK lifetime value must be greater than the TEK lifetime value (it is recommended that the KEK

lifetime value be at least three times greater than the TEK lifetime value). If the **rekey lifetime** command is not configured, the default value of 86400 seconds takes effect. To configure a KEK lifetime, see the [“Setting up a Multicast Rekey” section on page 25](#).

- **ISAKMP SA lifetime**—Defines how long each ISAKMP SA should exist before it expires. The ISAKMP SA lifetime is configured on a group member and on the key server. If the group members and key servers do not have a cooperative key server, the ISAKMP SA is not used after the group member registration. In this case (no cooperative key server), the ISAKMP SA can have a short lifetime (a minimum of 60 seconds). If there is a cooperative key server, all key servers must have long lifetimes to keep the ISAKMP SA "up" for cooperative key server communications. If the **lifetime** command is not configured, the default value of 86400 seconds takes effect. To configure an ISAKMP SA lifetime, see the [“Setting up an ISAKMP Lifetime Timer” section on page 29](#).

Routing

GET VPN routing is explained in the following section.

Header Preservation

As shown in [Figure 5](#), IPsec-protected data packets carry the original source and destination in the outer IP header rather than replacing them with tunnel endpoint addresses. This technique is known as IPsec Tunnel Mode with Address Preservation.

Figure 5 **Header Preservation**

IP Header src=10.1.1.1 dst=10.2.1.3	ESP	IP Header src=10.1.1.1 dst=10.2.1.3	Data
---	-----	---	------

170836

Address preservation allows GET VPN to use the routing functionality present within the core network. Address preservation allows routing to deliver the packets to any customer-edge device (CE) in the network that advertises a route to the destination address. Any source and destination matching the policy for the group will be treated in a similar manner. In the situation where a link between IPsec peers is not available, address preservation also helps combat traffic "black-hole" situations.

Header preservation also maintains routing continuity throughout the enterprise address space and in the WAN. As a result, end host addresses of the campus are exposed in the WAN (for MPLS, this applies to the edge of the WAN). For this reason, GET VPN is applicable only when the WAN network acts as a "private" network (for example, in a MPLS network).

Secure Data Plane Multicast

The multicast sender uses the TEK that is obtained from the key server and encrypts the multicast data packet with header preservation before it switches out the packet. The replication of the multicast packet is carried out in the core on the basis of the (S,G) state that is retained in the multicast data packet. This process is illustrated in [Figure 6](#).

The diagram illustrates a secure communication architecture. A central cloud connects to four Group Members (routers). A Key Server (cylinder) is connected to the cloud and the Group Members via dashed lines. A key icon is shown near the Key Server. Each Group Member is also connected to a local database (cylinder) via a vertical line and a horizontal line.

The unicast sender uses the TEK that is obtained from the key server and encrypts the unicast data packet with header preservation before it switches out the packet to the destination. This process is illustrated in [Figure 7](#).

The diagram illustrates a secure communication architecture. A Unicast Sender (cylinder) is connected to a Group Member (router) via a solid line. The Group Member is connected to a central cloud. The cloud is connected to three other Group Members (routers) via solid lines. A Key Server (cylinder) is connected to the cloud and the three Group Members via dashed lines. A key icon is shown near the Key Server. Each Group Member is also connected to a local data store (cylinder) via a solid line.

Cisco Group Encrypted Transport VPN Features

This section includes the following subsections:

- [Rekeying, page 11](#)
- [Group Member Access Control List, page 14](#)
- [Time-Based Anti-Replay, page 15](#)
- [Cooperative Key Server, page 17](#)
- [Receive Only SA, page 18](#)
- [Enhanced Solutions Manageability, page 19](#)
- [Support with VRF-Lite Interfaces, page 19](#)

Rekeying

Rekey messages are used to refresh IPsec SAs. When the IPsec SAs or the rekey SAs are about to expire, one single rekey message for a particular group is generated on the key server. No new IKE sessions are created for the rekey message distribution. The rekey messages are distributed by the key server over an existing IKE SA.

Rekeying can use multicast or unicast messages. GET VPN supports both unicast and multicast rekeying.

Multicast Rekeying

Multicast rekeys are sent out using an efficient multicast rekey. Following a successful registration, the group member registers with a particular multicast group. All the group members that are registered to the group receives this multicast rekey. Multicast rekeys are sent out periodically on the basis of the configured lifetime on the key server. Multicast rekeys are also sent out if the IPsec or rekey policy is changed on the key server. Triggered by the configuration change, the rekey sends out the new updated policy to all the group members with an efficient multicast rekey.

The key server pushes the rekey time back as follows:

1. If the TEK timeout is 300 seconds:

$\text{tek_rekey_offset} = 90$ (because $300 < 900$)

If retransmissions are configured, the rekey timer is moved back more.

For three retransmissions every 10 seconds: $3 * 10$

So the rekey will actually happen at $(300 - 90 - 30) = 180$ seconds

2. If the TEK timeout is 3600 seconds:

$\text{tek_rekey_offset} = 3600 * 0\% = 360$ seconds

If retransmissions are configured, the rekey timer is moved back more.

For three retransmissions every 10 seconds: $3 * 10$

So the rekey will actually happen at $(3600 - 360 - 30) = 3210$ seconds

Unicast Rekeying and SAs

In a large unicast group, to alleviate latency issues, the key server generates rekey messages for only a small number of group members at a time. The key server is ensured that all group members receive the same rekey messages for the new SA before the expiration of the old SA. Also, in a unicast group, after receiving the rekey message from the key server, a group member sends an encrypted acknowledge (ACK) message to the key server using the keys that were received as part of the rekey message. When the key server receives this ACK message, it notes this receipt in its associated group table, which accomplishes the following:

- The key server keeps a current list of active group members.
- The key server sends rekey messages only to active members.

In addition, in a unicast group, the key server removes the group member from its active list and stops sending the rekey messages to that particular group member if the key server does not receive an ACK message for three consecutive rekeys. If no ACK message is received for three consecutive rekeys, the group member has to fully reregister with the key server after its current SA expires if the group member is still interested in receiving the rekey messages. The ejection of a nonresponsive group member is accomplished only when the key server is operating in the unicast rekey mode. The key server does not eject group members in the multicast rekey mode because group members cannot send ACK messages in that mode.

As in multicast rekeying, if retransmission is configured, each rekey will be retransmitted the configured number of times.

Rekey transport modes and authentication can be configured under a GDOI group.

If unicast rekey transport mode is not defined, multicast is applied by default.

If the TEK rekey is not received, the group member reregisters with the key server 60 seconds before the current IPsec SA expires. The key server has to send out the rekey before the group member reregistration occurs. If no retransmission is configured, the key server sends the rekey `tek_rekey_offset` before the SA expires. The `tek_rekey_offset` is calculated based on the configured rekey lifetime. If the TEK rekey lifetime is less than 900 seconds, the `tek_rekey_offset` is set to 90 seconds. If the TEK rekey lifetime is configured as more than 900 seconds, the `tek_rekey_offset` = (configured TEK rekey lifetime)/10. If retransmission is configured, the rekey occurs earlier than the `tek_rekey_offset` to let the last retransmission be sent 90 seconds before the SA expires.

The key server uses the formula in the example below to calculate when to start sending the rekey to all unicast group members. The unicast rekey process on the key server sends rekeys to unicast group members in groups of 50 within a loop. The time spent within this loop is estimated to be 5 seconds.

A key server rekeys group members in groups of 50, which equals two loops. For example, for 100 group members:

Number of rekey loops = (100 group members)/50 = 2 loops

Time it takes to rekey one loop (estimation) = 5 seconds

Time to rekey 100 group members in two loops of 50: 2 * 5 seconds = 10 seconds

So the key server pushes the rekey time back as follows:

If the TEK timeout is 300: 300 - 10 = 290

But the start has to be earlier than the TEK expiry (as in the multicast case).

Because 300 < 900, `tek_rekey_offset` = 90

So 90 seconds is subtracted from the actual TEK time: 290 - `tek_rekey_offset` = 200 seconds

If retransmissions are configured, the rekey timer is moved back more.

For three retransmissions every 10 seconds: $200 - (3 * 10) = 170$

If the TEK timeout is 3600 seconds: $3600 - 10 = 3590$

But the start has to be earlier than the TEK expiry (as in the multicast case).

Because $3600 > 900$, $\text{tek_rekey_offset} = 3600 * 10\% = 360$

So 360 seconds is subtracted from the actual TEK time: $3590 - \text{tek_rekey_offset} = 3230$ seconds.

If retransmissions are configured, the rekey timer is moved back more.

For three retransmissions every 10 seconds: $3230 - (3 * 10) = 3200$ seconds

**Note**

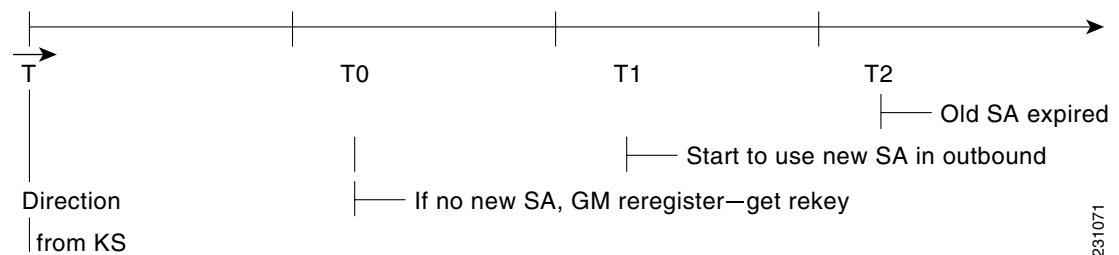
The `tek_rekey_offset` formula applies to unicast and multicast rekeying.

IPsec SA Usage on the Group Members

When a rekey is received and processed on a group member, the new IPsec SA (the Security Parameter Index [SPI]) is installed. There is a period of time when the old and the new IPsec SAs are used. After a certain specified interval, the old IPsec SA is deleted. This overlap ensures that all group members receive the current rekey and insert the new IPsec SAs. This behavior is independent of the transport method (multicast or unicast rekey transport) for the rekeys from the key server.

On the group member, approximately 30 seconds before the old SA expires, the group member starts to use the new SA in the outbound direction to encrypt the packet. Approximately 60 seconds before the old SA expires, if no new SA is received on the group member side via a rekey from the key server, the group member reregisters.

Figure 8 IPsec SA Usage on a Group Member



In [Figure 8](#), time T2 is when the old SA expires. T1 is 30 seconds before T2, which is when the group member (GM) starts to use the new SA in the outbound direction. T0 is another 30 seconds before T2. If no new SA is received at T0, the group member has to reregister. T is another 30 seconds from T0. The key server (KS) should send a rekey at T.

Configuration Changes Can Trigger a Rekey By a Key Server

Configuration changes on a key server can trigger a rekey by the key server. Please refer to the following sample configuration as you read through the events that will or will not cause a rekey.

```
crypto ipsec transform-set gdoi-p esp-3des esp-sha-hmac
!
crypto ipsec profile gdoi-p
```

```

set security-association lifetime seconds 900
set transform-set gdoi-p
!
crypto gdoi group diffint
identity number 3333
server local
rekey algorithm aes 128
rekey address ipv4 121
rekey lifetime seconds 3600
no rekey retransmit
rekey authentication mypubkey rsa mykeys
sa ipsec 1
profile gdoi-p
match address ipv4 120
replay counter window-size 3

```

Changes That Will Trigger a Rekey on a Key Server

- Any change in the TEK configuration (“sa ipsec 1” in the above example).
 - If the ACL (“match address ipv4 120” in the above example) is changed. Any addition, deletion, or change in the ACL causes a rekey.
 - If TEK replay is enabled or disabled on the key server, rekey is sent. Reconfiguring the replay window size does not trigger a rekey.
 - Removal or addition of the IPsec profile in the TEK (“profile gdoi-p” in the above example).
 - Changing from multicast to unicast transport.
 - Changing from unicast to multicast transport.

Changes That Will Not Trigger a Rekey on a Key Server

The following configuration changes on the key server will not trigger a rekey from the key server:

- Replay counter window size is changed under the TEK (“sa ipsec 1” in the above example).
- Changing the IPsec transform in the transform set.
- Configuring or removing rekey retransmit.
- Removing or configuring the rekey ACL.
- Changing the TEK lifetime (“set security-association lifetime seconds 300” in the above example) or changing the KEK lifetime (“rekey lifetime seconds 500” in the above example).
- Adding, deleting, or changing the rekey algorithm (“rekey algorithm aes 128” in the above example).

Group Member Access Control List

For GET VPN, the traffic that has to be protected is defined statically on the key server using the access control list (ACL). The group member gets information about what has to be protected from the key server. This structure allows the key server to choose and change the policy dynamically as needed. In Secure Multicast, the key server ACL is defined inclusively. The ACL includes only the exact traffic that should be encrypted, with an implicit deny causing all other traffic to be allowed in the clear (that is, if there is no permit, all other traffic is allowed).

GET VPN employs a different philosophy: the definition of which packets should be encrypted is delivered independently. GET VPN supports only statically defined traffic selectors. Policy can be defined by using both deny and permit ACLs on the key server. Only the deny ACL is allowed to be

manually configured on a group member. The policies that are downloaded from the key server and configured on the group member are merged. Any ACL that is configured on the group member has predominance over what is downloaded from the key server.

After the group member gets the ACL from the key server, the group member creates a temporary ACL and inserts it into the database. This ACL will be deleted if the group member is removed from the GDOI group for any reason. The packets that are going out of the interface are dropped by the group member if a packet matches the ACL but no IPsec SA exists for that packet.

The key server can send a set of traffic selectors, which may not exactly match the group member ACL on the group member. If such differences occur, the differences have to be merged and resolved. Because the group member is more aware of its topology than the key server, the downloaded ACLs are appended at the end of the group member ACL. The group member ACL (except the implicit deny) is inserted into the database first, followed by the downloaded key server ACL. The database is prioritized, and the database search stops whenever a matched entry is found.

For information about configuring a group member ACL, see [“Setting up Group Member ACLs” section on page 27.](#)

Time-Based Anti-Replay

Anti-replay is an important feature in a data encryption protocol such as IPsec (RFC 2401). Anti-replay prevents a third party from eavesdropping on an IPsec conversation, stealing packets, and injecting those packets into a session at a later time. The time-based anti-replay mechanism helps ensure that invalid packets are discarded by detecting the replayed packets that have already arrived at an earlier time.

GET VPN uses the Synchronous Anti-Replay (SAR) mechanism to provide anti-replay protection for multisender traffic. SAR is independent of real-world Network Time Protocol (NTP) clock or sequential-counter mechanisms (which guarantee packets are received and processed in order). A SAR clock advances regularly. The time tracked by this clock is called pseudotime. The pseudotime is maintained on the key server and is sent periodically to the group members within a rekey message as a timestamp field called pseudoTimeStamp. GET VPN uses a Cisco proprietary protocol called Metadata to encapsulate the pseudoTimeStamp. Group members have to be resynchronized to the pseudotime of the key server periodically. The pseudotime of the key server starts ticking from when the first group member registers. Initially, the key server sends the current pseudotime value of the key server and window size to group members during the registration process. New attributes, such as time-based replay-enabled information, window size, and the pseudotime of the keyserver, is sent under the SA payload (TEK).

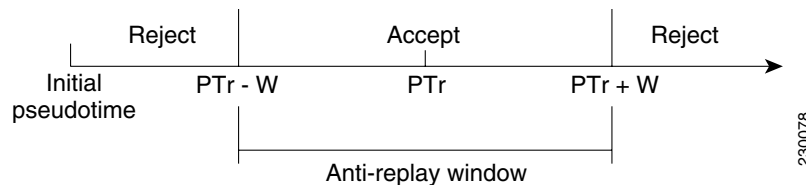
The group members use the pseudotime to prevent replay as follows: the pseudoTimeStamp contains the pseudotime value at which a sender created a packet. A receiver compares the pseudotime value of senders with its own pseudotime value to determine whether a packet is a replayed packet. The receiver uses a time-based anti-replay "window" to accept packets that contain a timestamp value within that window. The window size is configured on the key server and is sent to all group members.



Note

You should not configure time-based anti-replay if you are using a Cisco VSA as a group member.

Figure 9 illustrates an anti-replay window in which the value PTr denotes the local pseudotime of the receiver, and W is the window size.

Figure 9 Anti-Replay Window

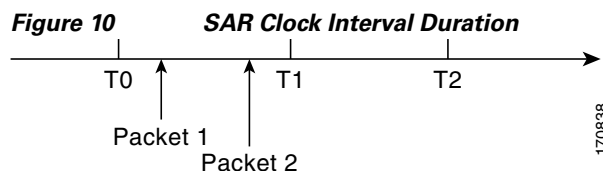
Keeping Clocks Synchronized

It is possible for the clocks of the group members to slip and lose synchronization with the key server. To keep the clocks synchronized, a rekey message (multicast or unicast, as appropriate), including the current pseudotime value of the key server, is sent periodically (either in a rekey message or at a minimum of every 30 minutes to the group member. If a packet fails this anti-replay check, the pseudotime of both the sender and receiver is printed, an error message is generated, and a count is increased.

To view anti-replay statistics, use the **show crypto gdoi group group-name gm replay** command on both the sender and receiver devices. If the configuration is changed by the administrator to affect the replay method of the size configuration, the key server initiates a rekey message.

Interval Duration

A tick is the interval duration of the SAR clock. Packets sent in this duration have the same pseudoTimeStamp. The tick is also downloaded to group members, along with the pseudotime from the key server. For example, as shown in Figure 10, packets sent between T0 and T1 would have the same pseudoTimeStamp T0. SAR provides loose anti-replay protection. The replayed packets are accepted if they are replayed during the window. The default window size is 100 seconds. It is recommended that you keep the window size small to minimize packet replay.



Anti-Replay Configurations

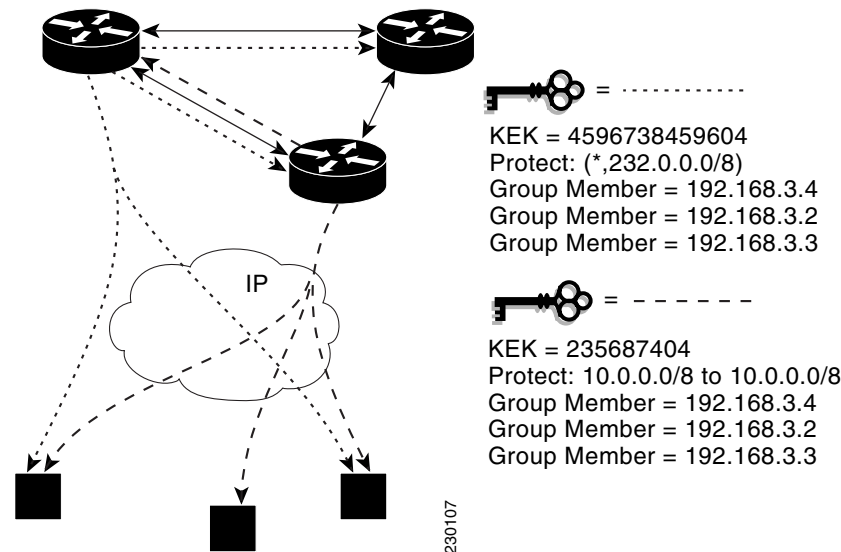
The Anti-Replay feature can be enabled under IPsec SA on a key server by using the following commands:

- **replay time window-size**—Enables the replay time option, which supports the nonsequential, or time-based, mode. The window size is in seconds. Use this mode only if you have more than two group members in a group.
- **replay counter window-size**—Enables sequential mode. This mode is useful if there are only two group members in a group.
- **no replay counter window-size**—Disables anti-replay.

Cooperative Key Server

Figure 11 illustrates cooperative key server key distribution. The text below the illustration explains the Cooperative Key Server feature.

Figure 11 Cooperative Key Server Key Distribution



Cooperative key servers provide redundancy to GET VPN. Multiple key servers are supported by GET VPN to ensure redundancy, high availability, and fast recovery if the primary key server fails. Cooperating GDOI key servers jointly manage the GDOI registrations for the group. Each key server is an active key server, handling GDOI registration requests from group members. Because the key servers are cooperating, each key server distributes the same state to the group members that register with it. Load balancing is achieved because each of the GDOI key servers can service a portion of the GDOI registrations.

The primary key server is responsible for creating and distributing group policy. The primary key server periodically sends out (or broadcasts) group information updates to all other key servers to keep those servers in synchronization. If the secondary key servers somehow miss the updates, they contact the primary key server to directly request information updates. The secondary key servers mark the primary key server as unreachable (that is, “dead”) if the updates are not received for an extended period of time.

When a new policy is created on a primary key server, regardless of which key server a group member may be registered with, it is the responsibility of the primary key server to distribute rekey messages to GDOI group members.



Note

If you are supporting a large number of group members in your cooperative key server setup (that is, more than 300), you should increase the buffer size by using the **buffers huge size** command.

Announcement Messages

Announcement messages are secured by IKE Phase 1 and are sent as IKE notify messages. Authentication and confidentiality that are provided by IKE is used to secure the messaging between the key servers. Anti-replay protection is provided by the sequence numbers in the announcement messages. Announcement messages are periodically sent from primary to secondary key servers.

Announcement messages include the following components that help maintain the current state.

Sender Priority of a Key Server

This value describes the priority of the sender, which is configurable using the CLI. The key server with the highest priority becomes the primary key server. If the priority values are the same, the key server with the highest IP address becomes the primary key server.

Maintaining the Role of the Sender

During the synchronization period, if the key servers are at geographically dispersed locations, they may suffer a network-partitioning event. If a network-partitioning event occurs, it is possible that more than one key server can become the primary key server for a period of time. When the network is operating normally again and all the key servers find each other, they need to be told the current role of the sender so the key servers can attain their proper roles.

Request for a Return Packet Flag

All messages are defined as one-way messages. When needed, a key server can request the current state from a peer to find out its role and/or request the current state of the group.

Group Policies

The group policies are the policies that are maintained for a group, such as group member information and IPsec SAs and keys.

Anti-replay functionalities and incorporated Cooperative announcement messages are supported. The primary key server updates the pseudotime value, sending it to all secondary key servers in the group. The secondary key servers should synchronize their SAR clocks to this updated value.

Receive Only SA

For multicast traffic using the GDOI protocol, bidirectional SAs are installed. The Receive Only feature enables an incremental deployment so that only a few sites can be verified before bringing up an entire network. To test the sites, one of the group members should send encrypted traffic to all the other group members and have them decrypt the traffic and forward the traffic “in the clear.” Receive Only SA mode allows encryption in only the inbound direction for a period of time. (See the steps below for the Receive Only SA process.) If you configure the **sa receive-only** command on the key server, Steps 2 and 3 happen automatically.

1. Mark IPsec SAs as "receive-only" on the GDOI key server.

This action allows the group members to install SAs in the inbound direction only. Receive-only SAs can be configured under a crypto group. (See [“Setting up the Group ID, Server Type, and SA Type” section on page 21.](#))

2. Mark GDOI TEK payloads as "receive only."

If the **sa receive-only** command is configured, all TEKs under this group are going to be marked “receive only” by the key server when they are sent to the group member.

3. Install one-way IPsec flows.

Every time a GDOI group member receives an IPsec SA from the key server that is marked as "receive only," the group member installs this IPsec SA only in the inbound direction rather than in both incoming and outgoing directions.

4. Test individual group members using the following local-conversion commands:

- **crypto gdoi gm ipsec direction inbound optional**
- **crypto gdoi gm ipsec direction both**

Local Conversion

First, individually convert each of the group members to passive mode (this change tells the outbound check that there is a valid SA) and then to bi-directional mode.

5. Globally convert from “receive only” to “receive and send.”

The following method can be used when the testing phase is over and “receive only” SAs have to be converted to bi-directional SAs.

Global Conversion

Remove the **sa receive-only** command under the group. Removing the **sa receive-only** command creates new IPsec SAs for this group and causes a rekey. On receipt, group members reinstall the SA in both directions and begin to use it in passive mode. Because the SA cannot remain in passive mode forever, the group members change those SAs to receive or send mode if there is no rekey in 5 minutes. The conversion from passive mode to bidirectional encryption mode is automatic and does not require the administrator to do anything.

Enhanced Solutions Manageability

Several **show** and **debug** commands are supported to help verify functionality. See the [“Verifying and Troubleshooting Cisco Group Encrypted Transport VPN” section on page 37](#) for the details.

Support with VRF-Lite Interfaces

VRF-Lite application supports segmentation of traffic in the control and forwarding planes by keeping the routing tables separate for each user group (or VPN) and forwards the traffic on the associated or dedicated interfaces of each user group.

There are some deployment scenarios in which remote sites that are connecting to an MPLS VPN network might be extending segmentation from a campus to the WAN. In such an extended segmentation case, a CE-PE interface on a CE (group member or key server) device “bounds” to its associated Virtual Routing Forwarding (VRF) instance. This VRF interface connects to an MPLS PE device where it is directly mapped to its associated Border Gateway Protocol (BGP) VRF process, in which case the crypto map is applied to a VRF interface. No other configuration changes are necessary.

End-User Considerations

Multicast rekeying can be used with all modes of multicast. The **rekey retransmit** command should be used whenever the Protocol Independent Multicast-sparse mode (PIM-SM) is configured because the PIM-SM shortest path tree (SPT) can be torn down if it does not receive continuing traffic. When traffic resumes, PIM-SM must reestablish the SPT. Retransmitting rekey packets increases the chance that group members receive the rekeys when PIM-SM is setting up the SPT.

System Error Messages

For a list of system error messages, see [Appendix I: System Messages, page 51](#).

How to Configure Cisco Group Encrypted Transport VPN

This section includes the following required and optional tasks:

- [Setting up a Key Server, page 20](#) (required)
- [Setting up a Group Member, page 34](#) (required)
- [Verifying and Troubleshooting Cisco Group Encrypted Transport VPN, page 37](#)

Setting up a Key Server

To set up a key server, perform the steps in the following five subtasks.

- [Setting up RSA Keys to Sign Rekey Messages, page 20](#) (optional)
- [Setting up the Group ID, Server Type, and SA Type, page 21](#) (required)
- [Setting up the Rekey, page 22](#) (optional)
- [Setting up Group Member ACLs, page 27](#) (optional)
- [Setting up an IPsec Lifetime Timer, page 28](#) (optional)
- [Setting up an ISAKMP Lifetime Timer, page 29](#) (optional)
- [Setting up the IPsec SA, page 30](#) (required)
- [Configuring Time-Based Anti-Replay for a GDOI Group, page 32](#) (optional)

Prerequisites

Before creating the GDOI group, you must first configure IKE and the IPsec transform set, and you must create an IPsec profile. For information about how to configure IKE and the IPsec transform set and to create an IPsec profile, see the “Related Documents” subsection of the [“Additional References” section on page 47](#).

Setting up RSA Keys to Sign Rekey Messages

To set up RSA keys that will be used to sign rekey messages, perform the following steps.



Note

- Skip this subtask if rekey is not in use.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto key generate rsa general-keys label *name-of-key***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto key generate rsa general-keys label <i>name-of-key</i> Example: Router (config)# crypto key generate rsa general-keys label mykeys	Generates RSA keys that will be used to sign rekey messages. Note Skip this command if rekey is not in use.

What to Do Next

Set up the group ID, server type, and SA type. (See the section [“Setting up the Group ID, Server Type, and SA Type”](#) section on page 21.)

Setting up the Group ID, Server Type, and SA Type

To set up the group ID, server type, and SA type, perform the following steps.

**Note**

For a large number of sites, it is better to take precautions and add functionality incrementally, especially when one is migrating from any other encryption solutions like Dual Multipoint VPN (DMVPN). For example, instead of setting up all the CPE devices to encrypt the traffic bidirectionally, it is possible to set up one-way encryption so that only one or fewer members of a group are allowed to send encrypted traffic. Others are allowed to receive only encrypted traffic. After the one-way encryption is validated for one or a few members, bidirectional encryption can be turned on for all the members. This “inbound only” traffic can be controlled using the **sa receive only** command under a crypto group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **identity number** *number*
or
identity address ipv4 *address*
5. **server local**
6. **sa receive-only**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto gdoi group <i>group-name</i> Example: Router (config)# crypto gdoi group gdoigroupname	Identifies a GDOI group and enters GDOI group configuration mode.
Step 4	identity number <i>number</i> or identity address ipv4 <i>address</i> Example: Router (config-gdoi-group)# identity number 3333 or Router (config-gdoi-group)# identity address ipv4 10.2.2.2	Identifies a GDOI group number or address.
Step 5	server local Example: Router (config-gdoi-group)# server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.
Step 6	sa receive-only Example: Router (config-local-server)# sa receive-only	Specifies that an IPsec SA is to be installed by a group member as “inbound only.”

What to Do Next

Remove the receive-only configuration on the key server so that the group members are now operating in bidirectional receive and send mode.

Setting up the Rekey

Rekey is used in the control plane by the key server to periodically refresh the policy and IPsec SAs of the group. On the group-member side, instead of fully reregistering when timers expire for any other reasons, refreshing the registration with a rekey is more efficient. The initial registration is always a unicast registration.

The key server can be configured to send rekeys in unicast or multicast mode. The rekey transport mode is determined by whether the key server can use IP multicast to distribute the rekeys. If multicast capability is not present within the network of the customer, the key server will have to be configured to send rekeys using unicast messages.

Additional options for rekey use the **rekey authentication**, **rekey retransmit**, and **rekey address ipv4** commands. If unicast transport mode is configured, the **source address** command will have to be included to specify the source address of this unicast rekey message.

Multicast is the default transport type for rekey messages. The following bulleted items explain when to use rekey transport type multicast or unicast:

- If all members in a group are multicast capable, do not configure the **rekey transport unicast** command.



Note The **no rekey transport unicast** command is not needed if the rekey transport type “unicast” was not configured previously under this group because multicast rekeys are on by default.

- If all members in a group are unicast, use the **rekey transport unicast** command.
- If you have mixed members in a group (that is, the majority are multicast, but a few are unicast), do not configure the **rekey transport unicast** command. The rekeys will be distributed using multicast to the majority of group members. The remainder of the group members that do not receive the multicast messages (unicast group members) will have to reregister to the key server when their policies expire. Mixed mode (that is, unicast and multicast rekey mode) is currently not supported.



Note

- If the **no rekey transport unicast** command is used, members in the GDOI group that are unable to receive the multicast rekey messages need to reregister with the key server to get the latest group policies.

The reregistering forces the default transport type to multicast. If no transport type was configured previously, the multicast transport type will apply by default.

Prerequisites

Before configuring the **rekey authentication** command, you must have configured the router to have a RSA key generated using the **crypto key generate rsa** command and **general-keys** and **label** keywords (for example, “crypto key generate rsa general-key label my keys”).

Setting up a Unicast Rekey

To set up a unicast rekey, perform the following steps.



Note

In the configuration task table below, the address “ipv4 10.0.5.2” specifies the interface on the key server by which the unicast or multicast rekey messages are sent. This address is required for unicast rekeys, but it is optional for multicast rekeys. For multicast rekeys, the source address of the key server can be retrieved from the rekey ACL.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **identity number** *number*
or
identity address ipv4 *address*
5. **server local**
6. **rekey transport unicast**
7. **rekey lifetime seconds** *number-of-seconds*
8. **rekey retransmit** *number-of-seconds* **number** *number-of-retransmissions*
9. **rekey authentication** {**mypubkey** | **pubkey**} **rsa** *key-name*
10. **address ipv4** *ipv4-address*

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto gdoi group <i>group-name</i> Example: Router (config)# crypto gdoi group gdoigroupname	Identifies a GDOI group and enters GDOI group configuration mode.
Step 4	identity number <i>number</i> or identity address ipv4 <i>address</i> Example: Router (config-gdoi-group)# identity number 3333 or Router (config-gdoi-group)# identity address ipv4 10.2.2.2	Identifies a GDOI group number or address.
Step 5	server local Example: Router (config-gdoi-group)# server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

	Command or Action	Purpose
Step 6	rekey transport unicast Example: Router (config-local-server)# rekey transport unicast	Configures unicast delivery of rekey messages to group members.
Step 7	rekey lifetime seconds <i>number-of-seconds</i> Example: Router (gdoi-local-server)# rekey lifetime seconds 300	(Optional) Limits the number of seconds that any one encryption key should be used. If this command is not configured, the default value of 86400 seconds takes effect.
Step 8	rekey retransmit <i>number-of-seconds</i> number <i>number-of-retransmissions</i> Example: Router (gdoi-local-server)# rekey retransmit 10 number 3	(Optional) Specifies the number of times the rekey message is retransmitted. If this command is not configured, there will be no retransmits.
Step 9	rekey authentication { <i>mypubkey</i> <i>pubkey</i> } rsa <i>key-name</i> Example: Router (gdoi-local-server)# rekey authentication mypubkey rsa mykeys	(Optional) Specifies the keys to be used for a rekey to GDOI group members. This command is optional if rekeys are not required. If rekeys are required, this command is required.
Step 10	address ipv4 <i>ipv4-address</i> Example: Router (gdoi-local-server)# address ipv4 10.0.5.2	(Optional) Specifies the source information of the unicast rekey message. If rekeys are not required, this command is optional. If rekeys are required, this command is required.

Setting up a Multicast Rekey

To set up a multicast rekey, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **identity number** *number*
or
identity address ipv4 *address*
5. **server local**
6. **rekey address ipv4** {*access-list-name* | *access-list-number*}
7. **rekey lifetime seconds** *number-of-seconds*
8. **rekey retransmit** *number-of-seconds* **number** *number-of-retransmissions*
9. **rekey authentication** {*mypubkey* | *pubkey*} **rsa** *key-name*

10. **exit**
11. **exit**
12. **access-list** *access-list-number* {**deny** | **permit**} **udp** **host** *source* [*operator* *port*]] **host** *source* [*operator* *port*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto gdoi group <i>group-name</i> Example: Router (config)# crypto gdoi group gdoigroupname	Identifies a GDOI group and enters GDOI group configuration mode.
Step 4	identity number <i>number</i> or identity address ipv4 <i>address</i> Example: Router (config-gdoi-group)# identity number 3333 or Router (config-gdoi-group)# identity address ipv4 10.2.2.2	Identifies a GDOI group number or address.
Step 5	server local Example: Router (config-gdoi-group)# server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.
Step 6	rekey address ipv4 { <i>access-list-name</i> <i>access-list-number</i> } Example: Router (gdoi-local-server)# rekey address ipv4 121	Defines to which multicast subaddress range group members will register.

	Command or Action	Purpose
Step 7	rekey lifetime seconds <i>number-of-seconds</i> Example: Router (gdoi-local-server)# rekey lifetime seconds 300	(Optional) Limits the number of seconds that any one encryption key should be used. If this command is not configured, the default value of 86400 seconds takes effect.
Step 8	rekey retransmit <i>number-of-seconds</i> number <i>number-of-retransmissions</i> Example: Router (gdoi-local-server)# rekey retransmit 10 number 3	(Optional) Specifies the number of times the rekey message is retransmitted. If this command is not configured, there will be no retransmits.
Step 9	rekey authentication { mypubkey pubkey } rsa <i>key-name</i> Example: Router (gdoi-local-server)# rekey authentication mypubkey rsa mykeys	(Optional) Specifies the keys to be used for a rekey to GDOI group members. This command is optional if rekeys are not required. If rekeys are required, this command is required.
Step 10	exit Example: Router (gdoi-local-server)# exit	Exits GDOI server local configuration mode.
Step 11	exit Example: Router (config-gdoi-group)# exit	Exits GDOI group configuration mode.
Step 12	access-list <i>access-list-number</i> { deny permit } udp host <i>source</i> [<i>operator</i> [<i>port</i>]] host <i>source</i> [<i>operator</i> [<i>port</i>]] Example: Router (config)# access-list 121 permit udp host 10.0.5.2 eq 848 host 239.0.1.2 eq 848	Defines an extended IP access list.

Setting up Group Member ACLs

To set up group member ACLs, perform the following steps.



Note

Ensure that your ACL starts with a deny statement if all traffic does not need to be encrypted.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* **deny ip** *host source* **host** *source*
4. **access-list** *access-list-number* **permit ip** *source*

DETAILED STEPS

Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	access-list access-list-number deny ip host source host source Example: Router (config)# access-list 101 deny ip host 10.0.0.1 host 10.0.0.2	Defines a denied IP access list.
Step 4	access-list access-list-number permit ip source Example: Router (config)# Router (config)# access-list 103 permit ip 10.15.0.0. 0.255.255.255 10.20.0.0. 0.255.255.255	Defines an allowed IP access list.

What to Do Next

The above access list is the same one that should be used to set up the SA. See the [“Setting up the IPsec SA” section on page 30](#).

Setting up an IPsec Lifetime Timer

To set up an IPsec lifetime timer for a profile, perform the following steps. If this configuration task is not performed, the default is the maximum IPsec SA lifetime of 3600 seconds.

SUMMARY STEPS

- enable**
- configure terminal**
- crypto ipsec profile** *name*
- set security-association lifetime seconds** *seconds*

DETAILED STEPS

Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto ipsec profile <i>name</i> Example: Router (config)# crypto ipsec profile profile1	Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers and enters crypto ipsec profile configuration mode.
Step 4	set security-association lifetime seconds <i>seconds</i> Example: Router (ipsec-profile)# set security-association lifetime seconds 2700	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPsec SAs.

What to Do Next

Configure the IPsec SA. See the [“Setting up the IPsec SA”](#) section on page 30.

Setting up an ISAKMP Lifetime Timer

To set up an ISAKMP lifetime timer, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp policy *priority***
4. **lifetime *seconds***

DETAILED STEPS

Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto isakmp policy <i>priority</i> Example: Router (config)# crypto ipsec policy 1	Defines an IKE policy.
Step 4	lifetime <i>seconds</i> Example: Router (config-isakmp-policy)# lifetime 86400	Specifies the lifetime of an IKE SA.

Setting up the IPsec SA

To set up the IPsec SA, perform the following steps.



Note

If time-based anti-replay is configured on the key server but the group member is not capable of supporting it, the GDOI-3-GM_NO_CRYPT0_ENGINE system message is logged to the group member.

SUMMARY STEPS

- enable**
- configure terminal**
- crypto gdoi group** *group-name*
- identity number** *number*
or
identity address ipv4 *address*
- server local**
- sa ipsec** *sequence-number*
- profile** *ipsec-profile-name*
- match address ipv4** {*access-list-number* | *access-list-name*}
- exit**
- exit**
- exit**

12. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
13. **crypto ipsec profile** *ipsec-profile-name*
14. **set transform-set** *transform-set-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto gdoi group <i>group-name</i> Example: Router (config)# crypto gdoi group gdoigroupname	Identifies a GDOI group and enters GDOI group configuration mode.
Step 4	identity number <i>number</i> or identity address ipv4 <i>address</i> Example: Router (config-gdoi-group)# identity number 3333 or Router (config-gdoi-group)# identity address ipv4 10.2.2.2	Identifies a GDOI group number or address.
Step 5	server local Example: Router (config-gdoi-group)# server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.
Step 6	sa ipsec <i>sequence-number</i> Example: Router (gdoi-local-server)# sa ipsec 1	Specifies the IPsec SA policy information to be used for a GDOI group and enters GDOI SA IPsec configuration mode.
Step 7	profile <i>ipsec-profile-name</i> Example: Router (gdoi-sa-ipsec)# profile gdoi-p	Defines the IPsec SA policy for a GDOI group.

	Command or Action	Purpose
Step 8	match address ipv4 { <i>access-list-number</i> <i>access-list-name</i> } Example: Router (gdoi-sa-ipsec)# match address ipv4 102	Specifies an IP extended access list for a GDOI registration.
Step 9	exit Example: Router (gdoi-sa-ipsec)# exit	Exits GDOI SA IPsec configuration mode.
Step 10	exit Example: Router (gdoi-local-server)# exit	Exits GDOI local server configuration mode.
Step 11	exit Example: Router (config-gdoi-group)# exit	Exits GDOI group configuration mode.
Step 12	crypto ipsec transform-set <i>transform-set-name</i> <i>transform1</i> [<i>transform2</i>] [<i>transform3</i>] [<i>transform4</i>] Example: Router (config)# crypto ipsec transform-set gdoi-trans esp-3des esp-sha-hmac	Defines a transform set—an acceptable combination of security protocols and algorithms.
Step 13	crypto ipsec profile <i>ipsec-profile-name</i> Example: Router (config)# crypto ipsec profile profile1	Defines an ISAKMP profile and enters crypto ipsec profile configuration mode.
Step 14	set transform-set <i>transform-set-name</i> Example: Router (ipsec-profile)# set transform-set transformset1	Specifies which transform sets can be used with the crypto map entry.

What to Do Next

Replay should be configured. If not configured, the default is counter mode.

Configuring Time-Based Anti-Replay for a GDOI Group

To configure time-based anti-replay for a GDOI group, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **crypto gdoi group** *group-name*
4. **identity number** *policy-name*
5. **server local**
6. **address** *ip-address*
7. **sa ipsec** *sequence-number*
8. **profile** *ipsec-profile-name*
9. **match address** {**ipv4** *access-list-number* | *access-list-name*}
10. **replay counter window-size** *seconds*
11. **replay time window-size** *seconds*

DETAILED STEPS

Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto gdoi group <i>group-name</i> Example: Router (config)# crypto gdoi group gdoigroup1	Identifies a GDOI group and enters GDOI group configuration mode.
Step 4	identity number <i>policy-name</i> Example: Router (config-gdoi-group)# identity number 1234	Identifies a GDOI group number.
Step 5	server local Example: Router (config-gdoi-group)# server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.
Step 6	address <i>ip-address</i> Example: Router (config-server-local)# address ipv4 10.10.10.10	Sets the source address, which is used as the source for packets originated by the local key server.
Step 7	sa ipsec <i>sequence-number</i> Example: Router (config-server-local)#sa ipsec 1	Specifies the IPsec SA and enters GDOI SA IPsec configuration mode.

Step 8	profile <i>ipsec-profile-name</i> Example: Router (gdoi-sa-ipsec)# profile test1	Defines the IPsec SA policy for a GDOI group.
Step 9	match address { ipv4 <i>access-list-number</i> <i>access-list-name</i> } Example: Router (gdoi-sa-ipsec)# match address ipv4 101	Specifies an IP extended access list for a GDOI registration.
Step 10	replay counter window-size <i>seconds</i> Example: Router (gdoi-sa-ipsec)# replay counter window-size 512	Turns on counter-based anti-replay protection for traffic defined inside an access list using GDOI if there are only two group members in a group. Note This command and the replay time window-size command are mutually exclusive. You can configure either one without configuring the other one.
Step 11	replay time window-size <i>seconds</i> Example: Router (gdoi-sa-ipsec)# replay time window-size	Sets the window size for anti-replay protection using GDOI if there are more than two group members in a group. Note This command and the replay counter window-size command are mutually exclusive. You can configure either one without configuring the other one.

Setting up a Group Member

To set up a group member, perform the following subtasks:

- [Setting Up the Group Name, ID, and Key Server IP Address, page 34](#) (required)
- [Setting up the Crypto Map, page 35](#) (required)
- [Applying the Crypto Map to an Interface to Which the Traffic Has to Be Encrypted, page 36](#) (required)

Setting Up the Group Name, ID, and Key Server IP Address

To set up the group name, ID, and key server IP address, perform the following steps.



Note

You can set up to eight key server addresses.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*

4. **identity number** *number*
or
identity address ipv4 *address*
5. **server address ipv4** *address*

DETAILED STEPS

Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto gdoi group <i>group-name</i> Example: Router (config)# crypto gdoi group gdoigroupone	Identifies a GDOI group and enters GDOI group configuration mode.
Step 4	identity number <i>number</i> or identity address ipv4 <i>address</i> Example: Router (config-gdoi-group)# identity number 3333 or Router (config-gdoi-group)# identity address ipv4 10.2.2.2	Identifies a GDOI group number or address.
Step 5	server address ipv4 <i>address</i> Example: Router (config-gdoi-group)# server address ipv4 10.0.5.2	Specifies the address of the server a GDOI group is trying to reach. <ul style="list-style-type: none"> To disable the address, use the no form of the command.

What to Do Next

Set up the crypto map. See the section [“Setting up the Crypto Map”](#) section on page 35.

Setting up the Crypto Map

To set up the crypto map, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num gdoi*
4. **set group** *group-name*

DETAILED STEPS

Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto map <i>map-name seq-num gdoi</i> Example: Router (config)# crypto map mymap 10 gdoi	Enters crypto map configuration mode and creates or modifies a crypto map entry.
Step 4	set group <i>group-name</i> Example: Router (config-crypto-map)# set group group1	Associates the GDOI group to the crypto map.

What to Do Next

Apply the crypto map to an interface to which the traffic has to be encrypted. See the [“Applying the Crypto Map to an Interface to Which the Traffic Has to Be Encrypted”](#) section on page 36.

Applying the Crypto Map to an Interface to Which the Traffic Has to Be Encrypted

To apply the crypto map to an interface to which the traffic has to be encrypted, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **crypto map** *map-name redundancy standby-group-name stateful*

DETAILED STEPS

Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type slot/port</i> Example: Router (config)# interface gig0/0	Configures an interface type and enters interface configuration mode.
Step 4	crypto map <i>map-name</i> redundancy <i>standby-group-name</i> stateful Example: Router (config-if)# crypto map map1 redundancy groupred stateful	Applies the crypto map to the interface.

Verifying and Troubleshooting Cisco Group Encrypted Transport VPN

The following tasks can be used to verify and troubleshoot your GET VPN configurations. These tasks are optional and are used to gather information during troubleshooting.

- [Verifying Active Group Members on a Key Server, page 37](#)
- [Verifying Rekey-Related Statistics, page 38](#)
- [Verifying IPsec SAs That Were Created by GDOI on a Key Server, page 38](#)
- [Verifying Cooperative Key Server States and Statistics, page 39](#)
- [Verifying Anti-Replay Pseudotime-Related Statistics, page 40](#)

Verifying Active Group Members on a Key Server

To verify active group members on a key server, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show crypto gdoi ks members**

DETAILED STEPS

Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show crypto gdoi ks members Example: Router# show crypto gdoi ks members	Displays information about key server members.

Verifying Rekey-Related Statistics

To verify rekey-related statistics, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show crypto gdoi ks rekey**

DETAILED STEPS

Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show crypto gdoi ks rekey Example: Router# show crypto gdoi ks rekey	On the key server, this command displays information about the rekeys that are being sent from the key server.

Verifying IPsec SAs That Were Created by GDOI on a Key Server

To verify IPsec SAs that were created by GDOI on a key server, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show crypto gdoi group *group-name* ipsec sa**
3. **show crypto ipsec sa**

DETAILED STEPS

Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show crypto gdoi group <i>group-name</i> ipsec sa Example: Router# show crypto gdoi group diffint ipsec sa	Displays information about IPsec SAs that were created by GDOI on a key server. <ul style="list-style-type: none"> In this case, information will be displayed only for group “diffint.” For information about IPsec SAs for all groups, omit the group keyword and <i>group-name</i> argument.
Step 3	show crypto ipsec sa Example: Router# show crypto ipsec sa	Displays the settings used by current SAs.

Verifying Cooperative Key Server States and Statistics

To verify cooperative key server states and statistics, perform the following steps, using one or all of the **debug** and **show** commands shown.

SUMMARY STEPS

1. **enable**
2. **debug crypto gdoi ks coop**
3. **show crypto gdoi group *group-name* ks coop [version]**

DETAILED STEPS

Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	debug crypto gdoi ks coop Example: Router# debug crypto gdoi ks coop	Displays information about a cooperative key server.
Step 3	show crypto gdoi group <i>group-name</i> ks coop [version] Example: Router# show crypto gdoi group diffint ks coop engineer	Displays key server information for the group “diffint.”

Verifying Anti-Replay Pseudotime-Related Statistics

To verify anti-replay pseudotime-related statistics, perform the following steps using one or all of the **clear**, **debug**, and **show** commands.

SUMMARY STEPS

1. **enable**
2. **clear crypto gdoi group *group-name* replay**
3. **debug crypto gdoi replay**
4. **show crypto gdoi group *group-name***
5. **show crypto gdoi group *group-name* ks replay**

DETAILED STEPS

Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	clear crypto gdoi group <i>group-name</i> replay Example: Router# clear crypto gdoi group diffint replay	Clears the replay counters.
Step 3	debug crypto gdoi replay Example: Router# debug crypto gdoi replay	Displays information about the pseudotime stamp that is contained in a packet.
Step 4	show crypto gdoi group <i>group-name</i> Example: Router# show crypto gdoi group diffint	Displays information about the current pseudotime of the group member. It also displays the different counts that are related to the anti-replay for this group.
Step 5	show crypto gdoi group <i>group-name</i> ks replay Example: Router# show crypto gdoi group diffint ks replay	Displays information about the current pseudotime of the key server.

Configuration Examples for Cisco Group Encrypted Transport VPN

This section includes the following case study and configuration examples:

- [Key Server and Group Member Case Study, page 41](#)
- [Key Server 1: Example, page 41](#)

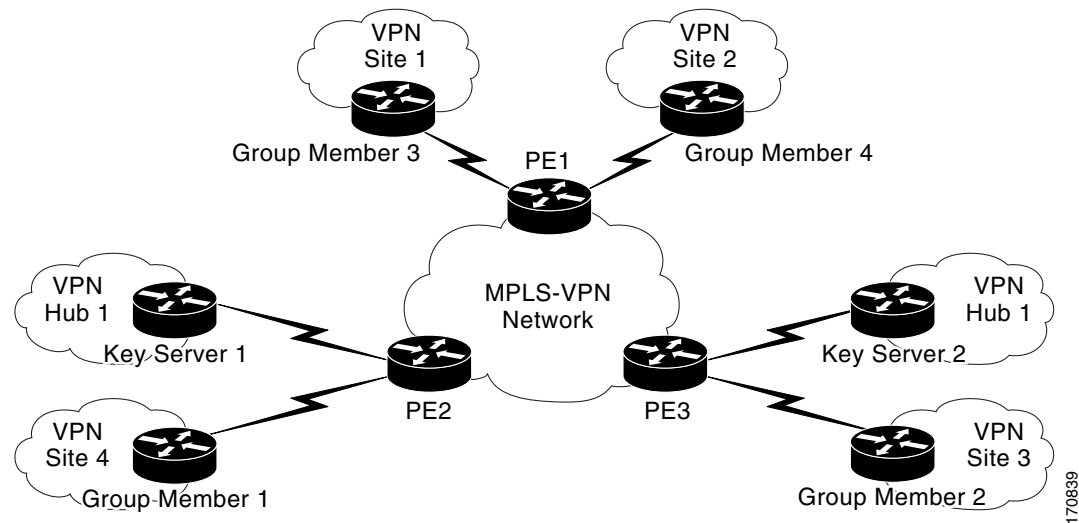
- [Key Server 2: Example, page 42](#)
- [Group Member 1: Example, page 44](#)
- [Group Member 2: Example, page 44](#)
- [Group Member 3: Example, page 45](#)
- [Group Member 4: Example, page 46](#)

Key Server and Group Member Case Study

The following case study includes encrypting traffic CE-CE in an MPLS VPN environment.

The MPLS VPN core interconnects VPN sites as is shown in [Figure 12](#). VPN site CPEs, Group Member 1 through Group Member 4, are grouped into a single GDOI group that correlates with a VPN with which these sites are a part. This scenario is an intranet VPN scenario. All the key servers and group members are part of the same VPN. Key Server 1 and Key Server 2 are the cooperative key servers that support VPN members Group Member 1 through Group Member 4. Key Server 1 is the primary key server and Key Server 2 is the secondary key server.

Figure 12 Key Server and Group Member Scenario



The following configuration examples are based on the case study in [Figure 12](#).

Key Server 1: Example

Key server 1 is the primary key server.

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname KS1
!
```

```

logging buffered 100000 debugging
no logging console
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
ip domain name cisco.com
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
  lifetime 400
crypto isakmp key cisco address 10.1.1.13
crypto isakmp key cisco address 10.1.1.9
crypto isakmp key cisco address 10.1.1.1
crypto isakmp key cisco address 10.1.1.5
crypto isakmp key cisco address 10.1.1.21
!
crypto ipsec transform-set gdoi-trans-group1 esp-3des esp-sha-hmac
!
crypto ipsec profile gdoi-profile-group1
  set security-association lifetime seconds 1800
  set transform-set gdoi-trans-group1
!
crypto gdoi group group1
  identity number 1
  server local
    rekey lifetime seconds 86400
    rekey retransmit 10 number 2
    rekey authentication mypubkey rsa group1-export-general
    rekey transport unicast
  sa ipsec 1
    profile gdoi-profile-group1
    match address ipv4 101
    replay counter window-size 64
    address ipv4 10.1.1.17
    redundancy
      local priority 10
      peer address ipv4 10.1.1.21
    !
  !
interface Ethernet0/0
  ip address 10.1.1.17 255.255.255.252
  !
  ip classless
  ip route 0.0.0.0 0.0.0.0 10.1.1.18
  !
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!
end

```

Key Server 2: Example

Key Server 2 is the secondary key server.

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec

```

```
no service password-encryption
service internal
!
hostname KS2
!
logging buffered 100000 debugging
no logging console
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
ip domain name cisco
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
  lifetime 400
crypto isakmp key cisco address 10.1.1.9
crypto isakmp key cisco address 10.1.1.1
crypto isakmp key cisco address 10.1.1.5
crypto isakmp key cisco address 10.1.1.17
crypto isakmp key cisco address 10.1.1.13
!
crypto ipsec transform-set gdoi-trans-group1 esp-3des esp-sha-hmac
!
crypto ipsec profile gdoi-profile-group1
  set security-association lifetime seconds 1800
  set transform-set gdoi-trans-group1
!
crypto gdoi group group1
  identity number 1
  server local

  rekey lifetime seconds 86400
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa group1-export-general
  rekey transport unicast
  sa ipsec 1
    profile gdoi-profile-group1
    match address ipv4 101
    replay counter window-size 64
    address ipv4 10.1.1.21
    redundancy
      local priority 1
      peer address ipv4 10.1.1.17
    !
interface Ethernet0/0
  ip address 10.1.1.21 255.255.255.252
  !
  ip classless
  ip route 0.0.0.0 0.0.0.0 10.1.1.22
  !

access-list 101 permit ip 10.1.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!
end
```

Group Member 1: Example

Group Member 1 is part of a GDOI group that correlates with a VPN with which these sites are a part.

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GM1
!
resource policy
!
clock timezone EST 0
ip subnet-zero
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
  lifetime 3600
crypto isakmp key cisco address 10.1.1.17
crypto isakmp key cisco address 10.1.1.21
!
crypto gdoi group group1
  identity number 1
  server address ipv4 10.1.1.17
  server address ipv4 10.1.1.21
!
crypto map map-group1 10 gdoi
  set group group1
!
interface Ethernet0/0
  ip address 10.1.1.1 255.255.255.252
  crypto map map-group1
!
router bgp 1000
  no synchronization
  bgp log-neighbor-changes
  network 10.1.1.0 mask 255.255.255.0
  neighbor 10.1.1.2 remote-as 5000
  no auto-summary
!
ip classless
!
End

```

Group Member 2: Example

Group Member 2 is part of a GDOI group that correlates with a VPN with which these sites are a part.

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname GM2
!
resource policy
!
clock timezone EST 0
ip subnet-zero

```

```

!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
  lifetime 3600
crypto isakmp key cisco address 10.1.1.17
crypto isakmp key cisco address 10.1.1.21
!
crypto gdoi group group1
  identity number 1
  server address ipv4 10.1.1.17
  server address ipv4 10.1.1.21
!
crypto map map-group1 10 gdoi
  set group group1
!
interface Ethernet0/0
  ip address 10.1.1.5 255.255.255.252
  crypto map map-group1
!
router bgp 2000
  no synchronization
  bgp log-neighbor-changes
  network 10.1.2.0 mask 255.255.255.0
  neighbor 10.1.1.6 remote-as 5000
  no auto-summary
!
ip classless
!
end

```

Group Member 3: Example

Group Member 3 is part of a GDOI group that correlates with a VPN with which these sites are a part.

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GM3
!
resource policy
!
clock timezone EST 0
ip subnet-zero
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
  lifetime 3600
crypto isakmp key cisco address 10.1.1.17
crypto isakmp key cisco address 10.1.1.21
!
crypto ipsec transform-set gdoi-trans-group1 esp-3des esp-sha-hmac
crypto gdoi group group1
  identity number 1
  server address ipv4 10.1.1.17
  server address ipv4 10.1.1.21
!

```

```

crypto map map-group1 10 gdoi
  set group group1
!
interface Ethernet0/0
  ip address 10.1.1.9 255.255.255.252
  crypto map map-group1
!
router bgp 3000
  no synchronization
  bgp log-neighbor-changes
  network 10.1.3.0 mask 255.255.255.0
  neighbor 10.1.1.10 remote-as 5000
  no auto-summary
!
ip classless
!
end

```

Group Member 4: Example

Group Member 4 is part of a GDOI group that correlates with a VPN with which these sites are a part.

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GM4
!
clock timezone EST 0
ip subnet-zero
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
  lifetime 3600
crypto isakmp key cisco address 10.1.1.17
crypto isakmp key cisco address 10.1.1.21
!
crypto gdoi group group1
  identity number 1
  server address ipv4 10.1.1.17
  server address ipv4 10.1.1.21
!
crypto map map-group1 10 gdoi
  set group group1
!
interface Ethernet0/0
  ip address 10.1.1.13 255.255.255.252
  crypto map map-group1
!
router bgp 4000
  no synchronization
  bgp log-neighbor-changes
  network 10.1.4.0 mask 255.255.255.0
  neighbor 10.1.1.14 remote-as 5000
  no auto-summary
!
ip classless
!
end

```


Additional References

The following sections provide references related to the Cisco Group Encrypted Transport VPN feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands (listed in an index)	Cisco IOS Master Commands List , Release 12.4
Cisco IOS security commands	Cisco IOS Security Command Reference , Release 12.4T
Configuring IKE and IKE policy	“ Configuring Internet Key Exchange for IPSec VPNs ” section of the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4
Configuring an IPsec transform	“ Configuring Security for VPNs with IPSec ” section of the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4

Standards

Standard	Title
No new or modified standards are supported by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 3547	The Group Domain of Interpretation

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features. For information about these commands, see the *Cisco IOS Security Command Reference* at

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at

<http://tools.cisco.com/Support/CLILookup> or the Master Commands List.

- **address ipv4 (GDOI)**
- **clear crypto gdoi**
- **crypto gdoi gm**
- **debug crypto gdoi**
- **local priority**
- **peer address ipv4**
- **redundancy (GDOI)**
- **rekey address ipv4**
- **rekey transport unicast**
- **replay counter window-size**
- **replay time window-size**
- **sa receive-only**
- **show crypto gdoi**

Feature Information for Cisco Group Encrypted Transport VPN

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Cisco Group Encrypted Transport VPN

Feature Name	Releases	Feature Information
Secure Multicast	12.4(6)T	The secure multicast part of this feature was first introduced in Cisco IOS Release 12.4(6)T in <i>Secure Multicast</i> . However, all pertinent information from that document has been integrated and updated in this current document (<i>Cisco Group Encrypted Transport VPN</i>).
Cisco Group Encrypted Transport VPN	12.4(11)T	Cisco Group Encrypted Transport VPN is an optimal encryption solution for large-scale IP or MPLS sites that require any-to-any connectivity with minimum convergence time, low processing, provisioning, managing, and troubleshooting overhead. The following commands were introduced or modified: address ipv4 (GDOI), clear crypto gdoi, crypto gdoi gm, debug crypto gdoi, local priority, peer address ipv4, redundancy, rekey address ipv4, rekey transport unicast, replay counter window-size, replay time window-size, sa receive-only, show crypto gdoi.
VSA Support for GET VPN	12.4(15)T5	Cisco VSA (high-performance crypto engine) support was added for GDOI and GET VPN. Note This platform does not support time-based anti-replay.

Glossary

DOI—Domain of Interpretation. For Internet Security Association Key Management Protocol (ISAKMP), a value in the security association (SA) payload that describes in which context the key management message is being sent (IPsec or Group Domain of Interpretation).

GDOI—Group Domain of Interpretation. For ISAKMP, a means of distributing and managing keys for groups of mutually trusted systems.

group member—Device (Cisco IOS router) that registers with a group that is controlled by the key server for purposes of communicating with other group members.

group security association—SA that is shared by all group members in a group.

IPsec—IP security. Data encryption protocol for IP packets that are defined in a set of RFCs (see IEEE RFC 2401).

ISAKMP—Internet Security Association and Key Management Protocol. Protocol that provides a framework for cryptographic key management protocols.

KEK—key encryption key. Key used to protect the rekey between the key server and group members.

key server—Device (Cisco IOS router) that distributes keys and policies to group members.

MTU—maximum transmission unit. Size (in bytes) of the largest packet or frame that a given layer of a communications protocol can pass onward.

SA—security association. SA that is shared by all group members in a group.

TEK—traffic encryption key. Key that is used to protect the rekey between group members.

**Note**

See [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

Appendix I: System Messages

Table 2 lists GET VPN system messages and explanations.

Table 2 GET VPN System Messages

Error Messages	Explanation
COOP_CONFIG_MISMATCH	The configuration between the primary key server and secondary key server are mismatched.
COOP_KS_ADD	A key server has been added to the list of cooperative key servers in a group.
COOP_KS_ELECTION	The local key server has entered the election process in a group.
COOP_KS_REACH	The reachability between the configured cooperative key servers is restored.
COOP_KS_REMOVE	A key server has been removed from the list of cooperative key servers in a group.
COOP_KS_TRANS_TO_PRI	The local key server transitioned to a primary role from being a secondary server in a group.
COOP_KS_UNAUTH	An authorized remote server tried to contact the local key server in a group. Could be considered a hostile event.
COOP_KS_UNREACH	The reachability between the configured cooperative key servers is lost. Could be considered a hostile event.
COOP_KS_VER_MISMATCH	Key servers are running different versions of the IOS code.
COOP_PACKET_DROPPED	Hard limit set on the driver buffer size prevents the sending of packets this size or bigger.
GDOI-3-GM_NO_CRYPTTO_ENGINE	No crypto engine is found due to lack of resource or unsupported feature requested.
GDOI_ACL_NUM	The ACL has too many entries. GDOI will honor only the first 100 ACL entries specified.
GDOI_REKEY_FAILURE	During GDOI rekey the payload parsing failed on this group member from the key server.
GM_ACL_MERGE	The ACL differences between a group member and key server are resolved and a merge took place.
GM_ACL_PERMIT	The group member can support only an ACL for “deny.” Any traffic matching the “permit” entry will be dropped.
GM_CLEAR_REGISTER	The clear crypto gdoi command has been executed by the local group member.
GM_CM_ATTACH	A crypto map has been attached for the local group member.
GM_CM_DETACH	A crypto map has been detached for the local group member.
GM_CONV_SA_DUPLEX	IPsec SAs have been converted to bidirectional mode in a group on a group member.

Table 2 GET VPN System Messages (continued)

Error Messages	Explanation
GM_CONV_SA_DUPLEX_LOCAL	IPsec SAs have been converted to bidirectional mode in a group on a group member by a CLI command.
GM_ENABLE_GDOI_CM	Group member has enabled ACL on a GDOI crypto map in a group with a key server.
GM_HASH_FAIL	During GDOI registration protocol, a message sent by the key server has bad or no hash.
GM_INCOMPLETE_CFG	Registration cannot be completed because the GDOI group configuration may be missing the group ID, server ID, or both.
GM_NO_IPSEC_FLOWS	Hardware limitation for IPsec flow limit reached. Cannot create any more IPsec SAs.
GM_RE_REGISTER	IPsec SA created for one group may have been expired or cleared. Need to reregister to the key server.
GM_RECV_DELETE	A message sent by the key server to delete the group member has been received.
GM_RECV_REKEY	Rekey received.
GM_REGS_COMPL	Registration complete.
GM_REJECTING_SA_PAYLOAD	During GDOI registration protocol, a proposal sent by the key server was refused by the local group member.
GM_REKEY_NOT_REC'D	Group member has not received a rekey message from a key server in a group. Currently unimplemented.
GM_REKEY_TRANS_2_MULTI	Group member has transitioned from using a unicast rekey mechanism to using a multicast mechanism.
GM_REKEY_TRANS_2_UNI	Group member has transitioned from using a multicast rekey mechanism to using a unicast mechanism.
GM_SA_INGRESS	Received-only ACL has been received by a group member from a key server in a group.
GM_UNREGISTER	A group member has left the group.
KS_BAD_ID	Configuration mismatch between a local key server and a group member during GDOI registration protocol.
KS_BLACKHOLE_ACK	Key server has reached a condition of blackholing messages from a group member. Could be considered a hostile event.
KS_CLEAR_REGISTER	The clear crypto gdoi command has been executed by the local key server.
KS_CONV_SAS_DUPLEX	IPsec SAs have been converted to bidirectional mode in a group.
KS_CONV_SAS_INGRESS	IPsec SAs have been converted to receive-only mode in a group.
KS_FIRST_GM, GDOI, LOG_INFO	Local key server has received the first group member joining the group.

Table 2 **GET VPN System Messages (continued)**

Error Messages	Explanation
KS_GM_REJECTS_SA_PAYLOAD	During GDOI registration protocol, a proposal sent by the key server was refused by the group member.
KS_GM_REVOKED	During rekey protocol, an unauthorized member tried to join a group. Could be considered a hostile event.
KS_GROUP_ADD	A configuration command has been executed to add a key server in a group.
KS_GROUP_DELETE	A configuration command has been executed to remove a key server from a group.
KS_HASH_FAIL	During GDOI registration protocol, a message sent by the group member has bad or no hash.
KS_LAST_GM	Last group member has left the group on the local key server.
KS_NACK_GM_EJECT	Key server has reached a condition of not receiving an ACK message from group member and has been ejected.
KS_NO_RSA_KEYS	RSA keys were not created or they are missing.
KS_REGS_COMPL	Key server has successfully completed a registration in a group.
KS_REKEY_TRANS_2_MULTI	Group has transitioned from using a unicast rekey mechanism to a multicast mechanism.
KS_REKEY_TRANS_2_UNI	Group has transitioned from using a multicast rekey mechanism to using a unicast mechanism.
KS_SEND_MCAST_REKEY	Sending multicast rekey.
KS_SEND_UNICAST_REKEY	Sending unicast rekey.
KS_UNAUTHORIZED	During GDOI registration protocol, an unauthorized member tried to join a group. Could be considered a hostile event.
KS_UNSol_ACK	Key server has received an unsolicited ACK message from a past group member or is under a DOS attack. Could be considered a hostile event.
PSEUDO_TIME_LARGE	A group member has received a pseudotime with a value that is largely different from its own pseudotime.
REPLAY_FAILED	A group member or key server has failed an anti-replay check.
UNAUTHORIZED_IDENTITY	The registration request was dropped because the requesting device was not authorized to join the group.
UNAUTHORIZED_IPADDR	The registration request was dropped because the requesting device was not authorized to join the group.
UNEXPECTED_SIGKEY	Unexpected signature key found: freeing the signature key.
UNREGISTERED_INTERFACE	Receiving registration from unregistered interface. Stop processing it.
UNSUPPORTED_TEK_PROTO	Unexpected TEK protocol.

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

©2006–2008 Cisco Systems, Inc. All rights reserved.



Crypto Access Check on Clear-Text Packets

The Crypto Access Check on Clear-Text Packets feature removes the checking of clear-text packets that go through the IP Security (IPSec) tunnel just prior to encryption or just after decryption. The clear-text packets were checked against the outside physical interface access control lists (ACLs). This checking was often referred to as a double ACL check. This feature enables easier configuration of ACLs and eliminates the security risks that are associated with a double check when using dynamic crypto maps.

Feature History for Crypto Access Check on Clear-Text Packets

Release	Modification
12.3(8)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel**

Contents

- [Prerequisites for Crypto Access Check on Clear-Text Packets, page 2](#)
- [Restrictions for Crypto Access Check on Clear-Text Packets, page 2](#)
- [Information About Crypto Access Check on Clear-Text Packets, page 2](#)
- [How to Configure Crypto Map Access ACLs, page 6](#)
- [Configuration Examples for Crypto Access Check on Clear-Text Packets, page 8](#)
- [Additional References, page 14](#)
- [Command Reference, page 15](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for Crypto Access Check on Clear-Text Packets

-
-

Restrictions for Crypto Access Check on Clear-Text Packets

- This feature does not apply to IPSec configurations on the Virtual Private Network (VPN) service module (card) on Cisco Catalyst 6500 series switches and Cisco 7600 series router platforms.

This feature supports only extended ACLs.

Information About Crypto Access Check on Clear-Text Packets

-
-
- [How ACL Access Checking Worked Prior to This Feature, page 3](#)
- [ACL Checking Behavior After Upgrading to This Feature, page 4](#)
- [Backward Compatibility, page 6](#)

Crypto Access Check on Clear-Text Packets Overview

-
-
-
-

Configuration Changes That Are Required for This Feature

Prior to Upgrading

After Upgrading

-

used because when the IPSec tunnel is not “up,” the ACEs will allow the clear-text packets into the network. If dynamic crypto maps are not being used, the ACEs can still be removed to simplify the outside interface ACLs.

Check all outside interfaces for outbound ACLs that contain ACEs that permit outbound clear-text packets that would be encrypted. These ACEs need to be removed if dynamic crypto maps are being used because when the IPSec tunnel is not up, these ACEs will allow the clear-text packets out of the network. If dynamic crypto maps are not being used, these ACEs can still be removed to simplify the outside interface ACLs.

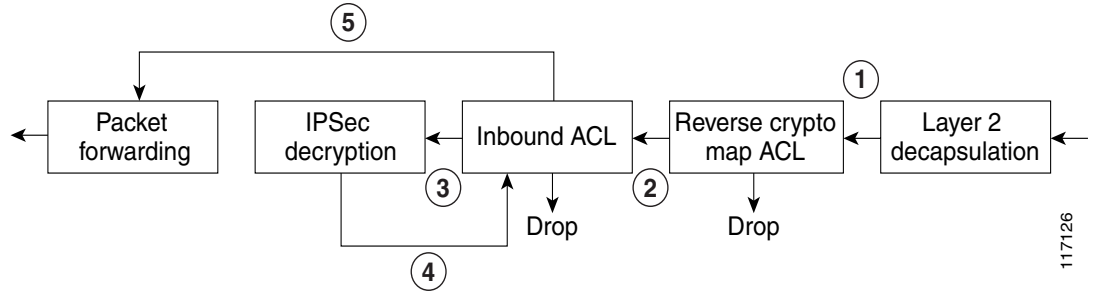
Add an outbound crypto map access ACL under the crypto map to deny to-be-encrypted, outbound clear-text packets that should be dropped. Be sure that you also permit all other packets in this ACL.

Add an inbound crypto map access ACL under the crypto map to deny just-decrypted, inbound clear-text packets that should be dropped. Be sure to also permit all other packets in this ACL.

The last two configuration changes are needed only in the rare cases in which the crypto map ACL (that selects packets to be encrypted) is more general than the packet flows that you want to encrypt. Adding outbound or inbound crypto map ACLs is usually done to keep the crypto map ACL small and simple, which saves CPU utilization and memory. The **set ip access-group**

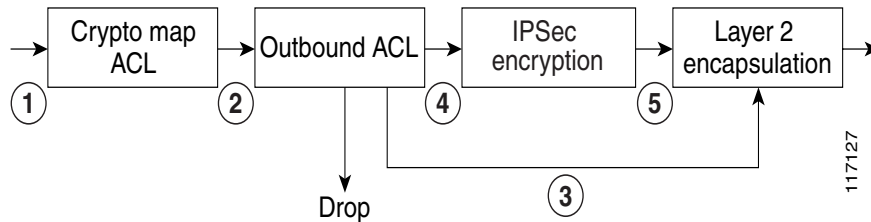
How ACL Access Checking Worked Prior to This Feature

Figure 1 *Inbound Encrypted Packet Flow Prior to This Feature*



- 1.
- 2.
- 3.
4. Just-decrypted IP packet is again checked against the interface inbound ACL. If denied, it is dropped.
- 5.

Figure 2 *Outbound Encrypted Packet Flow Prior to This Feature*



Departing IP packet is checked against the crypto map ACL. If permitted, the packet is marked for encryption.

All IP packets are checked against the outbound interface ACL. If denied, they are dropped.

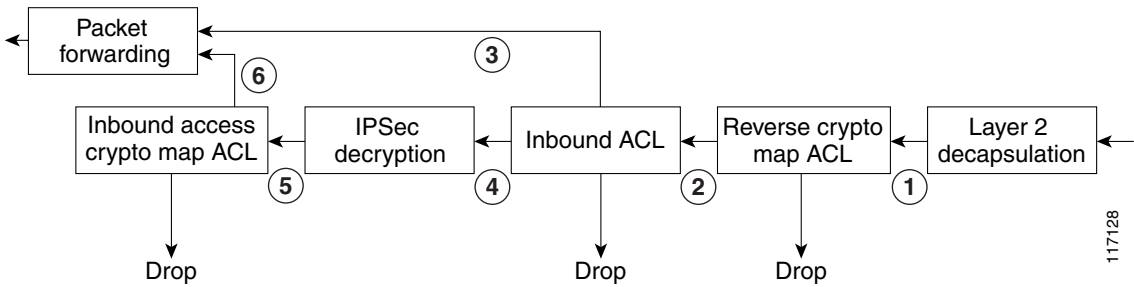
IP packets not marked for encryption are Layer 2 encapsulated.

IP packets marked for encryption are encrypted.

Encrypted IP packets are Layer 2 encapsulated.

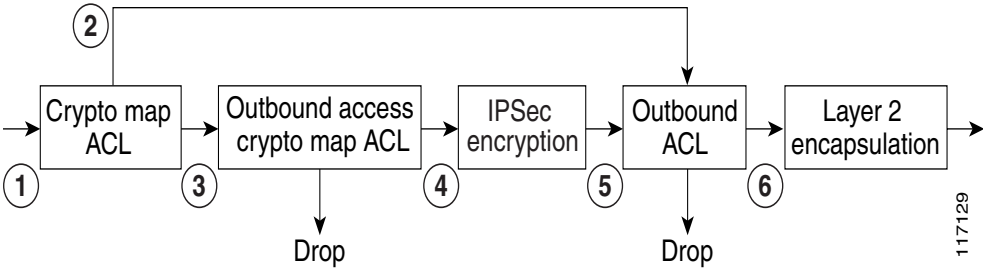
ACL Checking Behavior After Upgrading to This Feature

Figure 3 *New Inbound Encrypted Packet Flow*



6.

Figure 4 *New Outbound Encrypted Packet Flow*



Backward Compatibility

How to Configure Crypto Map Access ACLs

-
-

Adding or Removing ACLs

SUMMARY STEPS

1. **enable**
2. **configure terminal**
crypto map *map-name seq-number*
{access-list-number | access-list-name} { | }

DETAILED STEPS

Command or Action	Purpose
enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
configure terminal Router# configure terminal	
crypto map <i>map-name seq-number</i> Router(config)# crypto map vpn1 10	access ACL; also enters crypto map configuration mode.
set ip access-group { <i>access-list-number</i> <i>access-list-name</i> } { } Router(config-crypto-map)# set ip access-group 151 in	

Verifying the Configured ACLs

show ip access-list

show crypto map

enable

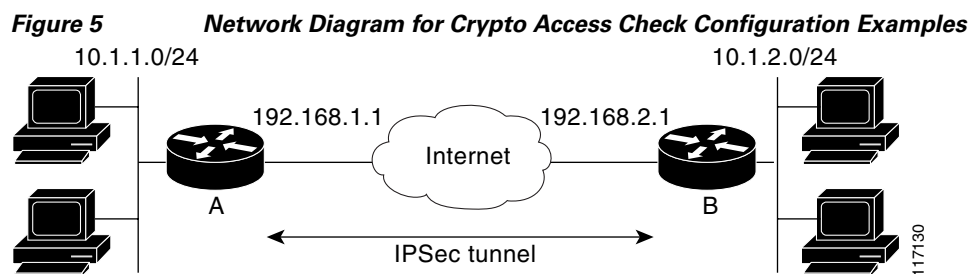
```
show ip access-list [ access-list-number | access-list-name | dynamic ]
                    [ interface | map-name ]
```

<pre>show ip access-list [dynamic]</pre>	
<pre>Router# show ip access-list Internetfilter</pre>	
<pre>show crypto map interface interface map-name</pre>	

Configuration Examples for Crypto Access Check on Clear-Text Packets

- [New IPSec ACL Configuration Without Crypto Access ACLs: Example, page 9](#)
[New IPSec ACL Configuration with Crypto Access ACLs: Example, page 10](#)
[Authentication Proxy, IPSec, and CBAC Configuration: Example](#)

The network diagram used for the following examples is shown in [Figure 5](#).



Previous IPSec ACL Configuration: Example

```
crypto map vpnmap 10 ipsec-isakmp
  set peer 192.168.2.1
  set transform-set trans1
  match address 101

interface Ethernet0/0
  ip address 10.1.1.1 255.255.255.0
interface Serial1/0
  ip address 192.168.1.1 255.255.255.0
  ip access-group 150 in
  ip access-group 160 out
  crypto map vpnmap

access-list 101 permit ip 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255
access-list 150 permit udp host 192.168.2.1 eq 500 host 192.168.1.1 eq 500
access-list 150 permit esp host 192.168.2.1 host 192.168.1.1
access-list 150 permit ip 10.1.2.0 0.0.0.255 10.1.1.0 0.0.0.255

access-list 160 permit udp host 192.168.1.1 eq 500 host 192.168.2.1 eq 500
access-list 160 permit ip 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255
```

New IPSec ACL Configuration Without Crypto Access ACLs: Example

```
crypto map vpnmap 10 ipsec-isakmp
  set peer 192.168.2.1
  set transform-set trans1
  match address 101

interface Ethernet0/0
  ip address 10.1.1.1 255.255.255.0
interface Serial1/0
  ip address 192.168.1.1 255.255.255.0
  ip access-group 150 in
  ip access-group 160 out
  crypto map vpnmap
access-list 101 permit ip 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255

access-list 150 permit udp host 192.168.2.1 eq 500 host 192.168.1.1 eq 500
access-list 150 permit esp host 192.168.2.1 host 192.168.1.1

access-list 160 permit udp host 192.168.1.1 eq 500 host 192.168.2.1 eq 500
access-list 160 permit esp host 192.168.1.1 host 192.168.2.1
```

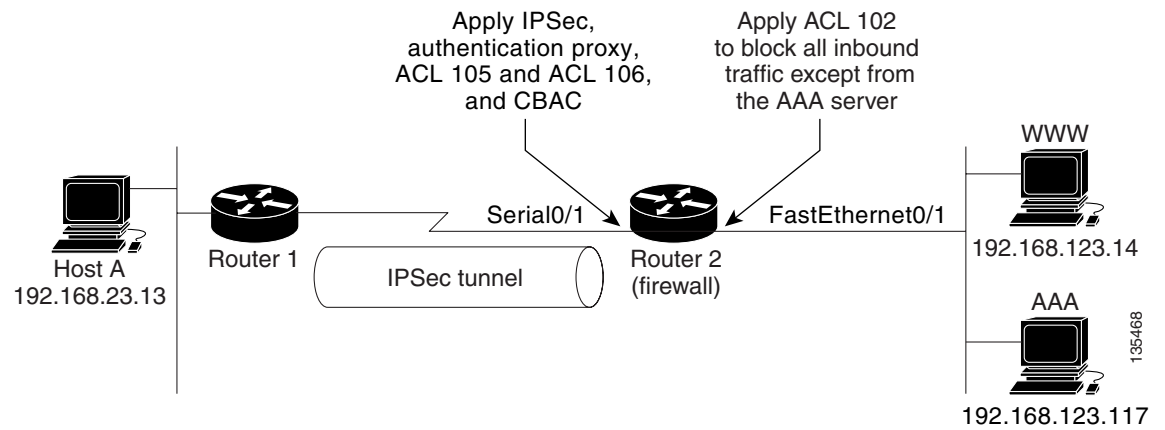


Note

Authentication Proxy, IPSec, and CBAC Configuration: Example



Note

Figure 6 Router Configuration Using Authentication Proxy, IPSec, and CBAC Features**Router 1 Configuration Example**

```

version 12.3
service timestamps debug uptime
service timestamps log uptime
!
hostname Router1
!
boot-start-marker
boot-end-marker
!
ip subnet-zero
ip cef
!
!
no ip dhcp use vrf connected
!
!
no ip ips deny-action ips-interface
!
no ftp-server write-enable
!
!
crypto isakmp policy 1

```

```

    authentication pre-share
crypto isakmp key cisco1234 address 10.0.0.2
!
!
crypto ipsec transform-set rule_1 ah-sha-hmac esp-des esp-sha-hmac
!
crypto map testtag 10 ipsec-isakmp
    set peer 10.0.0.2
    set transform-set rule_1
    match address 155
!
!
interface FastEthernet0/0
    ip address 192.168.23.2 255.255.255.0
    speed auto
!
interface Serial1/1
    ip address 10.0.0.1 255.0.0.0
    encapsulation ppp
    clockrate 2000000
    crypto map testtag
!
ip classless
ip route 192.168.123.0 255.255.255.0 10.0.0.2
!
no ip http server
no ip http secure-server
!
access-list 155 permit ip 192.168.23.0 0.0.0.255 192.168.123.0 0.0.0.255
!
control-plane
!
!
line con 0
    exec-timeout 0 0
line aux 0
line vty 0 4
!
end

```

Router 2 Configuration Example

```

version 12.3
service timestamps debug uptime
service timestamps log uptime
!
hostname Router2
!
boot-start-marker
boot-end-marker
!
!
resource policy
!
aaa new-model
!
!
aaa authentication login default group tacacs+
aaa authentication login console none
aaa authorization auth-proxy default group tacacs+
!
aaa session-id common
clock timezone MST -8
clock summer-time MDT recurring

```

```
no network-clock-participate slot 1
no network-clock-participate wic 0
ip subnet-zero
!
!
no ip dhcp use vrf connected
!
!
ip cef
ip inspect name rule22 tcp
ip inspect name rule22 ftp
ip inspect name rule22 smtp
ip auth-proxy name pxy http inactivity-time 60
no ip ips deny-action ips-interface
!
no ftp-server write-enable
!
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco1234 address 10.0.0.1
!
!
crypto ipsec transform-set rule_1 ah-sha-hmac esp-des esp-sha-hmac
!
crypto map testtag 10 ipsec-isakmp
 set peer 10.0.0.1
 ! Define crypto access check to filter traffic after IPSec decryption
 ! Authentication-proxy downloaded ACEs will be added to this ACL,
 ! not interface ACL.
 set ip access-group 106 in
 set transform-set rule_1
 match address 155
!
!
interface FastEthernet0/1
 ip address 192.168.123.2 255.255.255.0
 ip access-group 102 in
 duplex auto
 speed auto
!
interface Serial0/1
 ip address 10.0.0.2 255.0.0.0
 ip access-group 105 in
 ip inspect rule22 in
 ip auth-proxy pxy
 encapsulation ppp
 crypto map testtag
!
no ip classless
ip route 192.168.23.0 255.255.255.0 10.0.0.1
!
!
ip http server
ip http access-class 15
ip http authentication aaa
no ip http secure-server
!
access-list 15 deny any
access-list 102 permit tcp host 192.168.123.20 117 eq tacacs host 192.168.123.2
! ACL 155 is interface ACL which allows only IPSec traffic
access-list 105 permit ahp any any
access-list 105 permit esp any any
access-list 105 permit udp any any eq isakmp
```

TACAC+ User Profile Example

```
user = http_1 {  
    default service = permit  
    login = cleartext mypassword  
    service = auth-proxy  
    {  
        priv-lvl=15  
        proxyacl#1="permit tcp any any eq 23"  
        proxyacl#2="permit tcp any any eq 21"  
        proxyacl#3="permit tcp any any eq 25"  
        proxyacl#4="permit tcp any any eq 80"  
        proxyacl#5="permit udp any any eq 53"
```

ACL 106, Before Auth-Proxy Authentication

```
show access-list 106
```

```
show access-list 106
```

Additional References

Related Documents

Related Topic	Document Title
	Implementing IPsec and IKE ” section of the <i>Cisco IOS Security Configuration Guide</i>
	<i>Cisco IOS Security Configuration Guide</i>
	Cisco IOS Security Command Reference

Standards

Standards	Title
	—

MIBs

MIBs	MIBs Link

RFCs

RFCs	Title
	—

Technical Assistance

Description	Link

Command Reference

-
- **show crypto map (IPSec)**

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



DF Bit Override Functionality with IPSec Tunnels

Feature History

Release	Modification
Cisco IOS	For information about feature support in Cisco IOS software, use Cisco Feature Navigator.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

This feature module describes the DF Bit Override Functionality with IPSec Tunnels feature and contains the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 2](#)
- [Supported Standards, MIBs, and RFCs, page 3](#)
- [Prerequisites, page 3](#)
- [Configuration Tasks, page 4](#)
- [Configuration Examples, page 4](#)
- [Command Reference, page 5](#)

Feature Overview

The DF Bit Override Functionality with IPSec Tunnels feature allows customers to specify whether their router can clear, set, or copy the Don't Fragment (DF) bit from the encapsulated header. A DF bit is a bit within the IP header that determines whether a router is allowed to fragment a packet.

Some customer configurations have hosts that perform the following functions:

- Set the DF bit in packets they send
- Use firewalls that block Internet Control Message Protocol (ICMP) errors from outside the firewall, preventing hosts from learning about the maximum transmission unit (MTU) size outside the firewall
- Use IP Security (IPSec) to encapsulate packets, reducing the available MTU size



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Customers whose configurations have hosts that prevent them from learning about their available MTU size can configure their router to clear the DF bit and fragment the packet.

**Note**

In compliance with RFC 2401, this feature can be configured globally or per interface. If both levels are configured, the interface configuration will override the global configuration.

Benefits

The DF Bit Override Functionality with IPSec Tunnels feature allows customers to configure the setting of the DF bit when encapsulating tunnel mode IPSec traffic on a global or per-interface level. Thus, if the DF bit is set to clear, routers can fragment packets regardless of the original DF bit setting.

Restrictions

Performance Impact

Because each packet is reassembled at the process level, a significant performance impact occurs at a high data rate. Two major caveats are as follows:

- The reassemble queue can fill up and force fragments to be dropped.
- The traffic is slower because of the process switching.

DF Bit Setting Requirement

If several interfaces share the same crypto map using the local address feature, these interfaces must share the same DF bit setting.

Feature Availability

This feature is available only for IPSec tunnel mode. (IPSec transport mode is not affected because it does not provide an encapsulating IP header.)

Related Documents

The following documents provide information related to the DF Bit Override Functionality with IPSec Tunnels feature:

- “Configuring IPSec Network Security” chapter, *Cisco IOS Security Configuration Guide*, Release 12.2
- “IPSec Network Security Commands” chapter, *Cisco IOS Security Command Reference*, Release 12.2

Supported Platforms

This feature is supported on the following platforms:

- Cisco 800
- Cisco 827

- Cisco 1600
- Cisco 1600R
- Cisco 1700
- Cisco 2600
- Cisco 3620
- Cisco 3640
- Cisco 3660
- Cisco 4000
- Cisco 4500
- Cisco 5200
- Cisco 5300
- Cisco 5400
- Cisco 6400
- Cisco 7100
- Cisco 7200
- Cisco 7500
- Cisco uBR7200
- Cisco uBR900
- Cisco uBR905
- Cisco uBR910

This feature runs on all platforms that support IPSec.

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBS are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

RFCs

- RFC 2401, *Security Architecture for the Internet Protocol*

Prerequisites

IPSec must be enabled on your router.

Configuration Tasks

See the following section for configuration tasks for the DF-Bit Override Functionality with IPsec Tunnels feature:

- [Configuring the DF Bit for the Encapsulating Header in Tunnel Mode](#)

Configuring the DF Bit for the Encapsulating Header in Tunnel Mode

To set the DF bit for the encapsulating header in tunnel mode, use the following command in global configuration mode:

Command	Purpose
Router(config)# crypto ipsec df-bit [clear set copy]	<p>Sets the DF bit for the encapsulating header in tunnel mode for all interfaces.</p> <p>To set the DF bit for a specified interface, use the crypto ipsec df-bit command in interface configuration mode.</p> <p>Note DF bit interface configuration settings override all DF bit global configuration settings.</p>

Verifying DF Bit Setting

To verify the current DF Bit settings on your router, use the **show running-config** command in EXEC mode.

Configuration Examples

This section provides the following configuration example:

- [DF Bit Setting Configuration Example](#)

DF Bit Setting Configuration Example

In following example, the router is configured to globally clear the setting for the DF bit and copy the DF bit on the interface named Ethernet0. Thus, all interfaces *except* Ethernet0 will allow the router to send packets larger than the available MTU size; Ethernet0 will allow the router to fragment the packet.

```
crypto isakmp policy 1
  hash md5
  authentication pre-share
crypto isakmp key Delaware address 192.168.10.66
crypto isakmp key Key-What-Key address 192.168.11.19
!
!
crypto ipsec transform-set BearMama ah-md5-hmac esp-des
```

```
crypto ipsec df-bit clear
!
!
crypto map armadillo 1 ipsec-isakmp
set peer 192.168.10.66
set transform-set BearMama
match address 101
!
crypto map basilisk 1 ipsec-isakmp
set peer 192.168.11.19
set transform-set BearMama
match address 102

!
!
interface Ethernet0
 ip address 192.168.10.38 255.255.255.0
 ip broadcast-address 0.0.0.0
 media-type 10BaseT
 crypto map armadillo
 crypto ipsec df-bit copy
!
interface Ethernet1
 ip address 192.168.11.75 255.255.255.0
 ip broadcast-address 0.0.0.0
 media-type 10BaseT
 crypto map basilisk
!
interface Serial0
 no ip address
 ip broadcast-address 0.0.0.0
 no ip route-cache
 no ip mroute-cache
```

Command Reference

The following new commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **crypto ipsec df-bit (global configuration)**
- **crypto ipsec df-bit (interface configuration)**

For information about these commands, see the Cisco IOS Security Command Reference at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Distinguished Name Based Crypto Maps

Feature History

Release	Modification
12.2(4)T	This feature was introduced.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

This feature module describes the Distinguished Name Based Crypto Map feature in Cisco IOS Release 12.2(4)T. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 2](#)
- [Supported Standards, MIBs, and RFCs, page 3](#)
- [Prerequisites, page 3](#)
- [Configuration Tasks, page 3](#)
- [Configuration Examples, page 5](#)
- [Command Reference, page 6](#)

Feature Overview

The Distinguished Name Based Crypto Maps feature allows you to configure the router to restrict access to selected encrypted interfaces for those peers with specific certificates, especially certificates with particular Distinguished Names (DNs).

Previously, if the router accepted a certificate or a shared secret from the encrypting peer, Cisco IOS did not have a method of preventing the peer from communicating with any encrypted interface other than the restrictions on the IP address of the encrypting peer. This feature allows you to configure which crypto maps are usable to a peer based on the DN that a peer used to authenticate itself, thereby, enabling you to control which encrypted interfaces a peer with a specified DN can access.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Benefits

The Distinguished Name Based Crypto Maps feature allows you to set restrictions in the router configuration that prevent peers with specific certificates—especially certificates with particular DNs—from having access to selected encrypted interfaces.

Restrictions

System Requirements

To configure this feature, your router must support IP Security.

Performance Impact

If you restrict access to a large number of DNs, it is recommended that you specify a few number of crypto maps referring to large identity sections instead of specifying a large number of crypto maps referring to small identity sections.

Related Documents

The following documents provide information related to the Distinguished Name Based Crypto Maps feature:

- *Cisco IOS Security Command Reference*, Release 12.2
- *Cisco IOS Security Configuration Guide*, Release 12.2

Supported Platforms

This feature is supported on the following platforms:

- Cisco 1700 series
- Cisco 2600 series
- Cisco 3620
- Cisco 3640
- Cisco 3660
- Cisco 7100 series
- Cisco 7200 series
- Cisco uBR905 Cable Access Router
- Cisco uBR925 Cable Access Router

Determining Platform Support Through Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Feature Navigator. Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Feature Navigator home page at the following URL: <http://www.cisco.com/go/fn>

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

RFCs

None

Prerequisites

Before configuring a DN based crypto map, you must perform the following tasks:

- Create an Internet Key Exchange (IKE) policy at each peer.
For more information on creating IKE policies, refer to the chapter “Configuring Internet Key Exchange Security Protocol” of the *Cisco IOS Security Configuration Guide*.
- Create crypto map entries for IPsec.
For more information on creating crypto map entries, refer to the chapter “Configuring IPsec Network Security” of the *Cisco IOS Security Configuration Guide*.

Configuration Tasks

See the following sections for configuration tasks for the Distinguished Name Based Crypto Maps feature. Each task in the list is identified as either required or optional.

- [Configuring DN Based Crypto Maps \(authenticated by DN\)](#) (required)
- [Configuring DN Based Crypto Maps \(authenticated by hostname\)](#) (required)
- [Applying Identity to DN Based Crypto Maps](#) (required)
- [Verifying DN Based Crypto Maps](#) (optional)

Configuring DN Based Crypto Maps (authenticated by DN)

To configure a DN based crypto map that can be used only by peers that have been authenticated by a DN, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<code>Router(config)# crypto identity name</code>	Configures the identity of a router with the given list of DNs in the certificate of the router and enters crypto identity configuration mode.
Step 2	<code>Router(crypto-identity)# dn name=string [,name=string]</code>	Associates the identity of the router with the DN in the certificate of the router. Note The identity of the peer must match the identity in the exchanged certificate.

Configuring DN Based Crypto Maps (authenticated by hostname)

To configure a DN based crypto map that can be used only by peers that have been authenticated by a hostname, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<code>Router(config)# crypto identity name</code>	Configures the identity of a router with the given list of DNs in the certificate of the router and enters crypto identity configuration mode.
Step 2	<code>Router(crypto-identity)# fqdn name</code>	Associates the identity of the router with the hostname that the peer used to authenticate itself. Note The identity of the peer must match the identity in the exchanged certificate.

Applying Identity to DN Based Crypto Maps

To apply the identity (within the crypto map context), use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# crypto map <i>map-name seq-num ipsec-isakmp</i>	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
Step 2	Router(config-crypto-map)# identity <i>name</i>	<p>Applies the identity to the crypto map.</p> <p>When this command is applied, only the hosts that match a configuration listed within the identity <i>name</i> can use the specified crypto map.</p> <p>Note If the identity command does not appear within the crypto map, the encrypted connection does not have any restrictions other than the IP address of the encrypting peer.</p>

Verifying DN Based Crypto Maps

To verify that this functionality is properly configured, use the following command in EXEC mode:

Command	Purpose
Router# show crypto identity	Displays the configured identities.

Troubleshooting Tips

If an encrypting peer attempts to establish a connection that is blocked by the DN based crypto map configuration, the following error message will be logged:

```
<time>: %CRYPTO-4-IKE_QUICKMODE_BAD_CERT: encrypted connection attempted with a peer
without the configured certificate attributes.
```

Configuration Examples

This section provides the following configuration example:

- [DN Based Crypto Map Configuration Example](#)

DN Based Crypto Map Configuration Example

The following example shows how to configure DN based crypto maps that have been authenticated by DN and hostname. Comments are included inline to explain various commands.

```
! DN based crypto maps require you to configure an IKE policy at each peer.
crypto isakmp policy 15
  encryption 3des
  hash md5
  authentication rsa-sig
  group 2
  lifetime 5000
crypto isakmp policy 20
```

```

authentication pre-share
lifetime 10000
crypto isakmp key 1234567890 address 171.69.224.33
!
! The following is an IPSec crypto map (part of IPSec configuration). It can be used only
! by peers that have been authenticated by DN and if the certificate belongs to BigBiz.
crypto map map-to-bigbiz 10 ipsec-isakmp
set peer 172.21.114.196
set transform-set my-transformset
match address 124
identity to-bigbiz
!
crypto identity to-bigbiz
dn ou=BigBiz
!
!
! This crypto map can be used only by peers that have been authenticated by hostname
! and if the certificate belongs to little.com.
crypto map map-to-little-com 10 ipsec-isakmp
set peer 172.21.115.119
set transform-set my-transformset
match address 125
identity to-little-com
!
crypto identity to-little-com
fqdn little.com
!

```

Command Reference

The following new commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **crypto identity**
- **dn**
- **fqdn**
- **identity**

For information about these commands, see the Cisco IOS Security Command Reference at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Dynamic Multipoint VPN (DMVPN)

First Published: November 25, 2002

Last Updated: December 11, 2006

The Dynamic Multipoint VPN (DMVPN) feature allows users to better scale large and small IP Security (IPsec) Virtual Private Networks (VPNs) by combining generic routing encapsulation (GRE) tunnels, IPsec encryption, and Next Hop Resolution Protocol (NHRP).

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Dynamic Multipoint VPN \(DMVPN\)” section on page 53](#).

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Dynamic Multipoint VPN \(DMVPN\), page 2](#)
- [Restrictions for Dynamic Multipoint VPN \(DMVPN\), page 2](#)
- [Information About Dynamic Multipoint VPN \(DMVPN\), page 3](#)
- [How to Configure Dynamic Multipoint VPN \(DMVPN\), page 11](#)
- [Configuration Examples for Dynamic Multipoint VPN \(DMVPN\) Feature, page 31](#)
- [Additional References, page 50](#)
- [Command Reference, page 52](#)
- [Feature Information for Dynamic Multipoint VPN \(DMVPN\), page 53](#)
- [Glossary, page 54](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for Dynamic Multipoint VPN (DMVPN)

- Before a multipoint GRE (mGRE) and IPsec tunnel can be established, you must define an Internet Key Exchange (IKE) policy by using the **crypto isakmp policy** command.
- For the NAT-Transparency Aware enhancement to work, you must use IPsec transport mode on the transform set. Also, even though NAT-Transparency can support two peers (IKE and IPsec) being translated to the same IP address (using the User Datagram Protocol [UDP] ports to differentiate them [that is, Peer Address Translation (PAT)]), this functionality is not supported for DMVPN. All DMVPN spokes must have a unique IP address after they have been NAT translated. They can have the same IP address before they are NAT translated.
- To enable 2547oDMPVN—Traffic Segmentation Within DMVPN you must configure multiprotocol label switching (MPLS) by using the **mpls ip** command.

Restrictions for Dynamic Multipoint VPN (DMVPN)

- If you use the [Dynamic Creation for Spoke-to-Spoke Tunnels](#) benefit of this feature, you must use IKE certificates or wildcard preshared keys for Internet Security Association Key Management Protocol (ISAKMP) authentication.



Note

It is highly recommended that you *do not use* wildcard preshared keys because the attacker will have access to the VPN if one spoke router is compromised.

- GRE tunnel keepalives (that is, the **keepalive** command under a GRE interface) are not supported on point-to-point or multipoint GRE tunnels in a DMVPN Network.
- For best DMVPN functionality, it is recommended that you run the latest Cisco IOS software Release 12.4 mainline, 12.4T, or 12.2(18)SXF.

DMVPN Support on the Cisco 6500 and Cisco 7600

Blade-to-Blade Switchover on the Cisco 6500 and Cisco 7600

- DMVPN does not support blade-to-blade switchover on the Cisco 6500 and Cisco 7600.

Cisco 6500 or Cisco 7600 As a DMVPN Hub

- A Cisco 6500 or Cisco 7600 that is functioning as a DMVPN hub cannot be located behind a NAT router.
- If a Cisco 6500 or Cisco 7600 is functioning as a DMVPN hub, the spoke behind NAT must be a Cisco 6500 or Cisco 7600, respectively, or the router must be upgraded to Cisco IOS software Release 12.3(11)T02 or a later release.

Cisco 6500 or Cisco 7600 As a DMVPN Spoke

- If a Cisco 6500 or Cisco 7600 is functioning as a spoke, the hub cannot be behind NAT.
- If a Cisco 6500 or Cisco 7600 is functioning as a DMVPN spoke behind NAT, the hub must be a Cisco 6500 or Cisco 7600, respectively, or the router must be upgraded to Cisco IOS Release 12.3(11)T02 or a later release.

DMVPN Hub or Spoke Supervisor Engine

- Only a Supervisor Engine 720 can be used as a DMVPN hub or spoke. A Supervisor Engine 2 cannot be used.

Encrypted Multicast with GRE

- Encrypted Multicast with GRE is not supported on the Cisco 6500 nor on the Cisco 7600.

mGRE Interfaces

- If there are two mGRE interfaces on the same DMVPN node and they both do not have a tunnel key, the two mGRE interfaces must each have a unique tunnel source address (or interface) configured.
- On the Cisco 6500 and Cisco 7600, each GRE interface (multipoint or point-to-point) must have a unique tunnel source address (or interface).
- The following commands are not supported under mGRE with DMVPN: **ip tcp adjust-mss**, **qos pre-classify tunnel vrf**, **tunnel path-mtu-discovery**, and **tunnel vrf**.

Quality of Service (QoS)

- You cannot use QoS for DMVPN packets on a Cisco 6500 or Cisco 7600.

Tunnel Key

- The use of a tunnel key on a GRE (multipoint or point-to-point) interface is not supported in the hardware switching ASICs on the Cisco 6500 and Cisco 7600 platforms. If a tunnel key is configured, throughput performance is greatly reduced.
- In Cisco IOS Release 12.3(11)T3 and Release 12.3(14)T, the requirement that a mGRE interface must have a tunnel key was removed. Therefore, in a DMVPN network that includes a Cisco 6500 or Cisco 7600 as a DMVPN node, you should remove the tunnel key from all DMVPN nodes in the DMVPN network, thus preserving the throughput performance on the Cisco 6500 and Cisco 7600 platforms.
- If the tunnel key is not configured on any DMVPN node within a DMVPN network, it must not be configured on all DMVPN nodes with the DMVPN network.

VRF-Aware DMVPN Scenarios

- The **mls mpls tunnel-recir** command must be configured on the provider equipment (PE) DMVPN hub if customer equipment (CE) DMVPN spokes need to “talk” to other CEs across the MPLS cloud.
- The mGRE interface should be configured with a large enough IP maximum transmission unit (1400 packets to avoid having the route processor doing fragmentation).
- Enhanced Interior Gateway Routing Protocol (EIGRP) should be avoided.

Information About Dynamic Multipoint VPN (DMVPN)

To configure the Dynamic Multipoint VPN (DMVPN) feature, you must understand the following concepts:

- [Benefits of Dynamic Multipoint VPN \(DMVPN\), page 4](#)
- [Feature Design of Dynamic Multipoint VPN \(DMVPN\), page 5](#)
- [IPsec Profiles, page 6](#)

- [VRF Integrated DMVPN, page 6](#)
- [DMVPN—Enabling Traffic Segmentation Within DMVPN, page 7](#)
- [NAT-Transparency Aware DMVPN, page 9](#)
- [Call Admission Control with DMVPN, page 10](#)
- [NHRP Rate-Limiting Mechanism, page 10](#)

Benefits of Dynamic Multipoint VPN (DMVPN)

Hub Router Configuration Reduction

- Currently, for each spoke router, there is a separate block of configuration lines on the hub router that define the crypto map characteristics, the crypto access list, and the GRE tunnel interface. This feature allows users to configure a single mGRE tunnel interface, a single IPsec profile, and no crypto access lists on the hub router to handle all spoke routers. Thus, the size of the configuration on the hub router remains constant even if spoke routers are added to the network.
- DMVPN architecture can group many spokes into a single multipoint GRE interface, removing the need for a distinct physical or logical interface for each spoke in a native IPsec installation.

Automatic IPsec Encryption Initiation

- GRE has the peer source and destination address configured or resolved with NHRP. Thus, this feature allows IPsec to be immediately triggered for the point-to-point GRE tunneling or when the GRE peer address is resolved via NHRP for the multipoint GRE tunnel.

Support for Dynamically Addressed Spoke Routers

- When using point-to-point GRE and IPsec hub-and-spoke VPN networks, the physical interface IP address of the spoke routers must be known when configuring the hub router because IP address must be configured as the GRE tunnel destination address. This feature allows spoke routers to have dynamic physical interface IP addresses (common for cable and DSL connections). When the spoke router comes online, it will send registration packets to the hub router: within these registration packets, is the current physical interface IP address of this spoke.

Dynamic Creation for Spoke-to-Spoke Tunnels

- This feature eliminates the need for spoke-to-spoke configuration for direct tunnels. When a spoke router wants to transmit a packet to another spoke router, it can now use NHRP to dynamically determine the required destination address of the target spoke router. (The hub router acts as the NHRP server, handling the request for the source spoke router.) The two spoke routers dynamically create an IPsec tunnel between them so data can be directly transferred.

VRF Integrated DMVPN

- DMVPNs can be used to extend the Multiprotocol Label Switching (MPLS) networks that are deployed by service providers to take advantage of the ease of configuration of hub and spokes, to provide support for dynamically addressed customer premises equipment (CPEs), and to provide zero-touch provisioning for adding new spokes into a DMVPN.

Feature Design of Dynamic Multipoint VPN (DMVPN)

The Dynamic Multipoint VPN (DMVPN) feature combines GRE tunnels, IPsec encryption, and NHRP routing to provide users an ease of configuration via crypto profiles—which override the requirement for defining static crypto maps—and dynamic discovery of tunnel endpoints.

This feature relies on the following two Cisco enhanced standard technologies:

- NHRP—A client and server protocol where the hub is the server and the spokes are the clients. The hub maintains an NHRP database of the public interface addresses of the each spoke. Each spoke registers its real address when it boots and queries the NHRP database for real addresses of the destination spokes to build direct tunnels.
- mGRE Tunnel Interface —Allows a single GRE interface to support multiple IPsec tunnels and simplifies the size and complexity of the configuration.

The topology shown in [Figure 1](#) and the corresponding bullets explain how this feature works.

Figure 1 *Sample mGRE and IPsec Integration Topology*



- Each spoke has a permanent IPsec tunnel to the hub, not to the other spokes within the network. Each spoke registers as clients of the NHRP server.
- When a spoke needs to send a packet to a destination (private) subnet on another spoke, it queries the NHRP server for the real (outside) address of the destination (target) spoke.
- After the originating spoke “learns” the peer address of the target spoke, it can initiate a dynamic IPsec tunnel to the target spoke.
- The spoke-to-spoke tunnel is built over the multipoint GRE interface.
- The spoke-to-spoke links are established on demand whenever there is traffic between the spokes. Thereafter, packets can bypass the hub and use the spoke-to-spoke tunnel.



Note

After a preconfigured amount of inactivity on the spoke-to-spoke tunnels, the router will tear down those tunnels to save resources (IPsec security associations [SAs]).

IPsec Profiles

IPsec profiles abstract IPsec policy information into a single configuration entity, which can be referenced by name from other parts of the configuration. Therefore, users can configure functionality such as GRE tunnel protection with a single line of configuration. By referencing an IPsec profile, the user does not have to configure an entire crypto map configuration. An IPsec profile contains only IPsec information; that is, it does not contain any access list information or peering information.

VRF Integrated DMVPN

VPN Routing and Forwarding (VRF) Integrated DMVPN enables users to map DMVPN multipoint interfaces into MPLS VPNs. This mapping allows Internet service providers (ISPs) to extend their existing MPLS VPN services by mapping off-network sites (typically a branch office) to their respective MPLS VPNs. Customer equipment (CE) routers are terminated on the DMVPN PE router, and traffic is placed in the VRF instance of an MPLS VPN.

DMVPN can interact with MPLS VPNs in two ways:

1. The **ip vrf forwarding** command is used to inject the data IP packets (those packets inside the mGRE+IPsec tunnel) into the MPLS VPN. The **ip vrf forwarding** command is supported for DMVPN in Cisco IOS Release 12.3(6) and Release 12.3(7)T.
2. The **tunnel vrf** command is used to transport (route) the mGRE+IPsec tunnel packet itself within an MPLS VPN. The **tunnel vrf** command is supported in Cisco IOS Release 12.3(11)T but not in Cisco IOS Release 12.2(18)SXE.

**Note**

Clear-text data IP packets are forwarded in a VRF using the **ip vrf forwarding** command, and encrypted tunnel IP packets are forwarded in a VRF using the **tunnel vrf** command.

The **ip vrf forwarding** and **tunnel vrf** commands may be used at the same time. If they are used at the same time, the VRF name of each command may be the same or different.

For information about configuring the forwarding of clear-text data IP packets into a VRF, see the section “[Configuring the Forwarding of Clear-Text Data IP Packets into a VRF](#).” For information about configuring the forwarding of encrypted tunnel packets into a VRF, see the section “[Configuring the Forwarding of Encrypted Tunnel Packets into a VRF](#).”

For more information about configuring VRF, see reference in the “[Related Documents](#)” section.

[Figure 2](#) illustrates a typical VRF Integrated DMVPN scenario.

Figure 2 ***VRF Integrated DMVPN***

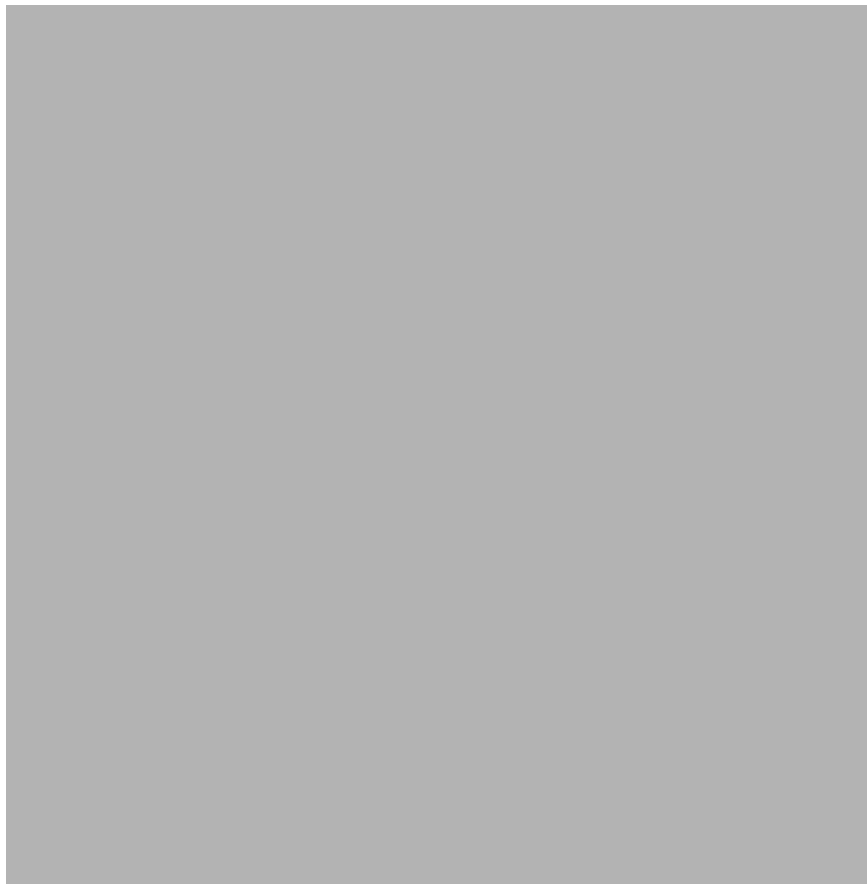


DMVPN—Enabling Traffic Segmentation Within DMVPN

Cisco IOS Release 12.4(11)T provides an enhancement that allows you to segment VPN traffic within a DMVPN tunnel. VRF instances are labeled, using MPLS, to indicate their source and destination.

The diagram in [Figure 3](#) and the corresponding bullets explain how traffic segmentation within DMVPN works.

Figure 3 **Traffic Segmentation with DMVPN**



- The hub shown in the diagram is a WAN-PE and a route reflector, and the spokes (PE routers) are clients.
- There are three VRFs, designated “red,” “green,” and “blue.”
- Each spoke has both a neighbor relationship with the hub (multiprotocol Border Gateway Protocol [MP-iBGP] peering) and a GRE tunnel to the hub.
- Each spoke advertises its routes and VPNv4 prefixes to the hub.
- The hub sets its own IP address as the next-hop route for all the VPNv4 addresses it learns from the spokes and assigns a local MPLS label for each VPN when it advertises routes back to the spokes. As a result, traffic from Spoke A to Spoke B is routed via the hub.

An example illustrates the process:

1. Spoke A advertises a VPNv4 route to the hub, and applies the label *X* to the VPN.
2. The hub changes the label to *Y* when the hub advertises the route to Spoke B.
3. When Spoke B has traffic to send to Spoke A, it applies the *Y* label, and the traffic goes to the hub.
4. The hub swaps the VPN label, by removing the *Y* label and applying an *X* label, and sends the traffic to Spoke A.

NAT-Transparency Aware DMVPN

DMVPN spokes are often situated behind a NAT router (which is often controlled by the ISP for the spoke site) with the outside interface address of the spoke router being dynamically assigned by the ISP using a private IP address (per Internet Engineering Task Force [IETF] RFC 1918).

Prior to Cisco IOS Release 12.3(6) and 12.3(7)T, these spoke routers had to use IPsec tunnel mode to participate in a DMVPN network. In addition, their assigned outside interface private IP address had to be unique across the DMVPN network. Even though ISAKMP and IPsec would negotiate NAT-T and “learn” the correct NAT public address for the private IP address of this spoke, NHRP could only “see” and use the private IP address of the spoke for its mapping entries. Effective with the NAT-Transparency Aware DMVPN enhancement, NHRP can now learn and use the NAT public address for its mappings as long as IPsec transport mode is used (which is the recommended IPsec mode for DMVPN networks). The restriction that the private interface IP address of the spoke must be unique across the DMVPN network has been removed. It is recommended that all DMVPN routers be upgraded to the new code before you try to use the new functionality even though spoke routers that are not behind NAT do not need to be upgraded. In addition, you cannot convert upgraded spoke routers that are behind NAT to the new configuration (IPsec transport mode) until the hub routers have been upgraded.

Also added in Cisco IOS Releases 12.3(9a) and 12.3(11)T is the capability to have the hub DMVPN router behind static NAT. This was a change in the ISAKMP NAT-T support. For this functionality to be used, all the DMVPN spoke routers and hub routers must be upgraded, and IPsec must use transport mode.

For these NAT-Transparency Aware enhancements to work, you must use IPsec transport mode on the transform set. Also, even though NAT-Transparency (IKE and IPsec) can support two peers (IKE and IPsec) being translated to the same IP address (using the UDP ports to differentiate them), this functionality is not supported for DMVPN. All DMVPN spokes must have a unique IP address after they have been NAT translated. They can have the same IP address before they are NAT translated.

Figure 4 illustrates a NAT-Transparency Aware DMVPN scenario.



Note

In Cisco IOS Release 12.4(6)T or earlier, DMVPN spokes behind NAT *will not* participate in dynamic direct spoke-to-spoke tunnels. Any traffic to or from a spoke that is behind NAT will be forwarded using the DMVPN hub routers. DMVPN spokes that are not behind NAT in the same DMVPN network may create dynamic direct spoke-to-spoke tunnels between each other.

In Cisco IOS Release 12.4(6)T or later releases, DMVPN spokes behind NAT *will* participate in dynamic direct spoke-to-spoke tunnels. The spokes must be behind NAT boxes that are performing NAT, not PAT. The NAT box must translate the spoke to the same outside NAT IP address for the spoke-spoke connections as the NAT box does for the spoke-hub connection. If there is more than one DMVPN spoke behind the same NAT box, then the NAT box *must* translate the DMVPN spokes to different outside NAT IP addresses. It is also likely that you may not be able to build a direct spoke-spoke tunnel between these spokes. If a spoke-spoke tunnel fails to form, then the spoke-spoke packets will continue to be forwarded via the spoke-hub-spoke path.

Figure 4 NAT-Transparency Aware DMVPN



Call Admission Control with DMVPN

In a DMVPN network, it is easy for a DMVPN router to become “overwhelmed” with the number of tunnels it is trying to build. Call Admission Control can be used to limit the number of tunnels that can be built at any one time, thus protecting the memory of the router and CPU resources.

It is most likely that Call Admission Control will be used on a DMVPN spoke to limit the total number of ISAKMP sessions (DMVPN tunnels) that a spoke router will attempt to initiate or accept. This limiting is accomplished by configuring an IKE SA limit under Call Admission Control, which configures the router to drop new ISAKMP session requests (inbound and outbound) if the current number of ISAKMP SAs exceeds the limit.

It is most likely that Call Admission Control will be used on a DMVPN hub to rate limit the number of DMVPN tunnels that are attempting to be built at the same time. The rate limiting is accomplished by configuring a system resource limit under Call Admission Control, which configures the router to drop new ISAKMP session requests (new DMVPN tunnels) when the system utilization is above a specified percentage. The dropped session requests allow the DMVPN hub router to complete the current ISAKMP session requests, and when the system utilization drops, it can process the previously dropped sessions when they are reattempted.

No special configuration is required to use Call Admission Control with DMVPN. For information about configuring Call Admission Control, see the reference in the section “[Related Documents](#).”

NHRP Rate-Limiting Mechanism

NHRP has a rate-limiting mechanism that restricts the total number of NHRP packets from any given interface. The default values, which are set using the **ip nhrp max-send** command, are 100 packets every 10 seconds per interface. If the limit is exceeded, you will get the following system message:

```
%NHRP-4-QUOTA: Max-send quota of [int]pkts/[int]Sec. exceeded on [chars]
```

For more information about this system message, see the document [12.4T System Message Guide](#).

How to Configure Dynamic Multipoint VPN (DMVPN)

To enable mGRE and IPsec tunneling for hub and spoke routers, you must configure an IPsec profile that uses a global IPsec policy template and configure your mGRE tunnel for IPsec encryption. This section contains the following procedures:

- [Configuring an IPsec Profile, page 11](#) (required)
- [Configuring the Hub for DMVPN, page 13](#) (required)
- [Configuring the Spoke for DMVPN, page 17](#) (required)
- [Configuring the Forwarding of Clear-Text Data IP Packets into a VRF, page 20](#) (optional)
- [Configuring the Forwarding of Encrypted Tunnel Packets into a VRF, page 21](#) (optional)
- [Configuring DMVPN—Traffic Segmentation Within DMVPN, page 22](#)
- [Troubleshooting Dynamic Multipoint VPN \(DMVPN\), page 27](#) (optional)

Configuring an IPsec Profile

The IPsec profile shares most of the same commands with the crypto map configuration, but only a subset of the commands are valid in an IPsec profile. Only commands that pertain to an IPsec policy can be issued under an IPsec profile; you cannot specify the IPsec peer address or the access control list (ACL) to match the packets that are to be encrypted.

Prerequisites

Before configuring an IPsec profile, you must define a transform set by using the **crypto ipsec transform-set** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec profile** *name*
4. **set transform-set** *transform-set-name*
5. **set identity**
6. **set security association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}
7. **set pfs** [*group1* | *group2*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto ipsec profile name Example: Router(config)# crypto ipsec profile vpnprof	Defines the IPsec parameters that are to be used for IPsec encryption between “spoke and hub” and “spoke and spoke” routers. This command enters crypto map configuration mode. <ul style="list-style-type: none"> The <i>name</i> argument specifies the name of the IPsec profile.
Step 4	set transform-set transform-set-name Example: Router(config-crypto-map)# set transform-set trans2	Specifies which transform sets can be used with the IPsec profile. <ul style="list-style-type: none"> The <i>transform-set-name</i> argument specifies the name of the transform set.
Step 5	set identity Example: Router(config-crypto-map)# set identity	(Optional) Specifies identity restrictions to be used with the IPsec profile.
Step 6	set security association lifetime {seconds seconds kilobytes kilobytes} Example: Router(config-crypto-map)# set security association lifetime seconds 1800	(Optional) Overrides the global lifetime value for the IPsec profile. <ul style="list-style-type: none"> The seconds seconds option specifies the number of seconds a security association will live before expiring; the kilobytes kilobytes option specifies the volume of traffic (in kilobytes) that can pass between IPsec peers using a given security association before that security association expires. The default for the <i>seconds</i> argument is 3600 seconds.
Step 7	set pfs [group1 group2] Example: Router(config-crypto-map)# set pfs group2	(Optional) Specifies that IPsec should ask for perfect forward secrecy (PFS) when requesting new security associations for this IPsec profile. If this command is not specified, the default (group1) will be enabled. <ul style="list-style-type: none"> The group1 keyword specifies that IPsec should use the 768-bit Diffie-Hellman (DH) prime modulus group when performing the new DH exchange; the group2 keyword specifies the 1024-bit DH prime modulus group.

What to Do Next

Proceed to the following sections “[Configuring the Hub for DMVPN](#)” and “[Configuring the Spoke for DMVPN](#).”

Configuring the Hub for DMVPN

To configure the hub router for mGRE and IPsec integration (that is, associate the tunnel with the IPsec profile configured in the previous procedure), use the following commands:

**Note**

NHRP network IDs are locally significant and can be different. It makes sense from a deployment and maintenance perspective to use unique network ID numbers (using the **ip nhrp network-id** command) across all routers in a DMVPN network, but it is not necessary that they be the same.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip address** *ip-address mask [secondary]*
5. **ip mtu** *bytes*
6. **ip nhrp authentication** *string*
7. **ip nhrp map multicast dynamic**
8. **ip nhrp network-id** *number*
9. **tunnel source** {*ip-address* | *type number*}
10. **tunnel key** *key-number*
11. **tunnel mode gre multipoint**
12. **tunnel protection ipsec profile** *name*
13. **bandwidth** *kbps*
14. **ip tcp adjust-mss** *max-segment-size*
15. **ip nhrp holdtime** *seconds*
16. **delay** *number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface tunnel number Example: Router(config)# interface tunnel 5	Configures a tunnel interface and enters interface configuration mode <ul style="list-style-type: none"> The <i>number</i> argument specifies the number of the tunnel interface that you want to create or configure. There is no limit on the number of tunnel interfaces you can create.
Step 4	ip address ip-address mask [secondary] Example: Router(config-if)# ip address 10.0.0.1 255.255.255.0	Sets a primary or secondary IP address for the tunnel interface. Note All hubs and spokes that are in the same DMVPN network must be addressed in the same IP subnet.
Step 5	ip mtu bytes Example: Router(config-if)# ip mtu 1400	Sets the maximum transmission unit (MTU) size, in bytes, of IP packets sent on an interface.
Step 6	ip nhrp authentication string Example: Router(config-if)# ip nhrp authentication donttell	Configures the authentication string for an interface using NHRP. Note The NHRP authentication string must be set to the same value on all hubs and spokes that are in the same DMVPN network.
Step 7	ip nhrp map multicast dynamic Example: Router(config-if)# ip nhrp map multicast dynamic	Allows NHRP to automatically add spoke routers to the multicast NHRP mappings.
Step 8	ip nhrp network-id number Example: Router(config-if)# ip nhrp network-id 99	Enables NHRP on an interface. <ul style="list-style-type: none"> The <i>number</i> argument specifies a globally unique 32-bit network identifier from a nonbroadcast multiaccess (NBMA) network. The range is from 1 to 4294967295.
Step 9	tunnel source {ip-address type number} Example: Router (config-if)# tunnel source Ethernet0	Sets source address for a tunnel interface.

	Command or Action	Purpose
Step 10	tunnel key <i>key-number</i> Example: Router (config-if)# tunnel key 100000	(Optional) Enables an ID key for a tunnel interface. <ul style="list-style-type: none"> The <i>key-number</i> argument specifies a number from 0 to 4,294,967,295 that identifies the tunnel key. Note The key number must be set to the same value on all hubs and spokes that are in the same DMVPN network. Note This command should not be configured if you are using a Cisco 6500 or Cisco 7600 platform.
Step 11	tunnel mode gre multipoint Example: Router(config-if)# tunnel mode gre multipoint	Sets the encapsulation mode to mGRE for the tunnel interface.
Step 12	tunnel protection ipsec profile <i>name</i> Example: Router(config-if)# tunnel protection ipsec profile vpnprof	Associates a tunnel interface with an IPsec profile. <ul style="list-style-type: none"> The <i>name</i> argument specifies the name of the IPsec profile; this value must match the <i>name</i> specified in the crypto ipsec profile <i>name</i> command.
Step 13	bandwidth <i>kbps</i> Example: Router(config-if)# bandwidth 1000	Sets the current bandwidth value for an interface to higher-level protocols. <ul style="list-style-type: none"> The <i>kbps</i> argument specifies the bandwidth in kilobits per second. The default value is 9. The recommend bandwidth value is 1000 or greater. Setting the bandwidth value to at least 1000 is critical if EIGRP is used over the tunnel interface. Higher bandwidth values may be necessary depending on the number of spokes supported by a hub.
Step 14	ip tcp adjust-mss <i>max-segment-size</i> Example: Router(config-if)# ip tcp adjust-mss 1360	Adjusts the maximum segment size (MSS) value of TCP packets going through a router. <ul style="list-style-type: none"> The <i>max-segment-size</i> argument specifies the maximum segment size, in bytes. The range is from 500 to 1460. The recommended value is 1360 when the number of IP MTU bytes is set to 1400. With these recommended settings, TCP sessions quickly scale back to 1400-byte IP packets so the packets will “fit” in the tunnel.

	Command or Action	Purpose
Step 15	ip nhrp holdtime <i>seconds</i> Example: Router(config-if)# ip nhrp holdtime 450	Changes the number of seconds that NHRP NBMA addresses are advertised as valid in authoritative NHRP responses. <ul style="list-style-type: none">The <i>seconds</i> argument specifies the time in seconds that NBMA addresses are advertised as valid in positive authoritative NHRP responses. The recommended value ranges from 300 seconds to 600 seconds.
Step 16	delay <i>number</i> Example: Router(config-if)# delay 1000	(Optional) Used to change the EIGRP routing metric for routes learned over the tunnel interface. <ul style="list-style-type: none">The <i>number</i> argument specifies the delay time in seconds. The recommend value is 1000.

Configuring the Spoke for DMVPN

To configure spoke routers for mGRE and IPsec integration, use the following commands.

**Note**

NHRP network IDs are locally significant and can be different. It makes sense from a deployment and maintenance perspective to use unique network ID numbers (using the **ip nhrp network-id** command) across all routers in a DMVPN network, but it is not necessary that they be the same.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip address** *ip-address mask [secondary]*
5. **ip mtu** *bytes*
6. **ip nhrp authentication** *string*
7. **ip nhrp map** *hub-tunnel-ip-address hub-physical-ip-address*
8. **ip nhrp map multicast** *hub-physical-ip-address*
9. **ip nhrp nhs** *hub-tunnel-ip-address*
10. **ip nhrp network-id** *number*
11. **tunnel source** {*ip-address* | *type number*}
12. **tunnel key** *key-number*
13. **tunnel mode gre multipoint**
or
tunnel destination *hub-physical-ip-address*
14. **tunnel protection ipsec profile** *name*
15. **bandwidth** *kbps*
16. **ip tcp adjust-mss** *max-segment-size*
17. **ip nhrp holdtime** *seconds*
18. **delay** *number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface tunnel number Example: Router(config)# interface tunnel 5	Configures a tunnel interface and enters interface configuration mode. <ul style="list-style-type: none">The <i>number</i> argument specifies the number of the tunnel interface that you want to create or configure. There is no limit on the number of tunnel interfaces you can create.
Step 4	ip address ip-address mask [secondary] Example: Router(config-if)# ip address 10.0.0.2 255.255.255.0	Sets a primary or secondary IP address for the tunnel interface. Note All hubs and spokes that are in the same DMVPN network must be addressed in the same IP subnet.
Step 5	ip mtu bytes Example: Router(config-if)# ip mtu 1400	Sets the MTU size, in bytes, of IP packets sent on an interface.
Step 6	ip nhrp authentication string Example: Router(config-if)# ip nhrp authentication donttell	Configures the authentication string for an interface using NHRP. Note The NHRP authentication string be set to the same value on all hubs and spokes that are in the same DMVPN network.
Step 7	ip nhrp map hub-tunnel-ip-address hub-physical-ip-address Example: Router(config-if)# ip nhrp map 10.0.0.1 172.17.0.1	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an MBMA network. <ul style="list-style-type: none"><i>hub-tunnel-ip-address</i>—Defines the NHRP server at the hub, which is permanently mapped to the static public IP address of the hub.<i>hub-physical-ip-address</i>—Defines the static public IP address of the hub.
Step 8	ip nhrp map multicast hub-physical-ip-address Example: Router(config-if)# ip nhrp map multicast 172.17.0.1	Enables the use of a dynamic routing protocol between the spoke and hub, and sends multicast packets to the hub router.

	Command or Action	Purpose
Step 9	ip nhrp nhs <i>hub-tunnel-ip-address</i> Example: Router(config-if)# ip nhrp nhs 10.0.0.1	Configures the hub router as the NHRP next-hop server.
Step 10	ip nhrp network-id <i>number</i> Example: Router(config-if)# ip nhrp network-id 99	Enables NHRP on an interface. <ul style="list-style-type: none"> The <i>number</i> argument specifies a globally unique 32-bit network identifier from a NBMA network. The range is from 1 to 4294967295.
Step 11	tunnel source { <i>ip-address</i> <i>type number</i> } Example: Router (config-if)# tunnel source Ethernet0	Sets the source address for a tunnel interface.
Step 12	tunnel key <i>key-number</i> Example: Router (config-if)# tunnel key 100000	(Optional) Enables an ID key for a tunnel interface. <ul style="list-style-type: none"> The <i>key-number</i> argument specifies a number from 0 to 4,294,967,295 that identifies the tunnel key. The key number must be set to the same value on all hubs and spokes that are in the same DMVPN network. Note This command should not be configured if you are using a Cisco 6500 or Cisco 7600 platform.
Step 13	tunnel mode gre multipoint or tunnel destination <i>hub-physical-ip-address</i> Example: Router(config-if)# tunnel mode gre multipoint or Router(config-if)# tunnel destination 172.17.0.1	Sets the encapsulation mode to mGRE for the tunnel interface. Use this command if data traffic can use dynamic spoke-to-spoke traffic. Specifies the destination for a tunnel interface. Use this command if data traffic can use hub-and-spoke tunnels.
Step 14	tunnel protection ipsec profile <i>name</i> Example: Router(config-if)# tunnel protection ipsec profile vpnprof	Associates a tunnel interface with an IPsec profile. <ul style="list-style-type: none"> The <i>name</i> argument specifies the name of the IPsec profile; this value must match the <i>name</i> specified in the crypto ipsec profile name command.
Step 15	bandwidth <i>kbps</i> Example: Router(config-if)# bandwidth 1000	Sets the current bandwidth value for an interface to higher-level protocols. <ul style="list-style-type: none"> The <i>kbps</i> argument specifies the bandwidth in kilobits per second. The default value is 9. The recommend bandwidth value is 1000 or greater. The bandwidth setting for the spoke does not need to equal the bandwidth setting for the DMVPN hub. It is usually easier if all of the spokes use the same or similar value.

	Command or Action	Purpose
Step 16	ip tcp adjust-mss <i>max-segment-size</i> Example: Router(config-if)# ip tcp adjust-mss 1360	Adjusts the maximum segment size (MSS) value of TCP packets going through a router. <ul style="list-style-type: none"> The <i>max-segment-size</i> argument specifies the maximum segment size, in bytes. The range is from 500 to 1460. The recommended number value is 1360 when the number of IP MTU bytes is set to 1400. With these recommended settings, TCP sessions quickly scale back to 1400-byte IP packets so the packets will “fit” in the tunnel.
Step 17	ip nhrp holdtime <i>seconds</i> Example: Router(config-if)# ip nhrp holdtime 450	Changes the number of seconds that NHRP NBMA addresses are advertised as valid in authoritative NHRP responses. <ul style="list-style-type: none"> The <i>seconds</i> argument specifies the time in seconds that NBMA addresses are advertised as valid in positive authoritative NHRP responses. The recommended value ranges from 300 seconds to 600 seconds.
Step 18	delay <i>number</i> Example: Router(config-if)# delay 1000	(Optional) Used to change the EIGRP routing metric for routes learned over the tunnel interface. <ul style="list-style-type: none"> The <i>number</i> argument specifies the delay time in seconds. The recommend value is 1000.

Configuring the Forwarding of Clear-Text Data IP Packets into a VRF

To configure the forwarding of clear-text data IP packets into a VRF, perform the following steps. This configuration assumes that the VRF BLUE has already been configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip vrf forwarding** *vrf-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables higher privilege levels, such as privileged EXEC mode.
	Example: Router> enable	Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	
Step 3	interface <i>type number</i>	Configures an interface type and enters interface configuration mode.
	Example: Router (config)# interface tunnel0	
Step 4	ip vrf forwarding <i>vrf-name</i>	Associates a VPN VRF with an interface or subinterface.
	Example: Router (config-if)# ip vrf forwarding BLUE	

Configuring the Forwarding of Encrypted Tunnel Packets into a VRF

To configure the forwarding of encrypted tunnel packets into a VRF, perform the following steps. This configuration assumes that the VRF RED has already been configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. interface *type number*
4. **tunnel vrf** *vrf-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables higher privilege levels, such as privileged EXEC mode.
	Example: Router> enable	Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	

	Command or Action	Purpose
Step 3	<code>interface type number</code> Example: Router (config)# interface tunnel0	Configures an interface type and enters interface configuration mode.
Step 4	<code>tunnel vrf vrf-name</code> Example: Router (config-if)# tunnel vrf RED	Associates a VPN VRF instance with a specific tunnel destination, interface, or subinterface.

Configuring DMVPN—Traffic Segmentation Within DMVPN

There are no new commands to use for configuring traffic segmentation, but there are tasks you must complete in order to segment traffic within a DMVPN tunnel:

- [Enabling MPLS on the VPN Tunnel, page 22](#)
- [Configuring Multiprotocol BGP on the Hub Router, page 23](#)
- [Configuring Multiprotocol BGP on the Spoke Routers, page 25](#)

Prerequisites

The tasks that follow assume that the DMVPN tunnel and the VRFs “red” and “blue” have already been configured.

For information on configuring a DMVPN tunnel, see the “[Configuring the Hub for DMVPN](#)” section on [page 13](#) and the “[Configuring the Spoke for DMVPN](#)” section on [page 17](#). For details about VRF configuration, see the “[Configuring the Forwarding of Clear-Text Data IP Packets into a VRF](#)” section on [page 20](#) and the “[Configuring the Forwarding of Encrypted Tunnel Packets into a VRF](#)” section on [page 21](#).

Enabling MPLS on the VPN Tunnel

Because traffic segmentation within a DMVPN tunnel depends upon MPLS, you must configure MPLS for each VRF instance in which traffic will be segmented. For detailed information about configuring MPLS, see [Cisco IOS Multiprotocol Label Switching Configuration Guide](#), Release 12.4.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. `interface type number`
4. **mpls ip**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables higher privilege levels, such as privileged EXEC mode.
	Example: Router> enable	Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	
Step 3	interface type number	Configures an interface type and enters interface configuration mode.
	Example: Router (config)# interface tunnel0	
Step 4	mpls ip	Enables MPLS tagging of packets on the specified tunnel interface.
	Example: Router (config-if)# mpls ip	

Configuring Multiprotocol BGP on the Hub Router

You must configure multiprotocol iBGP (MP-iBGP) to enable advertisement of VPNv4 prefixes and labels to be applied to the VPN traffic. Use BGP to configure the hub as a route reflector. To force all traffic to be routed via the hub, configure the BGP route reflector to change the next hop to itself when it advertises VPNv4 prefixes to the route reflector clients (spokes).

For more information about the BGP routing protocol, see the “BGP” chapter in the *Cisco IOS IP Routing Protocols Configuration Guide*, Release 12.4.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp**
4. **neighbor ipaddress remote-as as-number**
5. **neighbor ipaddress update-source interface**
6. **address-family vpnv4**
7. **neighbor ipaddress activate**
8. **neighbor ipaddress send-community extended**
9. **neighbor ipaddress route-reflector-client**
10. **neighbor ipaddress route-map nexthop out**
11. **exit-address family**
12. **address-family ipv4 vrf-name**

13. redistribute connected
14. route-map
15. set ip next-hop *ipaddress*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	router bgp Example: Router (config)# router bgp	Enters BGP configuration mode.
Step 4	neighbor ipaddress remote-as as-number Example: Router (config)# neighbor 10.0.0.11 remote-as 1	Adds an entry to the BGP or multiprotocol BGP neighbor table.
Step 5	neighbor ipaddress update-source interface Example: Router (config)# neighbor 10.10.10.11 update-source Tunnell	Configures the Cisco IOS software to allow BGP sessions to use any operational interface for TCP connections.
Step 6	address-family vpnv4 Example: Router (config)# address-family vpnv4	Enters address family configuration mode to configure a routing session using Virtual Private Network (VPN) Version 4 address prefixes.
Step 7	neighbor ipaddress activate Example: Router (config)# neighbor 10.0.0.11 activate	Enables the exchange of information with a BGP neighbor.
Step 8	neighbor ipaddress send-community extended Example: Router (config)# neighbor 10.0.0.11 send-community extended	Specifies that extended community attributes should be sent to a BGP neighbor.

	Command or Action	Purpose
Step 9	neighbor <i>ipaddress</i> route-reflector-client Example: Router (config)# neighbor 10.0.0.11 route-reflector-client	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
Step 10	neighbor <i>ipaddress</i> route-map <i>nexthop</i> out Example: Router (config)# neighbor 10.0.0.11 route-map nexthop out	Forces all traffic to be routed via the hub.
Step 11	exit-address-family Example: Router (config)# exit-address-family	Exits the address family configuration mode for VPNv4.
Step 12	address-family <i>ipv4</i> <i>vrf-name</i> Example: Router (config)# address-family ipv4 vrf red	Enters address family configuration mode to configure a routing session using standard IP Version 4 address prefixes.
Step 13	redistribute connected Example: Router (config)# redistribute connected	Redistributes routes that are established automatically by virtue of having enabled IP on an interface from one routing domain into another routing domain.
Step 14	route-map Example: Router (config)# route-map nexthop permit 10	Enters route map configuration mode to configure the next-hop that will be advertised to the spokes.
Step 15	set ip next-hop <i>ipaddress</i> Example: Router (config)# set ip next-hop 10.0.0.1	Sets the next hop to be the hub.

Configuring Multiprotocol BGP on the Spoke Routers

Multiprotocol-iBGP (MP-iBGP) must be configured on the spoke routers and the hub. Follow the steps below for each spoke router in the DMVPN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp**
4. **neighbor *ipaddress* remote-as *as-number***
5. **neighbor *ipaddress* update-source *interface***
6. **address-family vpnv4**

7. **neighbor ipaddress activate**
8. **neighbor ipaddress send-community extended**
9. **exit-address-family**
10. **address-family ipv4 vrf-name**
11. **redistribute connected**
12. **exit-address-family**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	router bgp Example: Router (config)# router bgp 1	Enters BGP configuration mode.
Step 4	neighbor ipaddress remote-as as-number Example: Router (config)# neighbor 10.0.0.1 remote-as 1	Adds an entry to the BGP or multiprotocol BGP neighbor table.
Step 5	neighbor ipaddress update-source interface Example: Router (config)# neighbor 10.10.10.1 update-source Tunnell	Configures the Cisco IOS software to allow BGP sessions to use any operational interface for TCP connections.
Step 6	address-family vpngv4 Example: Router (config)# address-family vpngv4	Enters address family configuration mode to configure a routing session using Virtual Private Network (VPN) Version 4 address prefixes.
Step 7	neighbor ipaddress activate Example: Router (config)# neighbor 10.0.0.1 activate	Enables the exchange of information with a BGP neighbor.
Step 8	neighbor ipaddress send-community extended Example: Router (config)# neighbor 10.0.0.1 send-community extended	Specifies that extended community attributes should be sent to a BGP neighbor.

	Command or Action	Purpose
Step 9	exit-address-family Example: Router (config)# exit-address-family	Exits the address family configuration mode.
Step 10	address-family ipv4 vrf-name Example: Router (config)# address-family ipv4 vrf red	Enters address family configuration mode to configure a routing session using standard IP Version 4 address prefixes.
Step 11	redistribute connected Example: Router (config)# redistribute connected	Redistributes routes that are established automatically by virtue of having enabled IP on an interface from one routing domain into another routing domain.
Step 12	exit-address-family Example: Router (config)# exit-address-family	Exits the address family configuration mode. Note Repeat Steps 10–12 for each VRF.

Troubleshooting Dynamic Multipoint VPN (DMVPN)

After configuring DMVPN, to verify that DMVPN is operating correctly, to clear DMVPN statistics or sessions, or to debug DMVPN, you may perform the following optional steps:

SUMMARY STEPS

1. **clear dmvpn session** [peer {nbma | tunnel} ip-address] [interface {tunnel number}] [vrf vrf-name] [static]
2. **clear dmvpn statistics** [peer {nbma | tunnel} ip-address] [interface {tunnel number}] [vrf vrf-name]
3. **debug dmvpn** {[condition [unmatched] | [peer [nbma | tunnel {ip-address}]] | [vrf {vrf-name}]] | [interface {tunnel number}]} | [{error | detail | packet | all} {nhrp | crypto | tunnel | socket | all}]}
4. **debug nhrp condition**
5. **debug nhrp error**
6. **logging dmvpn** [rate-limit seconds]
7. **show crypto ipsec sa** [active | standby]
8. **show crypto isakmp sa**
9. **show crypto map**
10. **show dmvpn** [peer [nbma | tunnel {ip-address}] | [network {ip-address} {mask}]] [vrf {vrf-name}] [interface {tunnel number}] [detail] [static] [debug-condition]
11. **show ip nhrp traffic** [interface {tunnel number}]

DETAILED STEPS

-
- Step 1** The **clear dmvpn session** command is used to clear DMVPN sessions.
- The following example clears only dynamic DMVPN sessions:
- ```
Router# clear dmvpn session peer nbma
```
- The following example clears all DMVPN sessions, both static and dynamic, for the specified tunnel:
- ```
Router# clear dmvpn session interface tunnel 100 static
```
- Step 2** The **clear dmvpn statistics** command is used to clear DMVPN related counters. The following example shows how to clear DMVPN related session counters for the specified tunnel interface:
- ```
Router# clear dmvpn statistics peer tunnel 192.0.2.3
```
- Step 3** The **debug dmvpn** command is used to debug DMVPN sessions. You can enable or disable DMVPN debugging based on a specific condition. There are three levels of DMVPN debugging, listed in the order of details from lowest to highest:
- Error level
  - Detail level
  - Packet level
- The following example shows how to enable conditional DMVPN debugging that displays all error debugs for next hop routing protocol (NHRP), sockets, tunnel protection and crypto information:
- ```
Router# debug dmvpn error all
```
- Step 4** The **debug nhrp condition** command enables or disables debugging based on a specific condition. The following example shows how to enable conditional NHRP debugging:
- ```
Router# debug nhrp condition
```
- Step 5** The **debug nhrp error** command displays information about NHRP error activity. The following example shows how to enable debugging for NHRP error messages:
- ```
Router# debug nhrp error
```
- Step 6** The **logging dmvpn** command is used to enable DMVPN system logging. The following command shows how to enable DMVPN system logging at the rate of 1 message every 20 seconds:
- ```
Router(config)# logging dmvpn rate-limit 20
```
- The following example shows a sample system log with DMVPN messages:
- ```
%DMVPN-7-CRYPTO_SS: Tunnel101-192.0.2.1 socket is UP
%DMVPN-5-NHRP_NHS: Tunnel101 192.0.2.251 is UP
%DMVPN-5-NHRP_CACHE: Client 192.0.2.2 on Tunnel1 Registered.
%DMVPN-5-NHRP_CACHE: Client 192.0.2.2 on Tunnel101 came UP.
%DMVPN-3-NHRP_ERROR: Registration Request failed for 192.0.2.251 on Tunnel101
```
- Step 7** The **show crypto ipsec sa** command displays the settings used by the current SAs. The following example output shows the IPsec SA status of only the active device:
- ```
Router# show crypto ipsec sa active

interface: Ethernet0/0
 Crypto map tag: to-peer-outside, local addr 209.165.201.3
 protected vrf: (none)
 local ident (addr/mask/prot/port): (192.168.0.1/255.255.255.255/0/0)
 remote ident (addr/mask/prot/port): (172.16.0.1/255.255.255.255/0/0)
 current_peer 209.165.200.225 port 500
 PERMIT, flags={origin_is_acl,}
 #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
```

```
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
local crypto endpt.: 209.165.201.3, remote crypto endpt.: 209.165.200.225
path mtu 1500, media mtu 1500
current outbound spi: 0xD42904F0(3559458032)
inbound esp sas:
spi: 0xD3E9ABD0(3555306448)
transform: esp-3des ,
in use settings ={Tunnel, }
conn id: 2006, flow_id: 6, crypto map: to-peer-outside
sa timing: remaining key lifetime (k/sec): (4586265/3542)
HA last key lifetime sent(k): (4586267)
ike_cookies: 9263635C CA4B4E99 C14E908E 8EE2D79C
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

**Step 8** The **show crypto isakmp sa** command displays all current IKE SAs at a peer. For example, the following sample output is displayed after IKE negotiations have successfully completed between two peers.

Router# **show crypto isakmp sa**

| dst           | src           | state   | conn-id | slot |
|---------------|---------------|---------|---------|------|
| 172.17.63.19  | 172.16.175.76 | QM_IDLE | 2       | 0    |
| 172.17.63.19  | 172.17.63.20  | QM_IDLE | 1       | 0    |
| 172.16.175.75 | 172.17.63.19  | QM_IDLE | 3       | 0    |

**Step 9** The **show crypto map** command displays the crypto map configuration.

The following sample output is displayed after a crypto map has been configured:

Router# **show crypto map**

```
Crypto Map "Tunnel5-head-0" 10 ipsec-isakmp
 Profile name: vpnprof
 Security association lifetime: 4608000 kilobytes/3600 seconds
 PFS (Y/N): N
 Transform sets={trans2, }

Crypto Map "Tunnel5-head-0" 20 ipsec-isakmp
 Map is a PROFILE INSTANCE.
 Peer = 172.16.175.75
 Extended IP access list
 access-list permit gre host 172.17.63.19 host 172.16.175.75
 Current peer: 172.16.175.75
 Security association lifetime: 4608000 kilobytes/3600 seconds
 PFS (Y/N): N
 Transform sets={trans2, }

Crypto Map "Tunnel5-head-0" 30 ipsec-isakmp
 Map is a PROFILE INSTANCE.
 Peer = 172.17.63.20
 Extended IP access list
 access-list permit gre host 172.17.63.19 host 172.17.63.20
 Current peer: 172.17.63.20
 Security association lifetime: 4608000 kilobytes/3600 seconds
 PFS (Y/N): N
 Transform sets={trans2, }

Crypto Map "Tunnel5-head-0" 40 ipsec-isakmp
 Map is a PROFILE INSTANCE.
 Peer = 172.16.175.76
```

```

Extended IP access list
 access-list permit gre host 172.17.63.19 host 172.16.175.76
Current peer: 172.16.175.76
Security association lifetime: 4608000 kilobytes/3600 seconds
PFS (Y/N): N
Transform sets={trans2, }
Interfaces using crypto map Tunnel5-head-0:
Tunnel5

```

**Step 10** The **show dmvpn** command displays DMVPN specific session information. The following example shows example summary output:

```

Router# show dmvpn

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
 N - NATed, L - Local, X - No Socket
 # Ent --> Number of NHRP entries with same NBMA peer

! The line below indicates that the sessions are being displayed for Tunnel1.
! Tunnel1 is acting as a spoke and is a peer with three other NBMA peers.

Tunnel1, Type: Spoke, NBMA Peers: 3,
Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb

 2 192.0.2.21 192.0.2.116 IKE 3w0d D
 1 192.0.2.102 192.0.2.11 NHRP 02:40:51 S
 1 192.0.2.225 192.0.2.10 UP 3w0d S

Tunnel2, Type: Spoke, NBMA Peers: 1,
Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb

 1 192.0.2.25 192.0.2.171 IKE never S

```

**Step 11** The **show ip nhrp traffic** command displays NHRP statistics. The following example shows output for a specific tunnel, tunnel7:

```

Router# show ip nhrp traffic interface tunnel7

Tunnel7: Max-send limit:100Pkts/10Sec, Usage:0%
Sent: Total 79
 18 Resolution Request 10 Resolution Reply 42 Registration Request
 0 Registration Reply 3 Purge Request 6 Purge Reply
 0 Error Indication 0 Traffic Indication
Rcvd: Total 69
 10 Resolution Request 15 Resolution Reply 0 Registration Request
 36 Registration Reply 6 Purge Request 2 Purge Reply
 0 Error Indication 0 Traffic Indication

```

## What to Do Next

If you have troubleshooted your DMVPN configuration and proceed to contact technical support, the **show tech-support** command includes information for DMVPN sessions. For more information, see the **show tech-support** command in the Cisco IOS Configuration Fundamentals Command Reference.

# Configuration Examples for Dynamic Multipoint VPN (DMVPN) Feature

This section provides the following comprehensive configuration examples:

- [Hub Configuration for DMVPN: Example, page 31](#)
- [Spoke Configuration for DMVPN: Example, page 32](#)
- [VRF Aware DMVPN: Example, page 33](#)

## Hub Configuration for DMVPN: Example

In the following example, which configures the hub router for multipoint GRE and IPsec integration, no explicit configuration lines are needed for each spoke; that is, the hub is configured with a global IPsec policy template that all spoke routers can talk to. In this example, EIGRP is configured to run over the private physical interface and the tunnel interface.

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
! Ensures longer packets are fragmented before they are encrypted; otherwise, the
receiving router would have to do the reassembly.
 ip mtu 1400
! The following line must match on all nodes that "want to use" this mGRE tunnel:
 ip nhrp authentication donttell
! Note that the next line is required only on the hub.
 ip nhrp map multicast dynamic
! The following line must match on all nodes that want to use this mGRE tunnel:
 ip nhrp network-id 99
 ip nhrp holdtime 300
! Turns off split horizon on the mGRE tunnel interface; otherwise, EIGRP will not
advertise routes that are learned via the mGRE interface back out that interface.
 no ip split-horizon eigrp 1
! Enables dynamic, direct spoke-to-spoke tunnels when using EIGRP.
 no ip next-hop-self eigrp 1
 ip tcp adjust-mss 1360
 delay 1000
! Sets IPsec peer address to Ethernet interface's public address.
 tunnel source Ethernet0
 tunnel mode gre multipoint
! The following line must match on all nodes that want to use this mGRE tunnel.
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address 172.17.0.1 255.255.255.0
!
interface Ethernet1
 ip address 192.168.0.1 255.255.255.0
```

```

!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.0.0 0.0.0.255
!

```

For information about defining and configuring ISAKMP profiles, see the references in the ["Related Documents"](#) section.

## Spoke Configuration for DMVPN: Example

In the following example, all spokes are configured the same except for tunnel and local interface address, thereby, reducing necessary configurations for the user:

```

crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.2 255.255.255.0
 ip mtu 1400
! The following line must match on all nodes that want to use this mGRE tunnel:
 ip nhrp authentication donttell
! Definition of NHRP server at the hub (10.0.0.1), which is permanently mapped to the
static public address of the hub (172.17.0.1).
 ip nhrp map 10.0.0.1 172.17.0.1
! Sends multicast packets to the hub router, and enables the use of a dynamic routing
protocol between the spoke and the hub.
 ip nhrp map multicast 172.17.0.1
! The following line must match on all nodes that want to use this mGRE tunnel:
 ip nhrp network-of 99
 ip nhrp holdtime 300
! Configures the hub router as the NHRP next-hop server.
 ip nhrp nhs 10.0.0.1
 ip tcp adjust-mss 1360
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
! The following line must match on all nodes that want to use this mGRE tunnel:
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
! This is a spoke, so the public address might be dynamically assigned via DHCP.
interface Ethernet0
 ip address dhcp hostname Spoke1
!
interface Ethernet1
 ip address 192.168.1.1 255.255.255.0
!
! EIGRP is configured to run over the inside physical interface and the tunnel.
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.1.0 0.0.0.255

```

## VRF Aware DMVPN: Example

When configuring VRF Aware DMVPN, you must create a separate DMVPN network for each VRF instance. In the following example, there are two DMVPN networks: BLUE and RED. In addition, a separate source interface has been used on the hub for each DMVPN tunnel—a must for Cisco IOS Release 12.2(18)SXE. For other Cisco IOS releases, you can configure the same tunnel source for both of the tunnel interfaces, but you must configure the **tunnel key** and **tunnel protection (tunnel protection ipsec profile {name} shared)** commands.



### Note

If you use the **shared** keyword, then you should be running Cisco IOS Release 12.4(5) or Release 12.4(6)T, or a later release. Otherwise the IPsec/GRE tunnels under the two mGRE tunnel interfaces may not function correctly.

### Hub Configuration

```
interface Tunnel0
! Note the next line.
 ip vrf forwarding BLUE
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1436
 ! Note the next line.
 ip nhrp authentication BLUE!KEY
 ip nhrp map multicast dynamic
 ! Note the next line
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 no ip split-horizon eigrp 1
 no ip next-hop-self eigrp 1
 ip tcp adjust-mss 1360
 delay 1000
 ! Note the next line.
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel protection ipsec profile vpnprof!
interface Tunnel1
! Note the next line.
 ip vrf forwarding RED
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1436
 ! Note the next line.
 ip nhrp authentication RED!KEY
 ip nhrp map multicast dynamic
 ! Note the next line.
 ip nhrp network-id 20000
 ip nhrp holdtime 600
 no ip split-horizon eigrp 1
 no ip next-hop-self eigrp 1
 ip tcp adjust-mss 1360
 delay 1000
 ! Note the next line.
 tunnel source Ethernet1
 tunnel mode gre multipoint
 tunnel protection ipsec profile vpnprof!
interface Ethernet0
 ip address 172.17.0.1 255.255.255.0
!
interface Ethernet1
```

```
ip address 192.0.2.171 255.255.255.0
```

**Note**

For the hub configuration shown above, a separate DMVPN network is configured for each VPN. The NHRP network ID and authentication keys must be unique on the two mGRE interfaces.

**EIGRP Configuration on the Hub**

```
router eigrp 1
auto-summary
!
address-family ipv4 vrf BLUE
network 10.0.0.0 0.0.0.255
no auto-summary
autonomous-system 1
exit-address-family
!
address-family ipv4 vrf RED
network 10.0.0.0 0.0.0.255
no auto-summary
autonomous-system 1
exit-address-family
```

**Spoke Configurations****Spoke 1:**

```
interface Tunnel0
bandwidth 1000
ip address 10.0.0.2 255.255.255.0
ip mtu 1436
! Note the next line.
ip nhrp authentication BLUE!KEY
ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 100000
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
ip tcp adjust-mss 1360
delay 1000
tunnel mode gre multipoint
tunnel source Ethernet0
tunnel destination 172.17.0.1
tunnel protection ipsec profile vpnprof
```

**Spoke 2:**

```
interface Tunnel0
bandwidth 1000
ip address 10.0.0.2 255.255.255.0
ip mtu 1436
ip nhrp authentication RED!KEY
ip nhrp map 10.0.0.1 192.0.2.171
ip nhrp network-id 200000
ip nhrp holdtime 300
ip nhrp nhs 10.0.0.1
ip tcp adjust-mss 1360
delay 1000
tunnel source Ethernet0
tunnel destination 192.0.2.171
tunnel protection ipsec profile vpnprof!
```



## 2547oDMVPN with Traffic Segmentation (with BGP only): Example

The following example show a traffic segmentation configuration in which traffic is segmented between two spokes that serve as provider edge (PE) devices.

### Hub Configuration

```
hostname hub-pe1

boot-start-marker
boot-end-marker

no aaa new-model

resource policy

clock timezone EST 0
ip cef
no ip domain lookup

!This section refers to the forwarding table for VRF blue:
ip vrf blue
 rd 2:2
 route-target export 2:2
 route-target import 2:2

!This section refers to the forwarding table for VRF red:
ip vrf red
 rd 1:1
 route-target export 1:1
 route-target import 1:1

mpls label protocol ldp

crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 0.0.0.0 0.0.0.0

crypto ipsec transform-set t1 esp-des
 mode transport

crypto ipsec profile prof
 set transform-set t1

interface Tunnel1
 ip address 10.9.9.1 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp network-id 1

!The command below enables MPLS on the DMVPN network:
mpls ip
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile prof

interface Loopback0
 ip address 10.0.0.1 255.255.255.255

interface Ethernet0/0
 ip address 172.0.0.1 255.255.255.0
```

!The multiprotocol BGP route reflector (the hub) configuration changes the next-hop information to set itself as the next-hop and assigns a new VPN label for the prefixes learned from the spokes and advertises the VPN prefix:

```
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.0.0.11 remote-as 1
 neighbor 10.0.0.11 update-source Tunnel1
 neighbor 10.0.0.12 remote-as 1
 neighbor 10.0.0.12 update-source Tunnel1
 no auto-summary

 address-family vpnv4
 neighbor 10.0.0.11 activate
 neighbor 10.0.0.11 send-community extended
 neighbor 10.0.0.11 route-reflector-client
 neighbor 10.0.0.11 route-map NEXTHOP out
 neighbor 10.0.0.12 activate
 neighbor 10.0.0.12 send-community extended
 neighbor 10.0.0.12 route-reflector-client
 neighbor 10.0.0.12 route-map NEXTHOP out
 exit-address-family

 address-family ipv4 vrf red
 redistribute connected
 no synchronization
 exit-address-family

 address-family ipv4 vrf blue
 redistribute connected
 no synchronization
 exit-address-family

no ip http server
no ip http secure-server

!In this route map information, the hub sets the next hop to itself, and the VPN prefixes
are advertised:
route-map NEXTHOP permit 10
 set ip next-hop 10.0.0.1

control-plane

line con 0
 logging synchronous
line aux 0
line vty 0 4
 no login

end
```

## Spoke Configurations

### Spoke 2

```
hostname spoke-pe2

boot-start-marker
boot-end-marker

no aaa new-model
```

```
resource policy

clock timezone EST 0
ip cef
no ip domain lookup

!This section refers to the forwarding table for VRF blue:
ip vrf blue
 rd 2:2
 route-target export 2:2
 route-target import 2:2

!This section refers to the forwarding table for VRF red:
ip vrf red
 rd 1:1
 route-target export 1:1
 route-target import 1:1

mpls label protocol ldp

crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 0.0.0.0 0.0.0.0

crypto ipsec transform-set t1 esp-des
 mode transport

crypto ipsec profile prof
 set transform-set t1

interface Tunnel1
 ip address 10.0.0.11 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp map 10.0.0.1 172.0.0.1
 ip nhrp map multicast 172.0.0.1
 ip nhrp network-id 1
 ip nhrp nhs 10.0.0.1

!The command below enables MPLS on the DMVPN network:
mpls ip
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile prof

interface Loopback0
 ip address 10.9.9.11 255.255.255.255

interface Ethernet0/0
 ip address 172.0.0.11 255.255.255.0
!
```

```

!
interface Ethernet1/0
 ip vrf forwarding red
 ip address 192.168.11.2 255.255.255.0

interface Ethernet2/0
 ip vrf forwarding blue
 ip address 192.168.11.2 255.255.255.0

!The multiprotocol BGP route reflector (the hub) configuration changes the next-hop
information to set itself as the next-hop and assigns a new VPN label for the prefixes
learned from the spokes and advertises the VPN prefix:
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.0.0.1 remote-as 1
 neighbor 10.0.0.1 update-source Tunnel1
 no auto-summary

address-family vpnv4
 neighbor 10.0.0.1 activate
 neighbor 10.0.0.1 send-community extended
 exit-address-family

!
address-family ipv4 vrf red
 redistribute connected
 no synchronization
 exit-address-family

!
address-family ipv4 vrf blue
 redistribute connected
 no synchronization
 exit-address-family

no ip http server
no ip http secure-server

control-plane

line con 0
 logging synchronous
line aux 0
line vty 0 4
 no login

end

```

### Spoke 3

```

hostname spoke-PE3

boot-start-marker
boot-end-marker

no aaa new-model

resource policy

clock timezone EST 0
ip cef
no ip domain lookup

```

```
!This section refers to the forwarding table for VRF blue:
ip vrf blue
 rd 2:2
 route-target export 2:2
 route-target import 2:2

!This section refers to the forwarding table for VRF red:
ip vrf red
 rd 1:1
 route-target export 1:1
 route-target import 1:1

mpls label protocol ldp

crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 0.0.0.0 0.0.0.0

crypto ipsec transform-set t1 esp-des
 mode transport

crypto ipsec profile prof
 set transform-set t1

interface Tunnel1
 ip address 10.0.0.12 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp map 10.0.0.1 172.0.0.1
 ip nhrp map multicast 172.0.0.1
 ip nhrp network-id 1
 ip nhrp nhs 10.0.0.1

!The command below enables MPLS on the DMVPN network:
mpls ip
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel protection ipsec profile prof
!
interface Loopback0
 ip address 10.9.9.12 255.255.255.255

interface Ethernet0/0
 ip address 172.0.0.12 255.255.255.0

interface Ethernet1/0
 ip vrf forwarding red
 ip address 192.168.12.2 255.255.255.0

interface Ethernet2/0
 ip vrf forwarding blue
 ip address 192.168.12.2 255.255.255.0

!The multiprotocol BGP route reflector (the hub) configuration changes the next-hop
information to set itself as the next-hop and assigns a new VPN label for the prefixes
learned from the spokes and advertises the VPN prefix:
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.0.0.1 remote-as 1
 neighbor 10.0.0.1 update-source Tunnel1
 no auto-summary
```

```

address-family vpnv4
neighbor 10.0.0.1 activate
neighbor 10.0.0.1 send-community extended
exit-address-family

address-family ipv4 vrf red
redistribute connected
no synchronization
exit-address-family

address-family ipv4 vrf blue
redistribute connected
no synchronization
exit-address-family

no ip http server
no ip http secure-server

control-plane

line con 0
 logging synchronous
line aux 0
line vty 0 4
 no login

end

```

## 2547oDMVPN with Traffic Segmentation (Enterprise Branch): Example

The following example shows a configuration for segmenting traffic between two spokes located at branch offices of an enterprise. In this example, EIGRP is configured to learn routes to reach BGP neighbors within the DMVPN.

### Hub Configuration

```

hostname HUB

boot-start-marker
boot-end-marker

no aaa new-model

resource policy

clock timezone EST 0
ip cef
no ip domain lookup

!This section refers to the forwarding table for VRF blue:
ip vrf blue
 rd 2:2
 route-target export 2:2
 route-target import 2:2

```

```
!This refers to the forwarding table for VRF red:
ip vrf red
 rd 1:1
 route-target export 1:1
 route-target import 1:1

mpls label protocol ldp

crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 0.0.0.0 0.0.0.0

crypto ipsec transform-set t1 esp-des
 mode transport

crypto ipsec profile prof
 set transform-set t1

interface Tunnel1
 ip address 10.0.0.1 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp network-id 1

!EIGRP is enabled on the DMVPN network to learn the IGP prefixes:
no ip split-horizon eigrp 1

!The command below enables MPLS on the DMVPN network:
mpls ip
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel protection ipsec profile prof

!This address is advertised by EIGRP and used as the BGP endpoint:
interface Loopback0
 ip address 10.9.9.1 255.255.255.255

interface Ethernet0/0
 ip address 172.0.0.1 255.255.255.0

!EIGRP is configured to learn the BGP peer addresses (10.9.9.x networks)
router eigrp 1
 network 10.9.9.1 0.0.0.0
 network 10.0.0.0 0.0.0.255
 no auto-summary

!The multiprotocol BGP route reflector (the hub) configuration changes the next-hop
information to set itself as the next-hop and assigns a new VPN label for the prefixes
learned from the spokes and advertises the VPN prefix:
router bgp 1
 no synchronization
 bgp router-id 10.9.9.1
 bgp log-neighbor-changes
 neighbor 10.9.9.11 remote-as 1
 neighbor 10.9.9.11 update-source Loopback0
 neighbor 10.9.9.12 remote-as 1
 neighbor 10.9.9.12 update-source Loopback0
 no auto-summary

address-family vpnv4
 neighbor 10.9.9.11 activate
 neighbor 10.9.9.11 send-community extended
 neighbor 10.9.9.11 route-reflector-client
```

```

neighbor 10.9.9.12 activate
neighbor 10.9.9.12 send-community extended
neighbor 10.9.9.12 route-reflector-client
exit-address-family

address-family ipv4 vrf red
redistribute connected
no synchronization
exit-address-family

address-family ipv4 vrf blue
redistribute connected
no synchronization
exit-address-family

no ip http server
no ip http secure-server

control-plane

line con 0
 logging synchronous
line aux 0
line vty 0 4
 no login

end

```

## Spoke Configurations

### Spoke 2

```

hostname Spoke2

boot-start-marker
boot-end-marker

no aaa new-model

resource policy

clock timezone EST 0
ip cef
no ip domain lookup

!This section refers to the forwarding table for VRF blue:
ip vrf blue
 rd 2:2
 route-target export 2:2
 route-target import 2:2

!This section refers to the forwarding table for VRF red:
ip vrf red
 rd 1:1
 route-target export 1:1
 route-target import 1:1

mpls label protocol ldp

crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 0.0.0.0 0.0.0.0

```



```
crypto ipsec transform-set t1 esp-des
mode transport

crypto ipsec profile prof
set transform-set t1

interface Tunnel1
 ip address 10.0.0.11 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp map 10.0.0.1 172.0.0.1
 ip nhrp map multicast 172.0.0.1
 ip nhrp network-id 1
 ip nhrp nhs 10.0.0.1

!The command below enables MPLS on the DMVPN network:
mpls ip
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel protection ipsec profile prof

!This address is advertised by EIGRP and used as the BGP endpoint:
interface Loopback0
 ip address 10.9.9.11 255.255.255.255

interface Ethernet0/0
 ip address 172.0.0.11 255.255.255.0

interface Ethernet1/0
 ip vrf forwarding red
 ip address 192.168.11.2 255.255.255.0

interface Ethernet2/0
 ip vrf forwarding blue
 ip address 192.168.11.2 255.255.255.0

!EIGRP is enabled on the DMVPN network to learn the IGP prefixes:
router eigrp 1
 network 10.9.9.11 0.0.0.0
 network 10.0.0.0 0.0.0.255
 no auto-summary

!The multiprotocol BGP route reflector (the hub) configuration changes the next-hop
information to set itself as the next-hop and assigns a new VPN label for the prefixes
learned from the spokes and advertises the VPN prefix:
router bgp 1
 no synchronization
 bgp router-id 10.9.9.11
 bgp log-neighbor-changes
 neighbor 10.9.9.1 remote-as 1
 neighbor 10.9.9.1 update-source Loopback0
 no auto-summary

address-family vpnv4
 neighbor 10.9.9.1 activate
 neighbor 10.9.9.1 send-community extended
 exit-address-family

address-family ipv4 vrf red
 redistribute connected
 no synchronization
 exit-address-family
```

```

 address-family ipv4 vrf blue
 redistribute connected
 no synchronization
 exit-address-family

no ip http server
no ip http secure-server

control-plane

line con 0
 logging synchronous
line aux 0
line vty 0 4
 no login

end

```

### Spoke 3

```

hostname Spoke3

boot-start-marker
boot-end-marker

no aaa new-model

resource policy

clock timezone EST 0
ip cef
no ip domain lookup

!This section refers to the forwarding table for VRF blue:
ip vrf blue
 rd 2:2
 route-target export 2:2
 route-target import 2:2

!This section refers to the forwarding table for VRF red:
ip vrf red
 rd 1:1
 route-target export 1:1
 route-target import 1:1

mpls label protocol ldp

crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 0.0.0.0 0.0.0.0

crypto ipsec transform-set t1 esp-des
 mode transport

crypto ipsec profile prof
 set transform-set t1

interface Tunnell
 ip address 10.0.0.12 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic

```

```
ip nhrp map 10.0.0.1 172.0.0.1
ip nhrp map multicast 172.0.0.1
ip nhrp network-id 1
ip nhrp nhs 10.0.0.1

!The command below enables MPLS on the DMVPN network:
mpls ip
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel protection ipsec profile prof

!This address is advertised by EIGRP and used as the BGP endpoint:
interface Loopback0
 ip address 10.9.9.12 255.255.255.255

interface Ethernet0/0
 ip address 172.0.0.12 255.255.255.0

interface Ethernet1/0
 ip vrf forwarding red
 ip address 192.168.12.2 255.255.255.0

interface Ethernet2/0
 ip vrf forwarding blue
 ip address 192.168.12.2 255.255.255.0

!EIGRP is enabled on the DMVPN network to learn the IGP prefixes:
router eigrp 1
 network 10.9.9.12 0.0.0.0
 network 10.0.0.0 0.0.0.255
 no auto-summary

!The multiprotocol BGP route reflector (the hub) configuration changes the next-hop
information to set itself as the next-hop and assigns a new VPN label for the prefixes
learned from the spokes and advertises the VPN prefix:
router bgp 1
 no synchronization
 bgp router-id 10.9.9.12
 bgp log-neighbor-changes
 neighbor 10.9.9.1 remote-as 1
 neighbor 10.9.9.1 update-source Loopback0
 no auto-summary

address-family vpnv4
 neighbor 10.9.9.1 activate
 neighbor 10.9.9.1 send-community extended
 exit-address-family

address-family ipv4 vrf red
 redistribute connected
 no synchronization
 exit-address-family

address-family ipv4 vrf blue
 redistribute connected
 no synchronization
 exit-address-family

no ip http server
no ip http secure-server

control-plane
```

```

line con 0
 logging synchronous
line aux 0
line vty 0 4
 no login

end

```

### Sample Command Output: show mpls ldp bindings

```

Spoke2# show mpls ldp bindings

tib entry: 10.9.9.1/32, rev 8
 local binding: tag: 16
 remote binding: tsr: 10.9.9.1:0, tag: imp-null
tib entry: 10.9.9.11/32, rev 4
 local binding: tag: imp-null
 remote binding: tsr: 10.9.9.1:0, tag: 16
tib entry: 10.9.9.12/32, rev 10
 local binding: tag: 17
 remote binding: tsr: 10.9.9.1:0, tag: 17
tib entry: 10.0.0.0/24, rev 6
 local binding: tag: imp-null
 remote binding: tsr: 10.9.9.1:0, tag: imp-null
tib entry: 172.0.0.0/24, rev 3
 local binding: tag: imp-null
 remote binding: tsr: 10.9.9.1:0, tag: imp-null
Spoke2#

```

### Sample Command Output: show mpls forwarding-table

```

Spoke2# show mpls forwarding-table

Local Outgoing Prefix Bytes tag Outgoing Next Hop
tag tag or VC or Tunnel Id switched interface
16 Pop tag 10.9.9.1/32 0 Tu1 10.0.0.1
17 17 10.9.9.12/32 0 Tu1 10.0.0.1
18 Aggregate 192.168.11.0/24[V] \
 0
19 Aggregate 192.168.11.0/24[V] \
 0
Spoke2#

```

### Sample Command Output: show ip route vrf red

```

Spoke2# show ip route vrf red

Routing Table: red
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

B 192.168.12.0/24 [200/0] via 10.9.9.12, 00:00:02
C 192.168.11.0/24 is directly connected, Ethernet1/0
Spoke2#

```

**Sample Command Output: show ip route vrf blue**

Spoke2# **show ip route vrf blue**

Routing Table: blue

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

B 192.168.12.0/24 [200/0] via 10.9.9.12, 00:00:08

C 192.168.11.0/24 is directly connected, Ethernet2/0

Spoke2#

Spoke2# **show ip cef vrf red 192.168.12.0**

192.168.12.0/24, version 5, epoch 0

0 packets, 0 bytes

tag information set

local tag: VPN-route-head

fast tag rewrite with Tu1, 10.0.0.1, tags imposed: {17 18}

via 10.9.9.12, 0 dependencies, recursive

next hop 10.0.0.1, Tunnel1 via 10.9.9.12/32

valid adjacency

tag rewrite with Tu1, 10.0.0.1, tags imposed: {17 18}

Spoke2#

**Sample Command Output: show ip bgp neighbors**

Spoke2# **show ip bgp neighbors**

BGP neighbor is 10.9.9.1, remote AS 1, internal link

BGP version 4, remote router ID 10.9.9.1

BGP state = Established, up for 00:02:09

Last read 00:00:08, last write 00:00:08, hold time is 180, keepalive interval is 60 seconds

Neighbor capabilities:

Route refresh: advertised and received(old & new)

Address family IPv4 Unicast: advertised and received

Address family VPNv4 Unicast: advertised and received

Message statistics:

InQ depth is 0

OutQ depth is 0

|                | Sent | Rcvd |
|----------------|------|------|
| Opens:         | 1    | 1    |
| Notifications: | 0    | 0    |
| Updates:       | 4    | 4    |
| Keepalives:    | 4    | 4    |
| Route Refresh: | 0    | 0    |
| Total:         | 9    | 9    |

Default minimum time between advertisement runs is 0 seconds

For address family: IPv4 Unicast

BGP table version 1, neighbor version 1/0

Output queue size : 0

Index 1, Offset 0, Mask 0x2

1 update-group member

|                    | Sent | Rcvd |
|--------------------|------|------|
| Prefix activity:   | ---- | ---- |
| Prefixes Current:  | 0    | 0    |
| Prefixes Total:    | 0    | 0    |
| Implicit Withdraw: | 0    | 0    |
| Explicit Withdraw: | 0    | 0    |
| Used as bestpath:  | n/a  | 0    |
| Used as multipath: | n/a  | 0    |

|                               | Outbound | Inbound |
|-------------------------------|----------|---------|
| Local Policy Denied Prefixes: | -----    | -----   |
| Total:                        | 0        | 0       |

Number of NLRIs in the update sent: max 0, min 0

For address family: VPNv4 Unicast  
 BGP table version 9, neighbor version 9/0  
 Output queue size : 0  
 Index 1, Offset 0, Mask 0x2  
 1 update-group member

|                    | Sent | Rcvd                   |
|--------------------|------|------------------------|
| Prefix activity:   | ---- | ----                   |
| Prefixes Current:  | 2    | 2 (Consumes 136 bytes) |
| Prefixes Total:    | 4    | 2                      |
| Implicit Withdraw: | 2    | 0                      |
| Explicit Withdraw: | 0    | 0                      |
| Used as bestpath:  | n/a  | 2                      |
| Used as multipath: | n/a  | 0                      |

|                               | Outbound | Inbound |
|-------------------------------|----------|---------|
| Local Policy Denied Prefixes: | -----    | -----   |
| ORIGINATOR loop:              | n/a      | 2       |
| Bestpath from this peer:      | 4        | n/a     |
| Total:                        | 4        | 2       |

Number of NLRIs in the update sent: max 1, min 1

Connections established 1; dropped 0  
 Last reset never  
 Connection state is ESTAB, I/O status: 1, unread input bytes: 0  
 Connection is ECN Disabled  
 Local host: 10.9.9.11, Local port: 179  
 Foreign host: 10.9.9.1, Foreign port: 12365

Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x2D0F0):

| Timer     | Starts | Wakeups | Next |
|-----------|--------|---------|------|
| Retrans   | 6      | 0       | 0x0  |
| TimeWait  | 0      | 0       | 0x0  |
| AckHold   | 7      | 3       | 0x0  |
| SendWnd   | 0      | 0       | 0x0  |
| KeepAlive | 0      | 0       | 0x0  |
| GiveUp    | 0      | 0       | 0x0  |
| PmtuAger  | 0      | 0       | 0x0  |
| DeadWait  | 0      | 0       | 0x0  |

iss: 3328307266 snduna: 3328307756 sndnxt: 3328307756 sndwnd: 15895  
 irs: 4023050141 rcvnxt: 4023050687 rcvwnd: 16384 delrcvwnd: 0

SRTT: 165 ms, RTT0: 1457 ms, RTV: 1292 ms, KRTT: 0 ms  
 minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms  
 Flags: passive open, nagle, gen tcbs  
 IP Precedence value : 6

```
Datagrams (max data segment is 536 bytes):
Rcvd: 13 (out of order: 0), with data: 7, total data bytes: 545
Sent: 11 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 0), with
data: 6, total data bytes: 489
Spoke2#
```

# Additional References

The following sections provide references related to Dynamic Multipoint VPN (DMVPN):

## Related Documents

| Related Topic                                          | Document Title                                                                                                                                                                                     |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Call Admission Control                                 | <a href="#">Call Admission Control for IKE</a> , Cisco IOS Release 12.4                                                                                                                            |
| GRE tunnel keepalive information                       | <a href="#">Generic Routing Encapsulation (GRE) Tunnel Keepalive</a> , Cisco IOS Release 12.2(8)T                                                                                                  |
| IKE configuration tasks such as defining an IKE policy | The chapter “ <a href="#">Configuring Internet Key Exchange for IPSec VPNs</a> ” in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4                                               |
| IPsec configuration tasks                              | The chapter “ <a href="#">Configuring Security for VPNs with IPsec</a> ” in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4                                                       |
| Tunnel interface configuration tasks                   | The section “ <a href="#">Implementing Tunnels</a> ” in the chapter “Interface Configuration Overview” in the <i>Cisco IOS Interface and Hardware Component Configuration Guide</i> , Release 12.4 |
| Configuring VRF-Aware IPsec                            | <a href="#">VRF-Aware IPsec</a> , in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4                                                                                              |
| Configuring MPLS                                       | <a href="#">Cisco IOS Multiprotocol Label Switching Configuration Guide</a> , Release 12.4.                                                                                                        |
| Configuring BGP                                        | The chapter “ <a href="#">BGP</a> ” in the <i>Cisco IOS IP Routing Protocols Configuration Guide</i> , Release 12.4                                                                                |
| System messages                                        | <a href="#">12.4T System Message Guide</a>                                                                                                                                                         |
| Defining and configuring ISAKMP profiles               | “ <a href="#">Certificate to ISAKMP Profile Mapping</a> ” chapter in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4                                                              |

## Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

## MIBs

| MIBs | MIBs Link                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |



## RFCs

| RFCs     | Title         |
|----------|---------------|
| RFC 2547 | BGP/MPLS VPNs |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Link                                                                            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Command Reference

The following commands are introduced or modified in the feature or features

- **clear dmvpn session**
- **clear dmvpn statistics**
- **debug dmvpn**
- **debug nhrp condition**
- **debug nhrp error**
- **logging dmvpn**
- **show dmvpn**
- **show ip nhrp traffic**

For information about these commands, see the Cisco IOS Security Command Reference at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

# Feature Information for Dynamic Multipoint VPN (DMVPN)

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for Dynamic Multipoint VPN (DMVPN)

| Feature Name                                          | Releases                             | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2547oDMVPN—Enabling Traffic Segmentation Within DMVPN | 12.4(11)T                            | The 2547oDMVPN feature allows users to segment VPN traffic within a DMVPN tunnel by applying MPLS labels to VRF instances to indicate the source and destination of each VRF.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Mangeability Enhancements for DMVPN                   | 12.4(9)T                             | DMVPN session manageabilty was expanded with DMVPN specific commands for debugging, show output, session and counter control, and system log information.<br><br>The following sections provide information about this feature: <ul style="list-style-type: none"> <li><a href="#">Troubleshooting Dynamic Multipoint VPN (DMVPN)</a></li> </ul> The following commands were introduced or modified by this feature: <b>clear dmvpn session</b> , <b>clear dmvpn statistics</b> , <b>debug dmvpn</b> , <b>debug nhrp condition</b> , <b>debug nhrp error</b> , <b>logging dmvpn</b> , <b>show dmvpn</b> , <b>show ip nhrp traffic</b> |
| DMVPN Phase 2                                         | 12.2(18)SXE<br>12.3(9)a<br>12.3(8)T1 | DMVPN Spoke-to-Spoke functionality was made more production ready. If you are using this functionality in a production network, the minimum release is Release 12.3(9a) or Release 12.3(8)T1.<br><br>In Release 12.2(18)SXE, support was added for the Cisco Catalyst 6500 series switch and the Cisco 7600 series router.                                                                                                                                                                                                                                                                                                            |

**Table 1** Feature Information for Dynamic Multipoint VPN (DMVPN)

| Feature Name                           | Releases                 | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| —                                      | 12.3(6)<br>12.3(7)T      | Virtual Route Forwarding Integrated DMVPN and Network Address Translation-Transparency (NAT-T) Aware DMVPN enhancements were added. In addition, DMVPN Hub-to-Spoke functionality was made more production ready. If you are using this functionality in a production network, the minimum release requirement is Cisco IOS Release 12.3(6) or 12.3(7)T.<br><br>The enhancements added in Cisco IOS Release 12.3(6) were integrated into Cisco IOS Release 12.3(7)T. |
| Dynamic Multipoint VPN (DMVPN) Phase 1 | 12.2(13)T                | The Dynamic Multipoint VPN (DMVPN) feature allows users to better scale large and small IPsec Virtual Private Networks (VPNs) by combining generic routing encapsulation (GRE) tunnels, IP security (IPsec) encryption, and Next Hop Resolution Protocol (NHRP).                                                                                                                                                                                                     |
| DMVPN - Phase 2                        | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                                                                        |
| Dynamic Multipoint VPN (DMVPN) Phase 1 | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                                                                        |

## Glossary

**AM**—aggressive mode. A mode during IKE negotiation. Compared to MM, AM eliminates several steps, making it faster but less secure than MM. Cisco IOS software will respond in aggressive mode to an IKE peer that initiates aggressive mode.

**GRE**—generic routing encapsulation. Tunnels that provide a specific pathway across the shared WAN and encapsulate traffic with new packet headers to ensure delivery to specific destinations. The network is private because traffic can enter a tunnel only at an endpoint. Tunnels do not provide true confidentiality (encryption does) but can carry encrypted traffic.

GRE tunneling can also be used to encapsulate non-IP traffic into IP and send it over the Internet or IP network. The Internet Package Exchange (IPX) and AppleTalk protocols are examples of non-IP traffic.

**IKE**—Internet Key Exchange. A hybrid protocol that implements Oakley key exchange and Skeme key exchange inside the ISAKMP framework. Although IKE can be used with other protocols, its initial implementation is with IPsec. IKE provides authentication of the IPsec peers, negotiates IPsec keys, and negotiates IPsec security associations.

**IPsec**—IP security. A framework of open standards developed by the Internet Engineering Task Force (IETF). IPsec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (“peers”), such as Cisco routers.

**ISAKMP**—Internet Security Association Key Management Protocol. A protocol framework that defines payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of a security association.

**MM**—main mode. Mode that is slower than aggressive mode but more secure and more flexible than aggressive mode because it can offer an IKE peer more security proposals. The default action for IKE authentication (rsa-sig, rsa-encr, or preshared) is to initiate main mode.

**NHRP**—Next Hop Resolution Protocol. Routers, access servers, and hosts can use NHRP to discover the addresses of other routers and hosts connected to a NBMA network.

The Cisco implementation of NHRP supports the IETF draft version 11 of *NBMA Next Hop Resolution Protocol (NHRP)*.

The Cisco implementation of NHRP supports IP Version 4, Internet Packet Exchange (IPX) network layers, and, at the link layer, ATM, Ethernet, SMDS, and multipoint tunnel networks. Although NHRP is available on Ethernet, NHRP need not be implemented over Ethernet media because Ethernet is capable of broadcasting. Ethernet support is unnecessary (and not provided) for IPX.

**PFS**—Perfect Forward Secrecy. A cryptographic characteristic associated with a derived shared secret value. With PFS, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys.

**SA**—security association. Describes how two or more entities will utilize security services to communicate securely. For example, an IPsec SA defines the encryption algorithm (if used), the authentication algorithm, and the shared session key to be used during the IPsec connection.

Both IPsec and IKE require and use SAs to identify the parameters of their connections. IKE can negotiate and establish its own SA. The IPsec SA is established either by IKE or by manual user configuration.

**transform**—The list of operations done on a dataflow to provide data authentication, data confidentiality, and data compression. For example, one transform is the ESP protocol with the HMAC-MD5 authentication algorithm; another transform is the AH protocol with the 56-bit DES encryption algorithm and the ESP protocol with the HMAC-SHA authentication algorithm.

**VPN**—Virtual Private Network. A framework that consists of multiple peers transmitting private data securely to one another over an otherwise public infrastructure. In this framework, inbound and outbound network traffic is protected using protocols that tunnel and encrypt all data. This framework permits networks to extend beyond their local topology, while remote users are provided with the appearance and functionality of a direct network connection.

**Note**

---

See [Networking Terms and Acronyms](#) for terms not included in this glossary.

---



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



# Easy VPN Remote RSA Signature Support

---

**First Published: March 1, 2004**  
**Last Updated: August 21, 2007**

The Easy VPN Remote RSA Signature Support feature provides for the support of Rivest, Shamir, and Adelman (RSA) signatures on Easy VPN remote devices. The support is provided through RSA certificates that can be stored on or off the remote device.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Easy VPN Remote RSA Signature Support](#)” section on page 6.*

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for Easy VPN Remote RSA Signature Support, page 1](#)
- [Restrictions for Easy VPN Remote RSA Signature Support, page 2](#)
- [Information About Easy VPN Remote RSA Signature Support, page 2](#)
- [How to Configure Easy VPN Remote RSA Signature Support, page 2](#)
- [Additional References, page 3](#)

## Prerequisites for Easy VPN Remote RSA Signature Support

- You must have a Cisco Virtual Private Network (VPN) remote device and be familiar with configuring the device.



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

- You must have a certification authority (CA) available to your network before you configure this interoperability feature. The CA must support the public key infrastructure (PKI) protocol of Cisco Systems, which is the Simple Certificate Enrollment Protocol (SCEP) (formerly called certificate enrollment protocol [CEP]).
- You should be familiar with IP Security (IPSec) and PKI.
- You should be familiar with configuring RSA key pairs.
- You should be familiar with configuring CAs.

## Restrictions for Easy VPN Remote RSA Signature Support

- This feature should be configured only when you also configure both IPSec and Internet Key Exchange (IKE) in your network.
- The Cisco IOS software does not support CA server public keys greater than 2048 bits.

## Information About Easy VPN Remote RSA Signature Support

To configure the Easy VPN Remote RSA Signature Support feature, you should understand the following concept:

- [Easy VPN Remote RSA Signature Support Overview, page 2](#)

## Easy VPN Remote RSA Signature Support Overview

The Easy VPN Remote RSA Signature Support feature allows you to configure RSA signatures on your Easy VPN remote device. The signatures can be stored on or off your remote device.

## How to Configure Easy VPN Remote RSA Signature Support

This section contains the following procedure:

- [Configuring Easy VPN Remote RSA Signature Support, page 2](#)

## Configuring Easy VPN Remote RSA Signature Support

The RSA signatures for an Easy VPN remote device are configured the same way that you would configure RSA signatures for any other Cisco device. (For information about configuring RSA signatures, refer to the “Configuring Certification Authority Interoperability” chapter of the “IP Security and Encryption” section of the *Cisco IOS Security Configuration Guide*, Release 12.4.)

To enable the RSA signatures, when you are configuring the Easy VPN remote and assigning the configuration to the outgoing interface, you must omit the **group** command. The content of the first Organizational Unit (OU) field will be used as the group. (For information about configuring Cisco Easy VPN remote devices, refer to the feature document “[Cisco Easy VPN Remote](#),” Release 12.4(11)T.)

To troubleshoot your Easy VPN remote RSA signature configuration, you can use the following **debug** commands. The **debug** commands can be used in any order or individually.



## SUMMARY STEPS

1. `enable`
2. `debug crypto ipsec client ezvpn`
3. `debug crypto isakmp`

## DETAILED STEPS

|        | Command or Action                                                                                                           | Purpose                                                                                                          |
|--------|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br>Router> <code>enable</code>                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <code>debug crypto ipsec client ezvpn</code><br><br><b>Example:</b><br>Router# <code>debug crypto ipsec client ezvpn</code> | Displays information about the VPN tunnel as it relates to the Easy VPN remote configuration.                    |
| Step 3 | <code>debug crypto isakmp</code><br><br><b>Example:</b><br>Router# <code>debug crypto isakmp</code>                         | Displays messages about IKE events.                                                                              |

## Additional References

The following sections provide references related to Easy VPN Remote RSA Signature Support.

## Related Documents

| Related Topic                              | Document Title                                                                                                                                                                 |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuring IPsec                          | “IP Security and Encryption Overview” chapter of the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4                                                              |
| Configuring IKE                            | “Configuring Internet Key Exchange Security Protocol” chapter of the “IP Security and Encryption” section of the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4  |
| Configuring RSA key pairs                  | Feature document “ <i>Exporting and Importing RSA Keys</i> ,” Release 12.2(15)T                                                                                                |
| Declaring a CA                             | “Configuring Certification Authority Interoperability” chapter of the “IP Security and Encryption” section of the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4 |
| Configuring a Cisco Easy VPN remote device | Feature document “ <i>Cisco Easy VPN Remote</i> ,” Release 12.4(11)T                                                                                                           |
| Security commands                          | <i>Cisco IOS Security Command Reference</i> , Release 12.4 T                                                                                                                   |

## Standards

| Standards                                                            | Title |
|----------------------------------------------------------------------|-------|
| There are no new or modified standards associated with this feature. | —     |

## MIBs

| MIBs                                                            | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| There are no new or modified MIBs associated with this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                                            | Title |
|-----------------------------------------------------------------|-------|
| There are no new or modified RFCs associated with this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                         | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Feature Information for Easy VPN Remote RSA Signature Support

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for Easy VPN Remote RSA Signature Support

| Feature Name                            | Releases                                | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Easy VPN Remote RSA Signature Support   | 12.3(7)T1<br>12.2(33)SRA<br>12.2(33)SXH | <p>The Easy VPN Remote RSA Signature Support feature provides for the support of Rivest, Shamir, and Adelman (RSA) signatures on Easy VPN remote devices. The support is provided through RSA certificates that can be stored on or off the remote device.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>“Easy VPN Remote RSA Signature Support Overview” section on page 2</li> <li>“Configuring Easy VPN Remote RSA Signature Support” section on page 2</li> </ul> |
| Easy VPN Client RSA - Signature Support | Cisco IOS XE Release 2.1                | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





# Easy VPN Server

---

**First Published: February 25, 2002**

**Last Updated: June 16, 2008**

The Easy VPN Server feature introduces server support for the Cisco VPN Client Release 3.x and later software clients and Cisco VPN hardware clients (such as the Cisco 800, Cisco 900, Cisco 1700, VPN 3002, and PIX 501 devices). This feature allows a remote end user to communicate using IP Security (IPsec) with any Cisco IOS Virtual Private Network (VPN) gateway. Centrally managed IPsec policies are “pushed” to the client device by the server, minimizing configuration by the end user.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all of the features documented in this module.* To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Easy VPN Server](#)” section on page 75.

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Restrictions for Easy VPN Server, page 2](#)
- [Information About Easy VPN Server, page 2](#)
- [How to Configure Easy VPN Server, page 19](#)
- [Configuration Examples for Easy VPN Server, page 53](#)
- [Additional References, page 71](#)
- [Command Reference, page 73](#)
- [Feature Information for Easy VPN Server, page 75](#)
- [Glossary, page 78](#)



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2008 Cisco Systems, Inc. All rights reserved.

# Restrictions for Easy VPN Server

## Nonsupported Protocols

Table 1 outlines IPsec protocol options and attributes that currently are *not* supported by Cisco VPN clients, so these options and attributes should not be configured on the router for these clients.

**Table 1** *Nonsupported IPsec Protocol Options and Attributes*

| Options                     | Attributes                                                                    |
|-----------------------------|-------------------------------------------------------------------------------|
| Authentication Types        | Authentication with public key encryption<br>Digital Signature Standard (DSS) |
| Diffie-Hellman (D-H) groups | 1                                                                             |
| IPsec Protocol Identifier   | IPSEC_AH                                                                      |
| IPsec Protocol Mode         | Transport mode                                                                |
| Miscellaneous               | Manual keys<br>Perfect Forward Secrecy (PFS)                                  |

## Cisco Secure VPN Client 1.x Restrictions

When used with this feature, the Cisco Secure VPN Client 1.x has the following restrictions:

- It does not support dead peer detection (DPD) or any other keepalive scheme.
- It does not support initial contact.

This feature cannot use per-group attribute policy profiles such as IP addresses, and Domain Name Service (DNS). Thus, customers must continue to use existing, globally defined parameters for IP address assignment, Windows Internet Naming Service (WINS) and DNS, and preshared keys.

## Virtual IPsec Interface Restrictions

The Virtual IPsec Interface Support feature works only with a Cisco software VPN Client that is version 4.x or later, and an Easy VPN remote device that is configured to use a virtual interface.

## cTCP Restrictions

- If a port is being used for Cisco Tunnel Control Protocol (cTCP), it cannot be used for other applications.
- cTCP can be used on only ten ports at a time.
- cTCP is supported on only Cisco IOS Easy VPN servers.
- If a cTCP connection is set up on a port, cTCP cannot be disabled on that port because doing so would cause the existing connection to stop receiving traffic.
- High Availability of cTCP is not currently supported on the Easy VPN server.

# Information About Easy VPN Server

Before using the Easy VPN Server Enhancements feature, you should understand the following concepts:



- [How It Works, page 3](#)
- [RADIUS Support for Group Profiles, page 4](#)
- [RADIUS Support for User Profiles, page 7](#)
- [Supported Protocols, page 8](#)
- [Functions Supported by Easy VPN Server, page 9](#)

## How It Works

When the client initiates a connection with a Cisco IOS VPN device, the “conversation” that occurs between the peers consists of device authentication via Internet Key Exchange (IKE), followed by user authentication using IKE Extended Authentication (Xauth), VPN policy push (using Mode Configuration), and IPsec security association (SA) creation. An overview of this process is as follows:

- The client initiates IKE Phase 1 via aggressive mode (AM) if a preshared key is to be used for authentication; the client initiates main mode (MM) if digital certificates are used. If the client identifies itself with a preshared key, the accompanying group name entered in the configuration GUI (ID\_KEY\_ID) is used to identify the group profile associated with this client. If digital certificates are used, the organizational unit (OU) field of a distinguished name (DN) is used to identify the group profile.

**Note**

Because the client may be configured for preshared key authentication, which initiates IKE AM, it is recommended that the administrator change the identity of the Cisco IOS VPN device via the **crypto isakmp identity hostname** command. This will not affect certificate authentication via IKE MM.

- The client attempts to establish an IKE SA between its public IP address and the public IP address of the Cisco IOS VPN device. To reduce the amount of manual configuration on the client, every combination of encryption and hash algorithms, in addition to authentication methods and D-H group sizes, is proposed.
- Depending on its IKE policy configuration, the Cisco IOS VPN device will determine which proposal is acceptable to continue negotiating Phase 1.

**Tip**

IKE policy is global for the Cisco IOS VPN device and can consist of several proposals. In the case of multiple proposals, the Cisco IOS VPN device will use the first match, so you should always list your most secure policies first.

**Note**

Device authentication ends and user authentication begins at this point.

- After the IKE SA is successfully established, and if the Cisco IOS VPN device is configured for Xauth, the client waits for a “username/password” challenge and then responds to the challenge of the peer. The information that is entered is checked against authentication entities using authentication, authorization, and accounting (AAA) protocols such as RADIUS and TACACS+. Token cards may also be used via AAA proxy. During Xauth, it is also possible for a user-specific attribute to be retrieved if the credentials of that user are validated via RADIUS.

**Note**

VPN devices that are configured to handle remote clients should always be configured to enforce user authentication.

- If the Cisco IOS VPN device indicates that authentication was successful, the client requests further configuration parameters from the peer. The remaining system parameters (for example, IP address, DNS, and split tunnel attributes) are pushed to the client at this time using Mode Configuration.

**Note**

The IP address pool and group preshared key (if Rivest, Shamir, and Adelman [RSA] signatures are not being used) are the only required parameter in a group profile, all other parameters are optional.

- After each client is assigned an internal IP address via Mode Configuration, it is important that the Cisco IOS VPN device knows how to route packets through the appropriate VPN tunnel. Reverse route injection (RRI) will ensure that a static route is created on the Cisco IOS VPN device for each client internal IP address.

**Note**

It is recommended that you enable RRI on the crypto map (static or dynamic) for the support of VPN clients unless the crypto map is being applied to a Generic Routing Encapsulation (GRE) tunnel that is already being used to distribute routing information.

- After the configuration parameters have been successfully received by the client, IKE quick mode is initiated to negotiate IPsec SA establishment.
- After IPsec SAs are created, the connection is complete.

## RADIUS Support for Group Profiles

Group policy information is stored in a profile that can be defined locally in the router configuration or on a RADIUS server that is accessible by the Cisco IOS VPN device. If RADIUS is used, you must configure access to the server and allow the Cisco IOS VPN device to send requests to the server.

To define group policy attributes for RADIUS, you must do the following task on your RADIUS server:

- Define a user that has a name equal to the group name as defined in the client graphical user interface (GUI). For example, if users will be connecting to the Cisco IOS VPN device using the group name “sales,” you will need a user whose name is “sales.” The password for this user is “cisco,” which is a special identifier that is used by the router for RADIUS purposes. The username must then be made a member of a group in which the correct policy is defined. For simplicity, it is recommended that the group name be the same as the username.

### For a Cisco Secure Access Control Server

If you are using a Cisco Secure access control server (ACS), you may configure your remote access VPN group profiles on this server. To perform this task, you must ensure that Internet Engineering Task Force (IETF) RADIUS attributes are selected for group configuration as shown in [Figure 1](#). (This figure also shows the compulsory attributes required for a remote access VPN group.) All values must be entered except the Tunnel-Password attribute, which is actually the preshared key for IKE purposes; if digital certificates are preferred, this attribute may be omitted.

**Figure 1** IETF RADIUS Attributes Selection for Group Configuration

The screenshot shows the Cisco Systems Group Setup web interface. On the left is a navigation menu with icons and labels for: User Setup, Group Setup (highlighted), Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled "Group Setup" and contains a tabbed interface with three tabs: "Access Restrictions", "Enable Options", and "IP Address Assignment". The "Enable Options" tab is active, showing a sub-tabbed interface with "TACACS+", "IETF Radius" (selected), and "Cisco IOS/PIX Radius". Below these tabs is the "IETF RADIUS Attributes" section, which includes a list of attributes with checkboxes and input fields. The attributes shown are: [006] Service-Type (checked, value: Outbound), [027] Session-Timeout (unchecked, value: 0), [028] Idle-Timeout (unchecked, value: 0), [064] Tunnel-Type (checked, with Tag 1 Value: IP ESP and Tag 2 Value: ), [065] Tunnel-Medium-Type (unchecked, with Tag 1 Value: and Tag 2 Value: ), and [069] Tunnel-Password (checked, with Tag 1 Value: cisco and Tag 2 Value: ). At the bottom are three buttons: "Submit", "Submit + Restart", and "Cancel".

**CISCO SYSTEMS**

## Group Setup

Access Restrictions    Enable Options    IP Address Assignment

TACACS+    IETF Radius    Cisco IOS/PIX Radius

### IETF RADIUS Attributes

☒ [006] Service-Type  
Outbound

☐ [027] Session-Timeout  
0

☐ [028] Idle-Timeout  
0

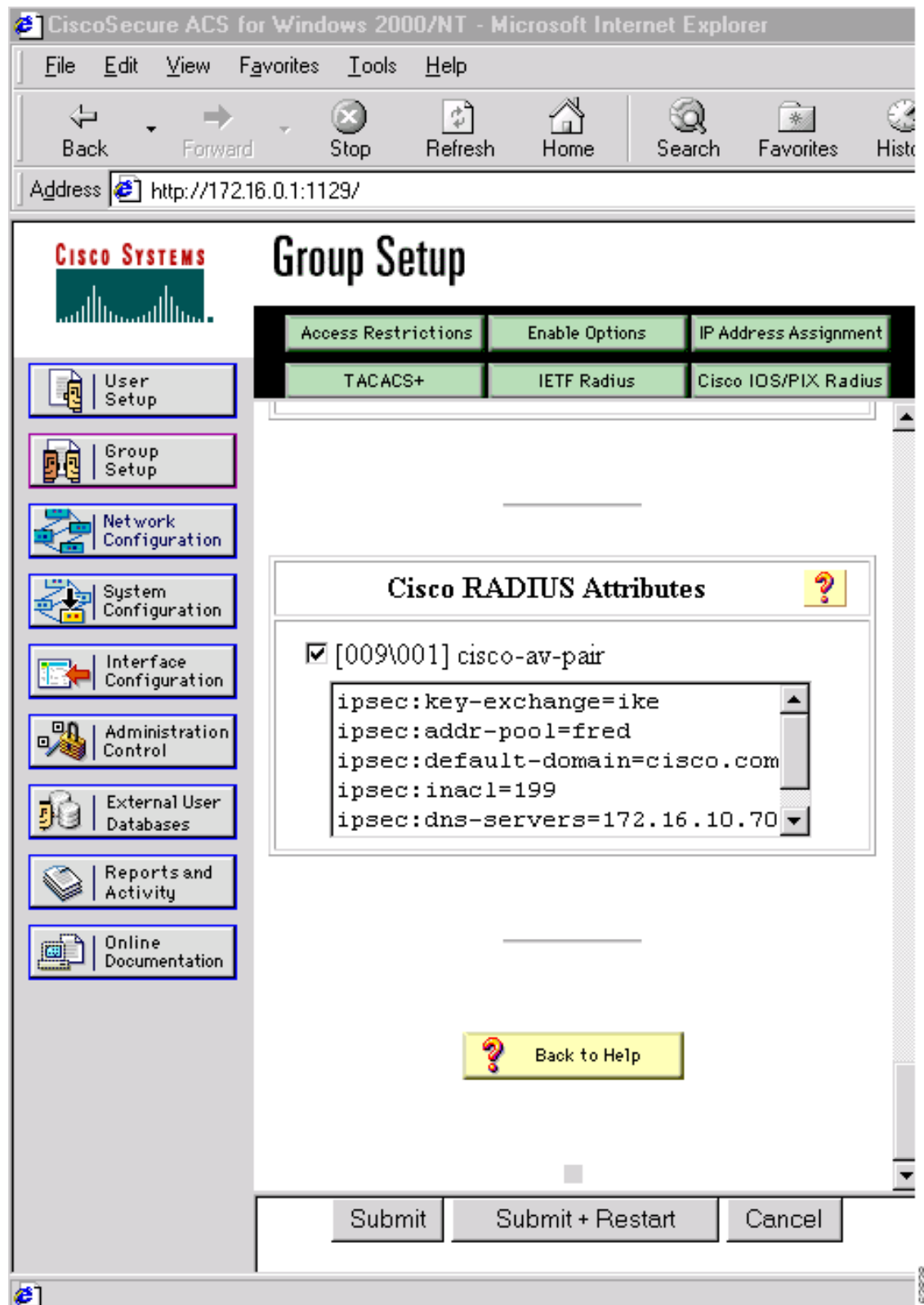
☒ [064] Tunnel-Type  
Tag 1 Value IP ESP  
Tag 2 Value

☐ [065] Tunnel-Medium-Type  
Tag 1 Value  
Tag 2 Value

☒ [069] Tunnel-Password  
Tag 1 Value cisco  
Tag 2 Value

Submit    Submit + Restart    Cancel

In addition to the compulsory attributes shown in [Figure 1](#), other values can be entered that represent the group policy that is pushed to the remote client via Mode Configuration. [Figure 2](#) shows an example of a group policy. All attributes are optional except the `addr-pool`, `key-exchange=preshared-key`, and `key-exchange=ike` attributes. The values of the attributes are the same as the setting that is used if the policy is defined locally on the router rather than in a RADIUS server. (These values are explained in the section “[Defining Group Policy Information for Mode Configuration Push](#)” later in this document.)

**Figure 2** CiscoSecure ACS Group Policy Setup

After the group profile is created, a user who is a member of the group should be added. (Remember that the username that is defined maps to the group name as defined on the remote client, and the password defined for the username in the RADIUS database must be “cisco.”) If digital certificates are the preferred method of IKE authentication, the username should reflect the OU field in the certificate presented by the remote client.

## For All Other RADIUS Servers

Ensure that your RADIUS server allows you to define attribute-value (AV) pairs. (For an example, see the section “[Configuring Cisco IOS for Easy VPN Server: Example](#)” later in this document).

**Note**

If digital certificates are used, the username defined in RADIUS must be equal to the OU field of the DN of the certificate of the client.

## RADIUS Support for User Profiles

Attributes may also be applied on a per-user basis. If you apply attributes on a per-user basis, you can override a group attribute value with an individual user attribute. The attributes are retrieved at the time that user authentication via Xauth occurs. The attributes are then combined with group attributes and applied during Mode Configuration.

User-based attributes are available only if RADIUS is being used for user authentication.

To define user policy attributes for RADIUS, you must do the following task on your RADIUS server:

- Define a user or add attributes to the existing profile of a user in your RADIUS database. The password for the user will be used during Xauth user authentication, or you may proxy to a third-party server, such as a token card server.

[Figure 3](#) shows how CiscoSecure ACS may be used for user authentication and for the assignment of a Framed-IP-Address attribute that may be pushed to the client. The presence of this attribute means that the local address pool defined for the group to which that user belongs will be overridden.

**Figure 3** *CiscoSecure ACS User Profile Setup*

## For All Other RADIUS Servers

Ensure that your RADIUS server allows you to define AV pairs. (For an example, see the [“Configuring Cisco IOS for Easy VPN Server: Example”](#) section later in this document.)

## Supported Protocols

[Table 2](#) outlines supported IPsec protocol options and attributes that can be configured for this feature. (See [Table 1](#) for nonsupported options and attributes.)

**Table 2** *Supported IPsec Protocol Options and Attributes*

| Options                   | Attributes                                                                                                                                                               |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authentication Algorithms | <ul style="list-style-type: none"> <li>Hashed Message Authentication Codes with Message Digest 5 (HMAC-MD5)</li> <li>HMAC-Secure Hash Algorithm 1 (HMAC-SHA1)</li> </ul> |
| Authentication Types      | <ul style="list-style-type: none"> <li>Preshared keys</li> <li>RSA digital signatures</li> </ul>                                                                         |

**Table 2**      **Supported IPsec Protocol Options and Attributes (continued)**

| Options                       | Attributes                                                                                                                           |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| D-H groups                    | <ul style="list-style-type: none"> <li>• 2</li> <li>• 5</li> </ul>                                                                   |
| Encryption Algorithms (IKE)   | <ul style="list-style-type: none"> <li>• Data Encryption Standard (DES)</li> <li>• Triple Data Encryption Standard (3DES)</li> </ul> |
| Encryption Algorithms (IPsec) | <ul style="list-style-type: none"> <li>• DES</li> <li>• 3DES</li> <li>• NULL</li> </ul>                                              |
| IPsec Protocol Identifiers    | <ul style="list-style-type: none"> <li>• Encapsulating Security Payload (ESP)</li> <li>• IP LZS compression (IPCOMP-LZS)</li> </ul>  |
| IPsec Protocol Mode           | Tunnel mode                                                                                                                          |

## Functions Supported by Easy VPN Server

- [Mode Configuration Version 6 Support, page 10](#)
- [Xauth Version 6 Support, page 10](#)
- [IKE DPD, page 10](#)
- [Split Tunneling Control, page 10](#)
- [Initial Contact, page 10](#)
- [Group-Based Policy Control, page 10](#)
- [User-Based Policy Control, page 11](#)
- [Session Monitoring for VPN Group Access, page 12](#)
- [Virtual IPsec Interface Support on a Server, page 13](#)
- [Virtual Tunnel Interface Per-User Attribute Support, page 13](#)
- [Banner, Auto-Update, and Browser Proxy, page 13](#)
- [Configuration Management Enhancements, page 14](#)
- [Per User AAA Policy Download with PKI, page 15](#)
- [Per-User Attribute Support for Easy VPN Servers, page 7](#)
- [Syslog Message Enhancements, page 16](#)
- [Network Admission Control Support for Easy VPN, page 16](#)
- [Central Policy Push Firewall Policy Push, page 17](#)
- [Password Aging, page 18](#)
- [Split DNS, page 18](#)
- [cTCP, page 18](#)

## Mode Configuration Version 6 Support

Mode Configuration version 6 is now supported for more attributes (as described in an IETF draft submission).

## Xauth Version 6 Support

Cisco IOS has been enhanced to support version 6 of Xauth. Xauth for user authentication is based on an IETF draft submission.

## IKE DPD

The client implements a new keepalives scheme—IKE DPD.

DPD allows two IPsec peers to determine whether the other is still “alive” during the lifetime of a VPN connection. DPD is useful because a host may reboot, or the dialup link of a remote user may disconnect without notifying the peer that the VPN connection has gone away. When an IPsec host determines that a VPN connection no longer exists, the host can notify a user, attempt to switch to another IPsec host, or clean up valuable resources that were allocated for the peer that no longer exists.

A Cisco IOS VPN device can be configured to send and reply to DPD messages. DPD messages are sent if no other traffic is being passed through the VPN tunnel. If a configured amount of time has lapsed since the last inbound data was received, DPD will send a message (“DPD R-U-THERE”) the next time it sends outbound IPsec data to the peer. DPD messages are unidirectional and are automatically sent by Cisco VPN clients. DPD *must* be configured on the router *only* if the router wishes to send DPD messages to the VPN client to determine the health of the client.

## Split Tunneling Control

Remote clients can support split tunneling, which enables a client to have intranet and Internet access at the same time. If split tunneling is not configured, the client will direct all traffic through the tunnel, even traffic destined for the Internet.

## Initial Contact

If a client is suddenly disconnected, the gateway may not be notified. Consequently, removal of connection information (IKE and IPsec SAs) for that client will not immediately occur. Thus, if the client attempts to reconnect to the gateway again, the gateway will refuse the connection because the previous connection information is still valid.

To avoid such a scenario, a new capability called initial contact has been introduced; it is supported by all Cisco VPN products. If a client or router is connecting to another Cisco gateway for the first time, an initial contact message is sent that tells the receiver to ignore and delete any old connection information that has been maintained for that newly connecting peer. Initial contact ensures that connection attempts are not refused because of SA synchronization problems, which are often identified via invalid security parameter index (SPI) messages and which require devices to have their connections cleared.

## Group-Based Policy Control

Policy attributes such as IP addresses, DNS, and split tunnel access can be provided on a per-group or per-user basis.



## User-Based Policy Control

Attributes may also be applied on a per-user basis. You can override a group attribute value with an individual user attribute. The attributes are retrieved at the time that user authentication via Xauth occurs. They are then combined with group attributes and applied during Mode Configuration.

From Cisco IOS Release 12.3(4)T forward, attributes can be applied on a per-user basis after the user has been authenticated. These attributes can override any similar group attributes. User-based attributes are available only if RADIUS is used as the database.

### Framed-IP-Address

To select the Framed-IP-Address attribute for CiscoSecure for NT, do the following: Under the user profile, choose the “use this IP address” option under addressing and manually enter the address. (You should check the method of configuring a framed IP address with your own RADIUS server because this procedure will vary.)

**Note**

If a framed IP address is present, and there is also a local pool address configured for the group that the user belongs to, the framed IP address will override the local pool setting.

### DHCP Client Proxy

Easy VPN servers currently assign an IP address to a remote device using either a local pool that is configured on the router or the framed IP address attribute that is defined in RADIUS. Effective with Cisco IOS Release 12.4(9)T, the DHCP Client Proxy feature provides the option of configuring an Easy VPN server to obtain an IP address from a DHCP server. The IP address is pushed to the remote device using mode configuration.

**Note**

This feature does not include functionality for the DHCP server to push the DNS, WINS server, or domain name to the remote client.

To configure DHCP Client Proxy, see the section [“Configuring an Easy VPN Server to Obtain an IP Address from a DHCP Server.”](#)

#### Benefits of DHCP Client Proxy

- The functionality provided with this feature helps in the creation of DDNS (dynamic Domain Name System) entries when a DNS server exists in conjunction with the DHCP server.
- The user is not restricted to IP address pools.

### User-Save-Password

As per the group description, the User-Save-Password attribute can be received in addition to the group variant (Save-Password), but if it is received, it will override the value asserted by the group.

The following is an output example of a RADIUS AV pair for the User-Save-Password attribute:

```
ipsec:user-save-password=1
```

### User-Include-Local-LAN

As per the group description, the User-Include-Local-LAN attribute can be received in addition to the group variant (Include-Local-LAN), but if it is received, it will override the value asserted by the group.

The following is an output example of a RADIUS AV pair for the User-Include-Local LAN attribute:

```
ipsec:user-include-local-lan=1
```

## User-VPN-Group

The User-VPN-Group attribute is a replacement for the [Group-Lock](#) attribute. It allows support for both preshared key and RSA signature authentication mechanisms such as certificates.

If you need to check that the group a user is attempting to connect to is indeed the group the user belongs to, use the User-VPN-Group attribute. The administrator sets this attribute to a string, which is the group that the user belongs to. The group the user belongs to is matched against the VPN group as defined by group name (ID\_KEY\_ID) for preshared keys or by the OU field of a certificate. If the groups do not match, the client connection is terminated.

This feature works only with AAA RADIUS. Local Xauth authentication must still use the Group-Lock attribute.

The following is an output example of a RADIUS AV pair for the Use-VPN-Group attribute:

```
ipsec:user-vpn-group=cisco
```

## Group-Lock

If you are only using pre-shared keys (no certificates or other RSA signature authentication mechanisms) with RADIUS or local AAA, you can continue to use the Group-Lock attribute. If you are only using pre-shared keys (no certificates or other RSA signature authentication mechanisms) with RADIUS, you can either continue to use the Group-Lock attribute or you can use the new [User-VPN-Group](#) attribute.



### Caution

Do not use the Group-Lock attribute if you are using RSA signature authentication mechanisms such as certificates. Use the [User-VPN-Group](#) attribute instead.

## Session Monitoring for VPN Group Access

It is possible to mimic the functionality provided by some RADIUS servers for limiting the maximum number of connections to a specific server group and also for limiting the number of simultaneous logins for users in that group. After user-defined thresholds are defined in each VPN group, connections will be denied until counts drop below these thresholds.

If you use a RADIUS server, such as CiscoSecure ACS, it is recommended that you enable this session control on the RADIUS server if the functionality is provided. In this way, usage can be controlled across a number of servers by one central repository. When enabling this feature on the router itself, only connections to groups on that specific device are monitored. Load-sharing scenarios are not accurately accounted for.

To configure session monitoring using command-line interface (CLI), use the **crypto isakmp client configuration group** command and the **max-users** and **max-logins** subcommands.

The following is an output example of RADIUS AV pairs that have been added to the relevant group:

```
ipsec:max-users=1000
ipsec:max-logins=1
```

## Virtual IPsec Interface Support on a Server

Virtual IPsec Interface Support on a Server allows you to selectively send traffic to different Easy VPN concentrators (servers) as well as to the Internet.

Before Cisco IOS Release 12.4(4)T, at the tunnel-up/tunnel-down transition, attributes that were pushed during the mode configuration had to be parsed and applied. When such attributes resulted in the configurations being applied on the interface, the existing configuration had to be overridden.

With the Virtual Ipsec Interface Support feature, the tunnel-up configuration can be applied to separate interfaces, making it easier to support separate features at tunnel-up. Features that are applied to the traffic going into the tunnel can be separate from the features that are applied to traffic that is not going through the tunnel (for example, split-tunnel traffic and traffic leaving the device when the tunnel is not up). When the Easy VPN negotiation is successful, the line protocol state of the virtual-access interface gets changed to up. When the Easy VPN tunnel goes down because the SA expires or is deleted, the line protocol state of the virtual-access interfaces changes to down.

**Note**

---

This feature does not support multicast.

---

For more information about this feature, see the document [Cisco Easy VPN Remote](#). (This feature is configured on the Easy VPN remote device.)

For information about the IPsec Virtual Tunnel Interface feature, see the document “IPSec Virtual Tunnel Interface” (link in the “[Related Documents](#)” section of this document).

## Virtual Tunnel Interface Per-User Attribute Support

Effective with Cisco IOS Release 12.4(9)T, Virtual Tunnel Interface provides per-user attribute support for Easy VPN servers.

For more information about this feature, see the document [IPsec Virtual Tunnel Interface](#).

## Banner, Auto-Update, and Browser Proxy

The following features provide support for attributes that aid in the management of the Cisco Easy VPN remote device.

### Banner

An Easy VPN server can be configured to push the banner to the Easy VPN remote device. A banner is needed for the web-based activation feature. The banner is displayed when the Easy VPN tunnel is up on the Easy VPN remote console or as a HTML page in the case of web-based activation.

### Auto-Update

An Easy VPN server can be configured to provide an automated mechanism for software and firmware upgrades on an Easy VPN remote device.

## Browser Proxy

An Easy VPN server can be configured so that an Easy VPN remote device can access resources on the corporate network. Using this feature, the user does not have to manually modify the proxy settings of his or her web browser when connecting to the corporate network using Cisco IOS VPN Client or manually revert the proxy settings upon disconnecting.

## Configuration Management Enhancements

### Pushing a Configuration URL Through a Mode-Configuration Exchange

When remote devices connect to a corporate gateway for creating an IPsec VPN tunnel, some policy and configuration information has to be applied to the remote device when the VPN tunnel is active to allow the remote device to become a part of the corporate VPN.

The Pushing a Configuration URL Through a Mode-Configuration Exchange feature provides for a mode-configuration attribute that “pushes” a URL from the concentrator (server) to the Cisco IOS Easy VPN remote device. The URL contains the configuration information that the remote device has to download and apply to the running configuration, and it contains the Cisco IOS CLI listing. (For more information about a Cisco IOS CLI listing, see Cisco IOS documentation for the **configuration url** command.) The CLI for this feature is configured on the concentrator.

The configuration that is pushed to the remote device is persistent by default. That is, the configuration is applied when the IPsec tunnel is “up,” but it is not withdrawn when the IPsec tunnel goes “down.” However, it is possible to write a section of configuration that is transient in nature, in which case the configuration of the section is reverted when the tunnel is disconnected.

There are no restrictions on where the configuration distribution server is physically located. However, it is recommended that a secure protocol such as HTTPS (Secure HTTP) be used to retrieve the configuration. The configuration server can be located in the corporate network, so because the transfer happens through the IPsec tunnel, insecure access protocols (HTTP) can be used.

Regarding backward compatibility: the remote device asks for the CONFIGURATION-URL and CONFIGURATION-VERSION attributes. Because the CONFIGURATION-URL and CONFIGURATION-VERSION attributes are not mandatory attributes, the server sends them only if it has them configured for the group. There is no built-in restriction to push the configuration, but bootstrap configurations (such as for the IP address) cannot be sent because those configurations are required to set up the Easy VPN tunnel, and the CONFIGURATION-URL comes into effect only after the Easy VPN tunnel comes up.

### After the Configuration Has Been Acquired by the Easy VPN Remote Device

After the configuration has been acquired by the Easy VPN remote device, the remote device sends a new ISAKMP notification to the Easy VPN server. The notification contains several manageability information messages about the client (remote device). The Easy VPN server takes two actions when this information is received:

- The Easy VPN server caches the information in its peer database. The information can be displayed by using the **show crypto isakmp peer config** command. This command output displays all manageability information that is sent by the client (remote device).
- If accounting is enabled, the Easy VPN server sends an accounting update record that contains the manageability information messages about the remote device to the accounting RADIUS server. This accounting update is later available in the accounting log of the RADIUS server.

## How to Configure This Feature

The commands that are used to configure this feature and the attributes CONFIGURATION-URL and CONFIGURATION-VERSION are described in the **crypto isakmp client configuration group** command documentation.

## Per User AAA Policy Download with PKI

With the Support of Per User AAA Policy Download with PKI feature, user attributes are obtained from the AAA server and pushed to the remote device through mode configuration. The username that is used to get the attributes is retrieved from the remote device certificate.

## Per-User Attribute Support for Easy VPN Servers

The Per-User Attribute Support for Easy VPN Servers feature provides users with the ability to support per-user attributes on Easy VPN servers. These attributes are applied on the virtual access interface.

### Local Easy VPN AAA Server

For a local Easy VPN AAA server, the per-user attributes can be applied at the group level or at the user level using the command-line interface (CLI).

To configure per-user attributes for a local Easy VPN server, see “[Configuring Per-User Attributes on a Local Easy VPN AAA Server](#).”

### Remote Easy VPN AAA Server

Attribute value (AV) pairs can be defined on a remote Easy VPN AAA server as shown in this example:  
cisco-avpair = “ip:outacl#101=permit tcp any any established

### Per-User Attributes

The following per-user attributes are currently defined in the AAA server and are applicable to IPsec:

- inacl
- interface-config
- outacl
- route
- rte-fltr-in
- rte-fltr-out
- sub-policy-In
- sub-policy-Out
- policy-route
- prefix

## Syslog Message Enhancements

Some new syslog messages have been added for Easy VPN in Cisco IOS Release 12.4(4)T. The syslog messages can be enabled on your server by using the command-line interface (CLI). The format of the syslog messages is as follows:

```
timestamp: %CRYPTO-6-VPN_TUNNEL_STATUS: (Server) <event message> User=<username>
Group=<groupname> Client_public_addr=<ip_addr> Server_public_addr=<ip_addr>
```

For an authentication-passed event, the syslog message looks like the following:

```
Jul 25 23:33:06.847: %CRYPTO-6-VPN_TUNNEL_STATUS: (Server) Authentication PASS
ED User=blue Group=Cisco1760group Client_public_addr=10.20.20.1
Server_public_addr=10.20.20.2
```

Three of the messages (Max users, Max logins, and Group does not exist) are authorization issues and are printed only with the group name in the format. The reason for only the group name being printed is that authorization check happens much before mode configuration happens. Therefore, the peer information is not yet present and cannot be printed. The following is an example of a “Group does not exist” message.

```
*Jun 30 18:02:58.107: %CRYPTO-6-VPN_TUNNEL_STATUS: Group: group_1 does not exist
```

## Easy VPN Syslog Messages That Are Supported

Both `ezvpn_connection_up` and `ezvpn_connection_down` were already supported in a previous release of syslog messages. The enhancements in Cisco IOS Release 12.4(4)T follow the same format, but new syslogs are introduced. The added syslogs are as follows:

- Authentication Passed
- Authentication Rejected
  - Group Lock Enabled
  - Incorrect Username or Password
  - Max Users exceeded/Max Logins exceeded
  - No. of Retries exceeded
- Authentication Failed (AAA Not Contactable)
- IP Pool Not present/No Free IP Address available in the pool
- ACL associated with Ezvpn policy but NOT defined (hence, no split tunneling possible)
- Save password Turned ON
- Incorrect firewall record being sent by Client (incorrect vendor | product | capability)
- Authentication Rejected
  - Access restricted via incoming interface
  - Group does not exist

## Network Admission Control Support for Easy VPN

Network Admission Control was introduced in Cisco IOS Release 12.3(8)T as a way to determine whether a PC client should be allowed to connect to the LAN. Network Admission Control uses Extensible Authentication Protocol over UDP (EAPoUDP) to query the Cisco trust agent on the PC and allows a PC to access the network if the client status is healthy. Different policies can be applied on the server to deny or limit access of PCs that are infected.

Effective with Cisco IOS Release 12.4(4)T, Network Admission Control can now be used to monitor the status of remote PC clients as well. After the Easy VPN tunnel comes up and the PC starts to send traffic, the traffic is intercepted at the Easy VPN server, and the posture validation process starts. The posture validation process consists of sending an EAPoUDP request over the Easy VPN tunnel and querying the Cisco trust agent. The authentication server is configured inside the trusted network, behind the IPsec aggregator.

The configuration of an Easy VPN server that has Network Admission Control enabled is shown in the output in [Network Admission Control: Example, page 64](#).

## Central Policy Push Firewall Policy Push

The Easy VPN server supports Central Policy Push (CPP) Firewall Policy Push. This feature allows administrators to push policies that enforce security to the Cisco Easy VPN (software) Client and related firewall software.

A split tunnel enables access to corporate networks, but it also allows a remote device to be exposed to attacks from the Internet. This feature enables the server to determine whether to allow or deny a tunnel if the remote device does not have a required firewall, thereby reducing exposure to attacks.

The following firewall types are supported:

- Cisco-Integrated-firewall (central-policy-push)
- Cisco-Security-Agent (check-presence)
- Zonelabs-Zonealarm (both)
- Zonelabs-ZonealarmPro (both)

The server can be used either to check the presence of a firewall on the client (remote device) using the check-presence option or to specify the specifics of the firewall policies that must be applied by the client using the central-policy-push.



### Note

The **policy check-presence command and keyword**, which are used with this feature, replace the **firewall are-u-there command functionality** that was supported before Cisco IOS Release 12.4(6)T. The **firewall are-u-there command** will continue to be supported for backward compatibility.

To enable this feature, see the sections “[Defining a CPP Firewall Policy Push Using a Local AAA Server](#)” and “[Applying a CPP Firewall Policy Push to the Configuration Group](#).”

## Syslog Support for CPP Firewall Policy Push

Syslog support can be enabled using the **crypto logging ezvpn** command on your router. CPP syslog messages will be printed for the following error conditions:

- If policy is configured on a group configuration (using the **firewall policy** command), but a global policy with the same name is not defined (using the **crypto isakmp client firewall** command). The syslog message is as follows:

```
Policy enabled on group configuration but not defined
```

Tunnel setup proceeds as normal (with the firewall).

- If an incorrect firewall request (vendor/product/cap incorrect order) is received, the syslog message is as follows:

```
Incorrect firewall record received from client
```

- If a policy mismatch occurs between the Cisco VPN Client and the server, the syslog is as follows:  
`CPP policy mismatch between client and headend`

## Password Aging

Prior to Cisco IOS Release 12.4(6)T, EasyVPN remote devices (clients) sent username and password values to the Easy VPN server, which in turn sent them to the AAA subsystem. The AAA subsystem generated an authentication request to the RADIUS server. If the password had expired, the RADIUS server replied with an authentication failure. The reason for the failure was not passed back to the AAA subsystem. The user was denied access due to authentication failure, but he or she did not know that the failure was due to password expiration.

Effective with Cisco IOS Release 12.4(6)T, if you have configured the Password Aging feature, the EasyVPN client is notified when a password has expired, and you are prompted to enter a new password. To configure the Password Aging feature, see the section “[Configuring Password Aging](#).”

For more information about Password Aging, see the reference for “Password Aging” in the section [Additional References](#) (subsection “Related Documents”).

## Split DNS

Effective with Cisco IOS Release 12.4(9)T, split DNS functionality is available on Easy VPN servers. This feature enables the Easy VPN hardware client to use primary and secondary DNS values to resolve DNS queries. These values are pushed by the Easy VPN server to the Easy VPN remote device. To configure this feature on your server, use the **split-dns** command (see the section “[Defining Group Policy Information for Mode Configuration Push](#)”). Configuring this command adds the split-dns attribute to the policy group. The attribute will include the list of domain names that you configured. All other names will be resolved using the public DNS server.

For more information about configuring split DNS, see “Configuring Split and Dynamic DNS on the Cisco VPN 3000” at the following URL:

[http://www.cisco.com/warp/public/471/dns\\_split\\_dynam.pdf](http://www.cisco.com/warp/public/471/dns_split_dynam.pdf)

## cTCP

The Cisco Tunneling Control Protocol (cTCP) feature can be used for situations in which an Easy VPN remote device is operating in an environment in which standard IPsec does not function or in which it does not function transparently without modification to existing firewall rules. These situations include the following:

- Small or home office router performing Network Address Translation (NAT) or Port Address Translation (PAT)
- PAT-provided IP address behind a larger router (for example, in a corporation)
- Non-NAT firewall (packet filtering or stateful)
- Proxy server

The firewall should be configured to allow the headend to accept cTCP connections on the configured cTCP port. This configuration is enabled on the Easy VPN server. If the firewall is not configured, it will not allow the cTCP traffic.



**Note**

cTCP traffic is actually Transmission Control Protocol (TCP) traffic. cTCP packets are IKE or Encapsulating Security Payload (ESP) packets that are being transmitted over TCP.

## How to Configure Easy VPN Server

This section includes the following procedures:

- [Enabling Policy Lookup via AAA, page 20](#) (required)
- [Defining Group Policy Information for Mode Configuration Push, page 21](#) (required)
- [Enabling VPN Session Monitoring, page 24](#) (optional)
- [Verifying a VPN Session, page 25](#) (optional)
- [Applying Mode Configuration and Xauth, page 26](#) (required)
- [Enabling Reverse Route Injection for the Client, page 27](#) (optional)
- [Enabling IKE Dead Peer Detection, page 28](#) (optional)
- [Configuring RADIUS Server Support, page 29](#) (optional)
- [Verifying Easy VPN Server, page 30](#) (optional)
- [Configuring a Banner, page 30](#) (optional)
- [Configuring Auto Upgrade, page 31](#) (optional)
- [Configuring Browser Proxy, page 32](#) (optional)
- [Configuring the Pushing of a Configuration URL Through a Mode-Configuration Exchange, page 33](#) (optional)
- [Configuring Per User AAA Download with PKI—Configuring the Crypto PKI Trustpoint, page 34](#) (optional)
- [Configuring the Actual Per User AAA Download with PKI, page 36](#) (optional)
- [Configuring Per-User Attributes on a Local Easy VPN AAA Server, page 38](#)
- [Configuring Per-User Attributes on a Local Easy VPN AAA Server, page 38](#) (optional)
- [Defining a CPP Firewall Policy Push Using a Local AAA Server, page 40](#) (optional)
- [Applying a CPP Firewall Policy Push to the Configuration Group, page 41](#) (optional)
- [Defining a CPP Firewall Policy Push Using a Remote AAA Server, page 42](#) (optional)
- [Adding the VSA CPP-Policy Under the Group Definition, page 42](#) (optional)
- [Verifying CPP Firewall Policy Push, page 43](#) (optional)
- [Configuring Password Aging, page 43](#) (optional)
- [Configuring Split DNS, page 45](#) (optional)
- [Verifying Split DNS, page 46](#) (optional)
- [Monitoring and Maintaining Split DNS, page 47](#) (optional)
- [Configuring an Easy VPN Server to Obtain an IP Address from a DHCP Server, page 48](#) (optional)
- [Verifying DHCP Client Proxy, page 49](#) (optional)
- [Monitoring and Maintaining DHCP Client Proxy, page 50](#) (optional)

- [Configuring cTCP, page 50](#) (optional)
- [Verifying cTCP, page 51](#) (optional)
- [Monitoring and Maintaining a cTCP Configuration, page 51](#) (optional)
- [Troubleshooting a cTCP Configuration, page 53](#) (optional)

## Enabling Policy Lookup via AAA

To enable policy lookup via AAA, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication password-prompt** *text-string*
5. **aaa authentication username prompt** *text-string*
6. **aaa authentication login** [*list-name method1*] [*method2...*]
7. **aaa authorization network** *list-name* **local group radius**
8. **username** *name* **password** *encryption-type* *encrypted-password*

### DETAILED STEPS

|        | Command                                                                                                                                                               | Purpose                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                        | Enters global configuration mode.                                                                                     |
| Step 3 | <b>aaa new-model</b><br><br><b>Example:</b><br>Router (config)# aaa new-model                                                                                         | Enables AAA.                                                                                                          |
| Step 4 | <b>aaa authentication password-prompt</b> <i>text-string</i><br><br><b>Example:</b><br>Router (config)# aaa authentication password-prompt "Enter your password now:" | (Optional) Changes the text displayed when users are prompted for a password.                                         |

|        | Command                                                                                                                                                                                         | Purpose                                                                                                                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <b>aaa authentication username-prompt</b><br><i>text-string</i><br><br><b>Example:</b><br>Router (config)# aaa authentication<br>username-prompt "Enter your name here:"                        | (Optional) Changes the text displayed when users are prompted to enter a username.                                                                                                                                        |
| Step 6 | <b>aaa authentication login</b> [ <i>list-name</i><br><i>method1</i> ] [ <i>method2...</i> ]<br><br><b>Example:</b><br>Router (config)# aaa authentication login<br>userlist local group radius | Sets AAA authentication at login. <ul style="list-style-type: none"> <li>A local and RADIUS server may be used together and will be tried in order.</li> </ul> <b>Note</b> This command must be enabled to enforce Xauth. |
| Step 7 | <b>aaa authorization network</b> <i>list-name</i> <b>local</b><br><b>group radius</b><br><br><b>Example:</b><br>Router (config)# aaa authorization<br>network grouplist local group radius      | Enables group policy lookup. <ul style="list-style-type: none"> <li>A local and RADIUS server may be used together and will be tried in order.</li> </ul>                                                                 |
| Step 8 | <b>username</b> <i>name</i> <b>password</b> <i>encryption-type</i><br><i>encrypted-password</i><br><br><b>Example:</b><br>Router (config)# username server_r<br>password 7 121F0A18             | (Optional) Defines local users for Xauth if RADIUS or TACACS+ is not used. <b>Note</b> Use this command only if no external validation repository will be used.                                                           |

## Defining Group Policy Information for Mode Configuration Push

Although users can belong to only one group per connection, they may belong to specific groups with different policy requirements. Thus, users may decide to connect to the client using a different group ID by changing their client profile on the VPN device. To define the policy attributes that are pushed to the client via Mode Configuration, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** {*group-name* | **default**}
4. **key** *name*
5. **dns** *primary-server secondary-server*
6. **wins** *primary-server secondary-server*
7. **domain** *name*
8. **pool** *name*
9. **acl** *number*
10. **access-restrict** {*interface-name*}
11. **policy check-presence**

- or
- firewall are-u-there**
12. **group-lock**
  13. **include-local-lan**
  14. **save-password**
  15. **backup-gateway**
  16. **pfs**

## DETAILED STEPS

|        | Command                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                            |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                  | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                          | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                  |
| Step 3 | <b>crypto isakmp client configuration group</b><br>{group-name   default}<br><br><b>Example:</b><br>Router (config)# crypto isakmp client<br>configuration group group1 | Specifies the policy profile of the group that will be defined and enters Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. <ul style="list-style-type: none"> <li>If no specific group matches and a default group is defined, users will automatically be given the policy of a default group.</li> </ul> |
| Step 4 | <b>key name</b><br><br><b>Example:</b><br>Router (config-isakmp-group)# key group1                                                                                      | Specifies the IKE preshared key for group policy attribute definition. <p><b>Note</b> This command <i>must</i> be enabled if the client identifies itself with a preshared key.</p>                                                                                                                                                                |
| Step 5 | <b>dns primary-server secondary-server</b><br><br><b>Example:</b><br>Router (config-isakmp-group)# dns 10.2.2.2<br>10.3.3.3                                             | (Optional) Specifies the primary and secondary DNS servers for the group.                                                                                                                                                                                                                                                                          |
| Step 6 | <b>wins primary-server secondary-server</b><br><br><b>Example:</b><br>Router (config-isakmp-group)# wins<br>10.10.10.10 10.12.12.12                                     | (Optional) Specifies the primary and secondary WINS servers for the group.                                                                                                                                                                                                                                                                         |
| Step 7 | <b>domain name</b><br><br><b>Example:</b><br>Router (config-isakmp-group)# domain<br>domain.com                                                                         | (Optional) Specifies the DNS domain to which a group belongs.                                                                                                                                                                                                                                                                                      |

|         | Command                                                                                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 8  | <b>pool</b> <i>name</i><br><br><b>Example:</b><br>Router (config-isakmp-group)# pool green                                                                                                                                        | Defines a local pool address. <ul style="list-style-type: none"> <li>Although a user must define at least one pool name, a separate pool may be defined for each group policy.</li> </ul> <b>Note</b> This command <i>must</i> be defined and refer to a valid IP local pool address or the client connection will fail.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 9  | <b>acl</b> <i>number</i><br><br><b>Example:</b><br>Router (config-isakmp-group)# acl 199                                                                                                                                          | (Optional) Configures split tunneling. <ul style="list-style-type: none"> <li>The <i>number</i> argument specifies a group of access control list (ACL) rules that represent protected subnets for split tunneling purposes.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Step 10 | <b>access-restrict</b> { <i>interface-name</i> }<br><br><b>Example:</b><br>Router (config-isakmp-group)#<br>access-restrict fastethernet0/0                                                                                       | Restricts clients in a group to an interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 11 | <b>policy check-presence</b><br><br>or<br><br><b>firewall are-u-there</b><br><br><b>Example:</b><br>Router (config-isakmp-group)# policy<br>check-presence<br><br>or<br><br>Router (config-isakmp-group)# firewall<br>are-u-there | (Optional) Denotes that the server should check for the presence of the specified firewall (as shown as the firewall type on the client).<br><br>or<br><br>Adds the firewall are-u-there attribute to the server group if your PC is running the Black Ice or Zone Alarm personal firewalls.<br><br><b>Note</b> The <b>policy</b> command and <b>check-presence</b> keyword were added to Cisco IOS documentation in Cisco IOS 12.4(6)T. It is recommended that the <b>policy</b> command be used instead of the <b>firewall are-u-there</b> command because the <b>policy</b> command is supported in local AAA and remote AAA configurations. The <b>firewall are-u-there</b> command can be figured only locally, but it is still supported for backward compatibility. |
| Step 12 | <b>group-lock</b><br><br><b>Example:</b><br>Router (config-isakmp-group)# group-lock                                                                                                                                              | Enforces the group lock feature.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 13 | <b>include-local-lan</b><br><br><b>Example:</b><br>Router (config-isakmp-group)#<br>include-local-lan                                                                                                                             | (Optional) Configures the Include-Local-LAN attribute to allow a nonsplit-tunneling connection to access the local subnetwork at the same time as the client.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 14 | <b>save-password</b><br><br><b>Example:</b><br>Router (config-isakmp-group)#<br>save-password                                                                                                                                     | (Optional) Saves your Xauth password locally on your PC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

|         | Command                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 15 | <b>backup-gateway</b><br><br><b>Example:</b><br>Router (config-isakmp-group)# backup gateway | (Optional) Rather than have backup gateways added to client configurations manually, it is possible to have the server “push down” a list of backup gateways to the client device. <ul style="list-style-type: none"> <li>These gateways are tried in order in the case of a failure of the previous gateway. The gateways may be specified using IP addresses or host names.</li> </ul>                                                                                                        |
| Step 16 | <b>pfs</b><br><br><b>Example:</b><br>Router (config-isakmp-group)# pfs                       | (Optional) Notifies the client of the central-site policy regarding whether PFS is required for any IPsec SA. <ul style="list-style-type: none"> <li>Because the client device does not have a user interface option to enable or disable PFS negotiation, the server will notify the client device of the central site policy using this parameter. The Diffie-Hellman (D-H) group that is proposed for PFS will be the same that was negotiated in Phase 1 of the IKE negotiation.</li> </ul> |

## Enabling VPN Session Monitoring

If you wish to set restrictions on the maximum number of connections to the router per VPN group and the maximum number of simultaneous logins per user, add the following attributes to the VPN group.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** *group-name*
4. **exit**
5. **max-logins** *number-of-logins*
6. **max-users** *number-of-users*

### DETAILED STEPS

|        | Command                                                                        | Purpose                                                                                                          |
|--------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                |

|        | Command                                                                                                                                                      | Purpose                                                                                                                                                                                                                                             |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>crypto isakmp client configuration group</b> <i>group-name</i><br><br><b>Example:</b><br>Router (config)# crypto isakmp client configuration group group1 | Specifies the policy profile of the group that will be defined and enters ISAKMP group configuration mode. <ul style="list-style-type: none"> <li><i>group-name</i>—Group definition that identifies which policy is enforced for users.</li> </ul> |
| Step 4 | <b>exit</b><br><br><b>Example:</b><br>Router (config-isakmp-group)# exit                                                                                     | Exits ISAKMP group configuration mode.                                                                                                                                                                                                              |
| Step 5 | <b>max-logins</b> <i>number-of-logins</i><br><br><b>Example:</b><br>Router (config-isakmp-group)# max-logins 10                                              | (Optional) Limits the number of simultaneous logins for users in a specific server group.                                                                                                                                                           |
| Step 6 | <b>max-users</b> <i>number-of-users</i><br><br><b>Example:</b><br>Router (config)# max-users 1000                                                            | (Optional) Limits the number of connections to a specific server group.                                                                                                                                                                             |

## Verifying a VPN Session

To verify a VPN session, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **show crypto session group**
3. **show crypto session summary**

### DETAILED STEPS

|        | Command                                                                                      | Purpose                                                                                                          |
|--------|----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                       | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>show crypto session group</b><br><br><b>Example:</b><br>Router# show crypto session group | Displays groups that are currently active on the VPN device.                                                     |

|        | Command                                                                                          | Purpose                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>show crypto session summary</b><br><br><b>Example:</b><br>Router# show crypto session summary | Displays groups that are currently active on the VPN device and the users that are connected for each of those groups. |

## Applying Mode Configuration and Xauth

Mode Configuration and Xauth must be applied to a crypto map to be enforced. To apply Mode Configuration and Xauth to a crypto map, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map tag client configuration address [initiate | respond]**
4. **crypto map map-name isakmp authorization list list-name**
5. **crypto map map-name client authentication list list-name**

### DETAILED STEPS

|        | Command                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                  | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                                                                               |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                          | Enters global configuration mode.                                                                                                                                                                                                                                                                                                 |
| Step 3 | <b>crypto map tag client configuration address [initiate   respond]</b><br><br><b>Example:</b><br>Router (config)# crypto map dyn client configuration address initiate | Configures the router to initiate or reply to Mode Configuration requests.<br><br><b>Note</b> Cisco clients require the <b>respond</b> keyword to be used; however, if the Cisco Secure VPN Client 1.x is used, the <b>initiate</b> keyword must be used; <b>initiate</b> and <b>respond</b> keywords may be used simultaneously. |
| Step 4 | <b>crypto map map-name isakmp authorization list list-name</b><br><br><b>Example:</b><br>Router (config)# crypto map ikessaaamap isakmp authorization list ikessaaalist | Enables IKE querying for group policy when requested by the client.<br><ul style="list-style-type: none"><li>• The <i>list-name</i> argument is used by AAA to determine which storage source is used to find the policy (local or RADIUS) as defined in the <b>aaa authorization network</b> command.</li></ul>                  |



|        | Command                                                                                                                                                                                                             | Purpose                                                                                                                                                                                                                                                  |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <b>crypto map</b> <i>map-name</i> <b>client authentication</b><br><b>list</b> <i>list-name</i><br><br><b>Example:</b><br>Router (config)# <b>crypto map</b> xauthmap<br><b>client authentication</b> list xauthlist | Enforces Xauth. <ul style="list-style-type: none"> <li>The <i>list-name</i> argument is used to determine the appropriate username and password storage location (local or RADIUS) as defined in the <b>aaa authentication login</b> command.</li> </ul> |

## Enabling Reverse Route Injection for the Client

To enable RRI on the crypto map (static or dynamic) for VPN client support, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto dynamic** *map-name* *seq-num*  
or  
**crypto map** *map-name* *seq-num* **ipsec-isakmp**
4. **set peer** *ip-address*
5. **set transform-set** *transform-set-name*
6. **reverse-route**
7. **match-address**

### DETAILED STEPS

|        | Command                                                                               | Purpose                                                                                                         |
|--------|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> <b>enable</b>                         | Enables privileged EXEC mode <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b> | Enters global configuration mode.                                                                               |

|               | Command                                                                                                                                                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                               |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 3</b> | <b>crypto dynamic</b> <i>map-name seq-num</i><br>or<br><b>crypto map</b> <i>map-name seq-num ipsec-isakmp</i><br><br><b>Example:</b><br>Router (config)# <b>crypto dynamic</b> mymap 10<br><br>or<br>Router (config)# <b>crypto map</b> yourmap 15<br>ipsec-isakmp | Creates a dynamic crypto map entry and enters crypto map configuration mode.<br><br>or<br><br>Adds a dynamic crypto map set to a static crypto map set and enters crypto map configuration mode.                                                                                                      |
| <b>Step 4</b> | <b>set peer</b> <i>ip-address</i><br><br><b>Example:</b><br>Router (config-crypto-map)# <b>set peer</b> 10.20.20.20                                                                                                                                                | Specifies an IPsec peer IP address in a crypto map entry. <ul style="list-style-type: none"> <li>This step is optional when configuring dynamic crypto map entries.</li> </ul>                                                                                                                        |
| <b>Step 5</b> | <b>set transform-set</b> <i>transform-set-name</i><br><br><b>Example:</b><br>Router (config-crypto-map)# <b>set transform-set</b> dessha                                                                                                                           | Specifies which transform sets are allowed for the crypto map entry. <ul style="list-style-type: none"> <li>Lists multiple transform sets in order of priority (highest priority first).</li> </ul> <b>Note</b> This list is the only configuration statement required in dynamic crypto map entries. |
| <b>Step 6</b> | <b>reverse-route</b><br><br><b>Example:</b><br>Router (config-crypto-map)# <b>reverse-route</b>                                                                                                                                                                    | Creates source proxy information.                                                                                                                                                                                                                                                                     |
| <b>Step 7</b> | <b>match address</b><br><br><b>Example:</b><br>Router (config-crypto-map)# <b>match address</b>                                                                                                                                                                    | Specifies an extended access list for a crypto map entry. <ul style="list-style-type: none"> <li>This step is optional when configuring dynamic crypto map entries.</li> </ul>                                                                                                                        |

## Enabling IKE Dead Peer Detection

To enable a Cisco IOS VPN gateway (instead of the client) to send IKE DPD messages, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp keepalive** *secs retries*

## DETAILED STEPS

|        | Command                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                             |
|--------|----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                    |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                       | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                   |
| Step 3 | <b>crypto isakmp keepalive secs retries</b><br><br><b>Example:</b><br>Router (config)# crypto isakmp keepalive 20 10 | Allows the gateway to send DPD messages to the router. <ul style="list-style-type: none"> <li>The <i>secs</i> argument specifies the number of seconds between DPD messages (the range is from 1 to 3600 seconds); the <i>retries</i> argument specifies the number of seconds between retries if DPD messages fail (the range is from 2 to 60 seconds).</li> </ul> |

## Configuring RADIUS Server Support

To configure access to the server and allow the Cisco IOS VPN device to send requests to the server, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius server host *ip-address* [auth-port *port-number*] [acct-port *port-number*] [key string]**

### DETAILED STEPS

|        | Command                                                | Purpose                                                                                                          |
|--------|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |

|        | Command                                                                                                                                                  | Purpose                                                                                               |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Step 2 | <b>configure terminal</b>                                                                                                                                | Enters global configuration mode.                                                                     |
|        | <b>Example:</b><br>Router# configure terminal                                                                                                            |                                                                                                       |
| Step 3 | <b>radius server host</b> <i>ip-address</i> [ <b>auth-port</b> <i>port-number</i> ] [ <b>acct-port</b> <i>port-number</i> ] [ <b>key</b> <i>string</i> ] | Specifies a RADIUS server host.                                                                       |
|        | <b>Example:</b><br>Router (config)# radius server host<br>192.168.1.1. auth-port 1645 acct-port 1646<br>key XXXX                                         | <b>Note</b> This step is required if you choose to store group policy information in a RADIUS server. |

## Verifying Easy VPN Server

To verify your configurations for this feature, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **show crypto map** [*interface interface* | *tag map-name*]

### DETAILED STEPS

|        | Command                                                                     | Purpose                                                                              |
|--------|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                                               | Enables privileged EXEC mode.                                                        |
|        | <b>Example:</b><br>Router> enable                                           | <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>show crypto map</b> [ <i>interface interface</i>   <i>tag map-name</i> ] | Displays the crypto map configuration.                                               |
|        | <b>Example:</b><br>Router# show crypto map interface ethernet 0             |                                                                                      |

## Configuring a Banner

To configure an Easy VPN server to push a banner to an Easy VPN remote device, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** {*group-name*}

#### 4. `banner c {banner-text} c`

### DETAILED STEPS

|        | Command                                                                                                                                                 | Purpose                                                                                                          |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                  | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                          | Enters global configuration mode.                                                                                |
| Step 3 | <b>crypto isakmp client configuration group {group-name}</b><br><br><b>Example:</b><br>Router (config)# crypto isakmp client configuration group Group1 | Specifies to which group a policy profile will be defined and enters crypto ISAKMP group configuration mode.     |
| Step 4 | <b>banner c {banner-text} c</b><br><br><b>Example:</b><br>Router (config-isakmp-group)# banner c The quick brown fox jumped over the lazy dog c         | Specifies the text of the banner.                                                                                |

## Configuring Auto Upgrade

To configure an Easy VPN server to provide an automated mechanism to make software and firmware upgrades automatically available to an Easy VPN remote device, perform the following steps.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `crypto isakmp client configuration group {group-name}`
4. `auto-update client {type-of-system} {url url} {rev review-version}`

## DETAILED STEPS

|        | Command                                                                                                                                                                                                                     | Purpose                                                                                                          |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                      | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                              | Enters global configuration mode.                                                                                |
| Step 3 | <b>crypto isakmp client configuration group</b> {group-name}<br><br><b>Example:</b><br>Router (config)# crypto isakmp client configuration group Group2                                                                     | Specifies to which group a policy profile will be defined and enters crypto ISAKMP group configuration mode.     |
| Step 4 | <b>auto-update client</b> {type-of-system} {url} {rev review-version}<br><br><b>Example:</b><br>Router (config-isakmp-group)# auto-update client Win2000 url http:www.ourcompanysite.com/newclient rev 3.0.1(Rel), 3.1(Rel) | Configures auto-update parameters for an Easy VPN remote device.                                                 |

## Configuring Browser Proxy

To configure an EasyVPN server so that the Easy VPN remote device can access resources on the corporate network when using Cisco IOS VPN Client software, perform the following steps. With this configuration, the user does not have to manually modify the proxy settings of his or her web browser when connecting and does not have to manually revert the proxy settings when disconnecting.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration browser-proxy** {browser-proxy-name}
4. **proxy** {proxy-parameter}

## DETAILED STEPS

|        | Command                                                                                                                                                                         | Purpose                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                          | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>      |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                  | Enters global configuration mode.                                                                                     |
| Step 3 | <b>crypto isakmp client configuration browser-proxy {browser-proxy-name}</b><br><br><b>Example:</b><br>Router (config)# crypto isakmp client configuration browser-proxy bproxy | Configures browser-proxy parameters for an Easy VPN remote device and enters ISAKMP Browser Proxy configuration mode. |
| Step 4 | <b>proxy {proxy-parameter}</b><br><br><b>Example:</b><br>Router (config-ikmp-browser-proxy)# proxy auto-detect                                                                  | Configures proxy parameters for an Easy VPN remote device.                                                            |

## Configuring the Pushing of a Configuration URL Through a Mode-Configuration Exchange

To configure an Easy VPN server to push a configuration URL through a Mode-Configuration Exchange, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group {group-name}**
4. **configuration url {url}**
5. **configuration version {version-number}**

## DETAILED STEPS

|        | Command                                                                                                                                                 | Purpose                                                                                                                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                  | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                          | Enters global configuration mode.                                                                                                                                                                                                                     |
| Step 3 | <b>crypto isakmp client configuration group</b> {group-name}<br><br><b>Example:</b><br>Router (config)# crypto isakmp client configuration group Group1 | Specifies to which group a policy profile will be defined and enters crypto ISAKMP group configuration mode.                                                                                                                                          |
| Step 4 | <b>configuration url</b> {url}<br><br><b>Example:</b><br>Router (config-isakmp-group)# configuration url http://10.10.88.8/easy.cfg                     | Specifies the URL the remote device must use to get the configuration from the server. <ul style="list-style-type: none"><li>The URL must be a non-NULL terminated ASCII string that specifies the complete path of the configuration file.</li></ul> |
| Step 5 | <b>configuration version</b> {version-number}<br><br><b>Example:</b><br>Router (config-isakmp-group)# configuration version 10                          | Specifies the version of the configuration. <ul style="list-style-type: none"><li>The version number will be an unsigned integer in the range 1 through 32767.</li></ul>                                                                              |

## Configuring Per User AAA Download with PKI—Configuring the Crypto PKI Trustpoint

To configure a AAA server to push user attributes to a remote device, perform the following steps.

### Prerequisites

Before configuring a AAA server to push user attributes to a remote device, you must have configured AAA. The crypto PKI trustpoint must also be configured (see the first configuration task below). It is preferable that the trustpoint configuration contain the **authorization username** command.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment url** *url*



5. **revocation-check none**
6. **rsakeypair** *key-label*
7. **authorization username** {**subjectname** *subjectname*}
8. **exit**

## DETAILED STEPS

|        | Command                                                                                                                                                                           | Purpose                                                                                                          |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                    | Enters global configuration mode.                                                                                |
| Step 3 | <b>crypto pki trustpoint</b> <i>name</i><br><br><b>Example:</b><br>Router (config)# crypto pki trustpoint<br>ca-server                                                            | Declares the trustpoint that your router should use and enters ca-trustpoint configuration mode.                 |
| Step 4 | <b>enrollment url</b> <i>url</i><br><br><b>Example:</b><br>Router (config-ca-trustpoint)# enrollment<br>url http://10.7.7.2:80                                                    | Specifies the URL of the certification authority (CA) server to which to send enrollment requests.               |
| Step 5 | <b>revocation-check none</b><br><br><b>Example:</b><br>Router (config-ca-trustpoint)#<br>revocation-check none                                                                    | Checks the revocation status of a certificate.                                                                   |
| Step 6 | <b>rsakeypair</b> <i>key-label</i><br><br><b>Example:</b><br>Router (config-ca-trustpoint)# rsakeypair<br>rsa-pair                                                                | Specifies which key pair to associate with the certificate.                                                      |
| Step 7 | <b>authorization username</b> { <b>subjectname</b> <i>subjectname</i> }<br><br><b>Example:</b><br>Router (config-ca-trustpoint)# authorization<br>username subjectname commonname | Specifies the parameters for the different certificate fields that are used to build the AAA username.           |
| Step 8 | <b>exit</b><br><br><b>Example:</b><br>Router (config-ca-trustpoint)# exit                                                                                                         | Exits ca-trustpoint configuration mode.                                                                          |

## Configuring the Actual Per User AAA Download with PKI

To configure the actual per-user download with PKI, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp policy** *priority*
4. **group** {1 | 2}
5. **exit**
6. **crypto isakmp profile** *profile-name*
7. **match certificate** *certificate-map*
8. **client pki authorization list** *listname*
9. **client configuration address** {*initiate* | *respond*}
10. **virtual-template** *template-number*
11. **exit**
12. **crypto ipsec transform-set** [*transform-set-name transform1*] [*transform2*] [*transform3*] [*transform4*]
13. **crypto ipsec profile** *name*
14. **set transform-set** *transform-set-name*

### DETAILED STEPS

|        | Command                                                                                                        | Purpose                                                                                                             |
|--------|----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                 | Enters global configuration mode.                                                                                   |
| Step 3 | <b>crypto isakmp policy</b> <i>priority</i><br><br><b>Example:</b><br>Router (config)# crypto isakmp policy 10 | Defines an IKE policy and enters ISAKMP policy configuration mode.                                                  |
| Step 4 | <b>group</b> {1   2}<br><br><b>Example:</b><br>Router (config-isakmp-policy)# group 2                          | Specifies the Diffie-Hellman group identifier within an IKE policy.                                                 |

|         | Command                                                                                                                                                                                                                           | Purpose                                                                                                                                                                |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5  | <b>exit</b><br><br><b>Example:</b><br>Router (config-isakmp-policy)# exit                                                                                                                                                         | Exits ISAKMP policy configuration mode.                                                                                                                                |
| Step 6  | <b>crypto isakmp profile</b> <i>profile-name</i><br><br><b>Example:</b><br>Router (config)# crypto isakmp profile<br>ISA-PROF                                                                                                     | Defines an ISAKMP profile and audits IPsec user sessions and enters crypto ISAKMP profile configuration mode.                                                          |
| Step 7  | <b>match certificate</b> <i>certificate-map</i><br><br><b>Example:</b><br>Router (config-isakmp-profile)# match<br>certificate cert_map                                                                                           | Assigns an ISAKMP profile to a peer on the basis of the contents of arbitrary fields in the certificate.                                                               |
| Step 8  | <b>client pki authorization list</b> <i>listname</i><br><br><b>Example:</b><br>Router (config-isakmp-profile)# client pki<br>authorization list usrgrp                                                                            | Specifies the authorization list of AAA servers that will be used for obtaining per-user AAA attributes on the basis of the username constructed from the certificate. |
| Step 9  | <b>client configuration address</b> { <b>initiate</b>   <b>respond</b> }<br><br><b>Example:</b><br>Router (config-isakmp-profile)# client<br>configuration address respond                                                        | Configures IKE configuration mode in the ISAKMP profile.                                                                                                               |
| Step 10 | <b>virtual-template</b> <i>template-number</i><br><br><b>Example:</b><br>Router(config-isakmp-profile)#<br>virtual-template 2                                                                                                     | Specifies which virtual template will be used to clone virtual access interfaces.                                                                                      |
| Step 11 | <b>exit</b><br><br><b>Example:</b><br>Router(config-isakmp-profile)# exit                                                                                                                                                         | Exits crypto ISAKMP profile configuration mode.                                                                                                                        |
| Step 12 | <b>crypto ipsec transform-set</b><br><i>transform-set-name transform1 [transform2]</i><br><i>[transform3] [transform4]</i><br><br><b>Example:</b><br>Router (config)# crypto ipsec transform-set<br>trans2 esp-3des esp-sha-hmac1 | Defines a transform set—an acceptable combination of security protocols and algorithms.                                                                                |

|         | Command                                                                                                                | Purpose                                                                                          |
|---------|------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Step 13 | <b>crypto ipsec profile</b> <i>name</i><br><br><b>Example:</b><br>Router (config)# crypto ipsec profile<br>IPSEC_PROF  | Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers. |
| Step 14 | <b>set transform-set</b> <i>transform-set-name</i><br><br><b>Example:</b><br>Router (config)# set transform-set trans2 | Specifies which transform sets can be used with the crypto map entry.                            |

## Configuring Per-User Attributes on a Local Easy VPN AAA Server

To configure per-user attributes on a local Easy VPN AAA server, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa attribute list** *list-name*
4. **attribute type** *name value* [**service** *service*] [**protocol** *protocol*]
5. **exit**
6. **crypto isakmp client configuration group** *group-name*
7. **crypto aaa attribute list** *list-name*

### DETAILED STEPS

|        | Command or Action                                                                                             | Purpose                                                                                                            |
|--------|---------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                        | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                | Enters global configuration mode.                                                                                  |
| Step 3 | <b>aaa attribute list</b> <i>list-name</i><br><br><b>Example:</b><br>Router(config)# aaa attribute list list1 | Defines a AAA attribute list locally on a router and enters attribute list configuration mode.                     |

|        | Command or Action                                                                                                                                                                   | Purpose                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Step 4 | <b>attribute type name value [service service] [protocol protocol]</b><br><br><b>Example:</b><br>Router(config-attr-list)# attribute type<br>attribute xxxx service ike protocol ip | Defines an attribute type that is to be added to an attribute list locally on a router.               |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-attr-list)# exit                                                                                                                | Exits attribute list configuration mode.                                                              |
| Step 6 | <b>crypto isakmp client configuration group group-name</b><br><br><b>Example:</b><br>Router (config)# crypto isakmp client<br>configuration group group1                            | Specifies to which group a policy profile will be defined and enters ISAKMP group configuration mode. |
| Step 7 | <b>crypto aaa attribute list list-name</b><br><br><b>Example:</b><br>Router (config-isakmp-group)# crypto aaa<br>attribute list listname1                                           | Defines a AAA attribute list locally on a router.                                                     |

## Enabling Easy VPN Syslog Messages

To enable Easy VPN syslog messages on a server, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto logging ezvpn group group-name**

### DETAILED STEPS

|        | Command                                                | Purpose                                                                                                            |
|--------|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |

|        | Command                                                               | Purpose                                                                                                                                                                                                                                                                                                                   |
|--------|-----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 2 | <b>configure terminal</b>                                             | Enters global configuration mode.                                                                                                                                                                                                                                                                                         |
|        | <b>Example:</b><br>Router# configure terminal                         |                                                                                                                                                                                                                                                                                                                           |
| Step 3 | <b>crypto logging ezvpn</b> [ <i>group group-name</i> ]               | Enables Easy VPN syslog messages on a server.                                                                                                                                                                                                                                                                             |
|        | <b>Example:</b><br>Router (config)# crypto logging ezvpn group group1 | <ul style="list-style-type: none"> <li>The <b>group</b> keyword and <i>group-name</i> argument are optional. If a group name is not provided, syslog messages are enabled for all Easy VPN connections to the server. If a group name is provided, syslog messages are enabled for that particular group only.</li> </ul> |

## Defining a CPP Firewall Policy Push Using a Local AAA Server

To define a CPP firewall policy push on a server to allow or deny a tunnel on the basis of whether a remote device has a required firewall for a local AAA server, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client firewall** {*policy-name*} {**required** | **optional**} {*firewall-type*}
4. **policy** {**check-presence** | **central-policy-push** {**access-list** {**in** | **out**} *access-list-name* | *access-list-number*}}

### DETAILED STEPS

|        | Command                                       | Purpose                                                                            |
|--------|-----------------------------------------------|------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                 | Enables privileged EXEC mode.                                                      |
|        | <b>Example:</b><br>Router> enable             | <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b>                     | Enters global configuration mode.                                                  |
|        | <b>Example:</b><br>Router# configure terminal |                                                                                    |

|        | Command                                                                                                                                                                                                                                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <p><b>crypto isakmp client firewall</b> {<i>policy-name</i>}<br/>{<b>required</b>   <b>optional</b>} {<i>firewall-type</i>}</p> <p><b>Example:</b><br/>Router (config)# crypto isakmp client<br/>firewall hw-client-g-cpp required<br/>Cisco-Security-Agent</p>                                                                                                             | <p>Defines the CPP firewall push policy on a server and enters ISAKMP client firewall configuration mode.</p> <p>The arguments and keywords are as follows:</p> <ul style="list-style-type: none"> <li>• <b>policy-name</b>—Uniquely identifies a policy. A policy name can be associated with the Easy VPN client group configuration of the server (local group configuration) or on the AAA server.</li> <li>• <b>required</b>—Policy is mandatory. If the CPP policy is defined as mandatory and is included in the Easy VPN server configuration, the tunnel setup is allowed only if the client confirms this policy. Otherwise, the tunnel is terminated.</li> <li>• <b>optional</b>—Policy is optional. If the CPP policy is defined as optional, and is included in the Easy VPN server configuration, the tunnel setup is continued even if the client does not confirm the defined policy.</li> <li>• <b>firewall-type</b>—Type of firewall (see the <b>crypto isakmp client firewall</b> command for a list of firewall types).</li> </ul> |
| Step 4 | <p><b>policy</b> {<b>check-presence</b>   <b>central-policy-push</b>}<br/>{<b>access-list</b> {<b>in</b>   <b>out</b>} <i>access-list-name</i>  <br/><i>access-list-number</i>}}</p> <p><b>Example:</b><br/>Router (config-ikmp-client-fw)# policy<br/>central-policy-push access-list out acl1</p> <p>or<br/>Router (config-ikmp-client-fw)# policy<br/>check-presence</p> | <p>Defines the CPP firewall policy push.</p> <p>The arguments and keywords are as follows:</p> <ul style="list-style-type: none"> <li>• <b>check-presence</b>—Denotes that the server should check for the presence of the specified firewall as shown by the value of the <i>firewall-type</i> argument on the client.</li> <li>• <b>central-policy-push</b>—The configuration following this keyword specifies the actual policy, such as the input and output access lists that have to be applied by the client firewall, which is of the type specified by the value of the <i>firewall-type</i> argument.</li> <li>• <b>access-list {in   out}</b>—Defines the inbound and outbound access lists.</li> <li>• <b>access-list-name   access-list-number</b>—Name or number of the access list.</li> </ul>                                                                                                                                                                                                                                          |

## What to Do Next

Apply the CPP firewall policy push to the configured group.

## Applying a CPP Firewall Policy Push to the Configuration Group

Now that the CPP firewall policy push has been defined, it must be applied to the configuration group by performing the following steps.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** {*group-name*}
4. **firewall policy** {*policy-name*}

## DETAILED STEPS

|        | Command                                                                                                                                                               | Purpose                                                                                                                             |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                 |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                        | Enters global configuration mode.                                                                                                   |
| Step 3 | <b>crypto isakmp client configuration group</b> { <i>group-name</i> }<br><br><b>Example:</b><br>Router (config)# crypto isakmp client configuration group hw-client-g | Specifies to which group a policy profile will be defined and enters ISAKMP group configuration mode.                               |
| Step 4 | <b>firewall policy</b> { <i>policy-name</i> }<br><br><b>Example:</b><br>Router (crypto-isakmp-group)# firewall policy hw-client-g-cpp                                 | Specifies the CPP firewall push policy name for the crypto ISAKMP client configuration group on a local authentication, AAA server. |

## Defining a CPP Firewall Policy Push Using a Remote AAA Server

To define a CPP firewall policy push using a remote AAA server, see the section “[Defining a CPP Firewall Policy Push Using a Local AAA Server](#).” The steps are the same for this configuration.

## What to Do Next

After defining the CPP firewall policy push, you should add the VSA cpp-policy under the group definition.

## Adding the VSA CPP-Policy Under the Group Definition

To add the the VSA cpp-policy under the group definition that is defined in RADIUS, perform the following step.



## SUMMARY STEPS

1. Add the VSA cpp-policy under the group definition that is defined in RADIUS.

## DETAILED STEPS

|        | Command                                                                                                                                         | Purpose                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| Step 1 | Add the VSA “cpp-policy” under the group definition that is defined in RADIUS.<br><br><b>Example:</b><br>ipsec:cpp-policy=”Enterprise Firewall” | Defines the CPP firewall push policy for a remote server. |

## Verifying CPP Firewall Policy Push

To verify the CPP firewall push policy on a local or remote AAA server, perform the following steps.

## SUMMARY STEPS

1. `enable`
2. `debug crypto isakmp`

## DETAILED STEPS

|        | Command                                                                                             | Purpose                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br>Router> <code>enable</code>                           | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <code>debug crypto isakmp</code><br><br><b>Example:</b><br>Router# <code>debug crypto isakmp</code> | Displays messages about IKE events.                                                                                   |

## Configuring Password Aging

To configure Password Aging so that the Easy VPN client is notified if the password has expired, perform the following steps.

## Restrictions

The following restrictions apply to the Password Aging feature:

- It works only with VPN software clients. It does not work with VPN client hardware.
- It works only with RADIUS servers.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login {list-name} password-expiry method1 [method2...]**
5. **radius-server host {ip-address} auth-port port-number acct-port port-number key string**
6. Configure the ISAKMP profile
7. **client authentication list {list-name}**

## DETAILED STEPS

|        | Command                                                                                                                                                                                                                                                               | Purpose                                                                                                             |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                        | Enters global configuration mode.                                                                                   |
| Step 3 | <b>aaa new-model</b><br><br><b>Example:</b><br>Router (config)# aaa new-model                                                                                                                                                                                         | Enables AAA.                                                                                                        |
| Step 4 | <b>aaa authentication login {list-name} password-expiry method1 [method2...]</b><br><br><b>Example:</b><br>Router (config)# aaa authentication login userauth paswd-expiry group radius                                                                               | Configures the authentication list so that the Password Aging feature is enabled.                                   |
| Step 5 | <b>radius-server host {ip-address} auth-port port-number acct-port port-number key string</b><br><br><b>Example:</b><br>Router (config)# radius-server host 172.19.217.96 255.255.255.0 auth-port 1645 acct-port 1646 key cisco radius-server vsa send authentication | Configures the RADIUS server.                                                                                       |

|        | Command                                                                                                                                           | Purpose                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6 | Configure the ISAKMP profile.<br><br><b>Example:</b><br>see the section “ <a href="#">Configuring Password Aging: Example</a> ”                   | Configures the ISAKMP profile and enters ISAKMP profile configuration mode (see the section “ <a href="#">Configuring Password Aging: Example</a> ”). |
| Step 7 | <code>client authentication list {list-name}</code><br><br><b>Example:</b><br>Router (config-isakmp-profile)# client authentication list userauth | Configures IKE extended authentication (Xauth) in an ISAKMP profile and includes the authentication list that was defined above.                      |

## Configuring Split DNS

To configure Split DNS, perform the following steps.

### Prerequisites

Before the Split DNS feature can work, the following commands should have been configured on the Easy VPN remote:

- `ip dns server`
- `ip domain-lookup`

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `crypto isakmp client configuration group group-name`
4. `dns primary-server secondary-server`
5. `split-dns domain-name`

### DETAILED STEPS

|        | Command                                                                              | Purpose                                                                                                             |
|--------|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                   |

|        | Command                                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                    |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>crypto isakmp client configuration group</b> <i>{group-name   default}</i><br><br><b>Example:</b><br>Router (config)# crypto isakmp client configuration group group1 | Specifies the policy profile of the group that will be defined and enters ISAKMP group configuration mode. <ul style="list-style-type: none"> <li>If no specific group matches and a default group is defined, users will automatically be given the policy of a default group.</li> </ul> |
| Step 4 | <b>dns primary-server secondary-server</b><br><br><b>Example:</b><br>Router (config-isakmp-group)# dns 10.2.2.2 10.3.3.3                                                 | Specifies the primary and secondary DNS servers for the group.                                                                                                                                                                                                                             |
| Step 5 | <b>split-dns domain-name</b><br><br><b>Example:</b><br>Router (config-isakmp-group)# split-dns green.com                                                                 | Specifies a domain name that must be tunneled or resolved to the private network.                                                                                                                                                                                                          |

## Verifying Split DNS

To verify a split DNS configuration, perform the following steps (the **show** commands can be used one at a time or together).

### SUMMARY STEPS

1. **enable**
2. **show ip dns name-list** *[name-list-number]*
3. **show ip dns view** *[vrf vrf-name] [default | view-name]*
4. **show ip dns view-list** *[view-list-name]*

### DETAILED STEPS

|        | Command                                                                                                          | Purpose                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                           | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>show ip dns name-list</b> <i>[name-list-number]</i><br><br><b>Example:</b><br>Router# show ip dns name-list 1 | Displays information about DNS name lists.                                                                       |

|        | Command                                                                                                                                                 | Purpose                                    |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
| Step 3 | <b>show ip dns view</b> [ <b>vrf</b> <i>vrf-name</i> ] [ <b>default</b>   <i>view-name</i> ]<br><br><b>Example:</b><br>Router# show ip dns view default | Displays information about DNS views.      |
| Step 4 | <b>show ip dns view-list</b> [ <i>view-list-name</i> ]<br><br><b>Example:</b><br>Router# show ip dns view-list<br>ezvpn-internal-viewlist               | Displays information about DNS view lists. |

## Monitoring and Maintaining Split DNS

To monitor and maintain the split DNS configuration on Easy VPN remote devices, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **debug ip dns name-list**
3. **debug ip dns view**
4. **debug ip dns view-list**

### DETAILED STEPS

|        |                                                                                        |                                                                                                                    |
|--------|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>debug ip dns name-list</b><br><br><b>Example:</b><br>Router# debug ip dns name-list | Enables debugging output for Domain Name System (DNS) name-list events.                                            |
| Step 3 | <b>debug ip dns view</b><br><br><b>Example:</b><br>Router# debug ip dns view           | Enables debugging output for DNS view events.                                                                      |
| Step 4 | <b>debug ip dns view-list</b><br><br><b>Example:</b><br>Router# debug ip dns view-list | Enables debugging output for DNS view-list events.                                                                 |

## Configuring an Easy VPN Server to Obtain an IP Address from a DHCP Server

When the Easy VPN server selects the method for address assignment, it does so in the following order of precedence:

1. Selects the Framed IP address
2. Uses the IP address from the authentication server (group/user)
3. Uses the global IKE address pools
4. Uses DHCP



### Note

To enable the Easy VPN server to obtain an IP address from a DHCP server, remove other address assignments.

To configure an Easy VPN server to obtain an IP address from a DHCP server, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** *group-name*
4. **dhcp server** {*ip-address* | *hostname*}
5. **dhcp timeout** *time*
6. **dhcp giaddr** *scope*

### DETAILED STEPS

|                                                                                                              |                                                                   |                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b><br><br><br><b>Example:</b><br>Router> enable                                                   | <b>enable</b>                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                |
| <b>Step 2</b><br><br><br><b>Example:</b><br>Router# configure terminal                                       | <b>configure terminal</b>                                         | Enters global configuration mode.                                                                                                                                                                                                               |
| <b>Step 3</b><br><br><br><b>Example:</b><br>Router (config)# crypto isakmp client configuration group group1 | <b>crypto isakmp client configuration group</b> <i>group-name</i> | Specifies to which group a policy profile will be defined. <p><b>Note</b> Entering this command places the CLI in ISAKMP group configuration mode. From this mode, you can use subcommands to specify characteristics for the group policy.</p> |
| <b>Step 4</b><br><br><br><b>Example:</b><br>Router (config-isakmp-group)# dhcp server 10.10.1.2              | <b>dhcp server</b> { <i>ip-address</i>   <i>hostname</i> }        | Specifies a primary (and backup) DHCP server to allocate IP addresses to MS users entering a particular public data network (PDN) access point.                                                                                                 |

|               |                                                                                                              |                                                                                 |
|---------------|--------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <b>Step 5</b> | <b>dhcp timeout</b> <i>time</i><br><br><b>Example:</b><br>Router (config-isakmp-group)# dhcp timeout 6       | Sets the wait time in seconds before the next DHCP server on the list is tried. |
| <b>Step 6</b> | <b>dhcp giaddr</b> <i>scope</i><br><br><b>Example:</b><br>Router (config-isakmp-group)# dhcp giaddr 10.1.1.4 | Specifies the giaddr for the DHCP scope.                                        |

## Verifying DHCP Client Proxy

To verify your DHCP client proxy configuration, perform the following steps (use the **show** commands one at a time or together).

### SUMMARY STEPS

1. **enable**
2. **show dhcp lease**
3. **show ip dhcp pool**
4. **show ip dhcp binding**

### DETAILED STEPS

|               |                                                                                    |                                                                                                                                                                                                                                               |
|---------------|------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> enable                             | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                            |
| <b>Step 1</b> | <b>show dhcp lease</b><br><br><b>Example:</b><br>Router# show dhcp lease           | Displays information about the DHCP address pools.<br><br><b>Note</b> Use this command when an external DHCP is used.                                                                                                                         |
| <b>Step 2</b> | <b>show ip dhcp pool</b><br><br><b>Example:</b><br>Router# show ip dhcp pool       | Displays information about the DHCP address pools.<br><br><b>Note</b> This command is applicable only when the Easy VPN server is also the DHCP server (generally not the case because in most cases, the DHCP server is an external server). |
| <b>Step 3</b> | <b>show ip dhcp binding</b><br><br><b>Example:</b><br>Router# show ip dhcp binding | Displays address bindings on the DHCP server.<br><br><b>Note</b> This command is applicable only when the Easy VPN server is also the DHCP server (generally not the case because in most cases, the DHCP server is an external server).      |

## Monitoring and Maintaining DHCP Client Proxy

To monitor and maintain your DHCP client proxy configuration, perform the following steps (use the **debug** commands one at a time or together).

### SUMMARY STEPS

1. **enable**
2. **debug crypto isakmp**
3. **debug dhcp**
4. **debug dhcp detail**
5. **debug ip dhcp server events**

### DETAILED STEPS

|        |                                                                                                  |                                                                                                                                                                                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                           | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                 |
| Step 2 | <b>debug crypto isakmp</b><br><br><b>Example:</b><br>Router# debug crypto isakmp                 | Displays messages about Internet Key Exchange (IKE) event.                                                                                                                                                                                                       |
| Step 3 | <b>debug dhcp</b><br><br><b>Example:</b><br>Router# debug dhcp                                   | Reports server events, like address assignments and database updates.                                                                                                                                                                                            |
| Step 4 | <b>debug dhcp detail</b><br><br><b>Example:</b><br>Router# debug dhcp detail                     | Displays detailed DHCP debugging information.                                                                                                                                                                                                                    |
| Step 5 | <b>debug ip dhcp server events</b><br><br><b>Example:</b><br>Router# debug ip dhcp server events | Reports server events, like address assignments and database updates.<br><br><b>Note</b> This command is applicable only when the Easy VPN server is also the DHCP server (generally not the case because in most cases, the DHCP server is an external server). |

## Configuring cTCP

To enable cTCP, perform the following steps on your Easy VPN server.

### Prerequisites

Before configuring cTCP, you should have configured crypto IPsec.



## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ctcp port** [*port-number*]

## DETAILED STEPS

|               |                                                                                                                |                                                                                                                                                                                                                                               |
|---------------|----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                         | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                              |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                 | Enters global configuration mode.                                                                                                                                                                                                             |
| <b>Step 3</b> | <b>crypto ctcp port</b> [ <i>port-number</i> ]<br><br><b>Example:</b><br>Router (config)# crypto ctcp port 120 | Configures cTCP encapsulation for Easy VPN. <ul style="list-style-type: none"><li>• Up to 10 port numbers can be configured.</li><li>• If the <i>port-number</i> argument is not configured, cTCP is enabled on port 80 by default.</li></ul> |

## Verifying cTCP

To verify your cTCP configuration, perform the following steps (the **show** commands can be used one at a time or together).

## SUMMARY STEPS

1. **enable**
2. **show crypto ctcp** [*peer ip-address*]

## DETAILED STEPS

|               |                                                                                                                         |                                                                                                                  |
|---------------|-------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                  | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| <b>Step 2</b> | <b>show crypto ctcp</b> [ <i>peer ip-address</i> ]<br><br><b>Example:</b><br>Router# show crypto ctcp peer 10.76.235.21 | Displays information about a specific cTCP peer.                                                                 |

## Monitoring and Maintaining a cTCP Configuration

To monitor and maintain your cTCP configuration, perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **debug crypto ctcp**

## DETAILED STEPS

|                                                                           |                          |                                                                                                                  |
|---------------------------------------------------------------------------|--------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b><br><br><br><br><b>Example:</b><br>Router> enable            | <b>enable</b>            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| <b>Step 2</b><br><br><br><br><b>Example:</b><br>Router# debug crypto ctcp | <b>debug crypto ctcp</b> | Displays information about a cTCP session.                                                                       |

## Clearing a cTCP Configuration

To clear a cTCP configuration, perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **clear crypto ctcp [peer *ip-address*]**

## DETAILED STEPS

|                                                                                            |                                                   |                                                                                                                  |
|--------------------------------------------------------------------------------------------|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b><br><br><br><br><b>Example:</b><br>Router> enable                             | <b>enable</b>                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| <b>Step 2</b><br><br><br><br><b>Example:</b><br>Router# clear crypto ctcp peer 10.76.23.21 | <b>clear crypto ctcp [peer <i>ip-address</i>]</b> | Displays information about a cTCP session.                                                                       |

## Troubleshooting a cTCP Configuration

To troubleshoot a cTCP configuration, perform the following steps.

### SUMMARY STEPS

1. Ensure that the cTCP session is in the CTCP\_ACK\_RECEIVED state.
2. If the cTCP session is not in the CTCP\_ACK\_RECEIVED state, enable the **debug crypto ctcp** command.
3. If no cTCP bugs are seen, ensure that the firewall is allowing the cTCP packets to get to the server.
4. If the firewall configuration is correct, debugging is enabled, and you do not see any cTCP debugs on your console, you must find out why the cTCP port on the router is not receiving packets.

### DETAILED STEPS

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | To ensure that the cTCP session is in the CTCP_ACK_RECEIVED state, use the <b>show crypto ctcp</b> command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Step 2</b> | If the cTCP session is not in the CTCP_ACK_RECEIVED state, enable the <b>debug crypto ctcp</b> command and then try using the <b>show crypto ctcp</b> command again.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 3</b> | If no cTCP bugs are seen, ensure that the firewall is allowing the cTCP packets to get to the server (check the firewall configuration).                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Step 4</b> | If the firewall configuration is correct, debugging is enabled, and you do not see any cTCP debugs on your console, you must find out why the cTCP port on the router is not receiving packets. If you do not see any cTCP debugs and a cTCP session has not been set up, there is a possibility that cTCP packets that are actually TCP packets could have been delivered to a TCP stack instead of to the cTCP port. By enabling the <b>debug ip packet</b> and <b>debug ip tcp packet</b> commands, you may be able to determine whether the packet is being given to the TCP stack. |
- 

## Configuration Examples for Easy VPN Server

This section provides the following configuration examples:

- [Configuring Cisco IOS for Easy VPN Server: Example, page 54](#)
- [RADIUS Group Profile with IPsec AV Pairs: Example, page 55](#)
- [RADIUS User Profile with IPsec AV Pairs: Example, page 56](#)
- [Backup Gateway with Maximum Logins and Maximum Users: Example, page 56](#)
- [Easy VPN with an IPsec Virtual Tunnel Interface: Example, page 56](#)
- [Pushing a Configuration URL Through a Mode-Configuration Exchange: Examples, page 58](#)
- [Per User AAA Policy Download with PKI: Example, page 58](#)
- [Per-User Attributes on an Easy VPN Server: Example, page 62](#)
- [Network Admission Control: Example, page 64](#)
- [Configuring Password Aging: Example, page 66](#)

- [Split DNS: Examples, page 68](#)
- [DHCP Client Proxy: Examples, page 69](#)
- [cTCP Session: Example, page 70](#)

## Configuring Cisco IOS for Easy VPN Server: Example

The following example shows how to define group policy information locally for mode configuration. In this example, a group name is named “cisco” and another group name is named “default.” The policy is enforced for all users who do not offer a group name that matches “cisco.”

```
! Enable policy look-up via AAA. For authentication and authorization, send requests to
! RADIUS first, then try local policy.
aaa new-model
aaa authentication login userlist group radius local
aaa authorization network grouplist group radius local
enable password XXXX
!
username cisco password 0 cisco
clock timezone PST -8
ip subnet-zero
! Configure IKE policies, which are assessed in order so that the first policy that
! matches the proposal of the client will be used.
crypto isakmp policy 1
 group 2
!
crypto isakmp policy 3
 hash md5
 authentication pre-share
 group 2
crypto isakmp identity hostname
!
! Define “cisco” group policy information for mode config push.
crypto isakmp client configuration group cisco
 key cisco
 dns 10.2.2.2 10.2.2.3
 wins 10.6.6.6
 domain cisco.com
 pool green
 acl 199
! Define default group policy for mode config push.
crypto isakmp client configuration group default
 key cisco
 dns 10.2.2.2 10.3.2.3
 pool green
 acl 199
!
!
crypto ipsec transform-set dessha esp-des esp-sha-hmac
!
crypto dynamic-map mode 1
 set transform-set dessha
!
! Apply mode config and xauth to crypto map “mode.” The list names that are defined here
! must match the list names that are defined in the AAA section of the config.
crypto map mode client authentication list userlist
crypto map mode isakmp authorization list grouplist
crypto map mode client configuration address respond
crypto map mode 1 ipsec-isakmp dynamic mode
!
!
```

```

controller ISA 1/1
!
!
interface FastEthernet0/0
 ip address 10.6.1.8 255.255.0.0
 ip route-cache
 ip mroute-cache
 duplex auto
 speed auto
 crypto map mode
!
interface FastEthernet0/1
 ip address 192.168.1.28 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 duplex auto
 speed auto
! Specify IP address pools for internal IP address allocation to clients.
 ip local pool green 192.168.2.1 192.168.2.10
 ip classless
 ip route 0.0.0.0 0.0.0.0 10.6.0.1
!
! Define access lists for each subnet that should be protected.
 access-list 199 permit ip 192.168.1.0 0.0.0.255 any
 access-list 199 permit ip 192.168.3.0 0.0.0.255 any
!
! Specify a RADIUS server host and configure access to the server.
 radius-server host 192.168.1.1 auth-port 1645 acct-port 1646 key XXXXX
 radius-server retransmit 3
!
!
line con 0
 exec-timeout 0 0
 length 25
 transport input none
line aux 0
line vty 5 15
!

```

## RADIUS Group Profile with IPsec AV Pairs: Example

The following is an example of a standard RADIUS group profile that includes RADIUS IPsec AV pairs. To get the group authorization attributes, “cisco” must be used as the password.

```

client_r Password = "cisco"
Service-Type = Outbound

cisco-avpair = "ipsec:tunnel-type*ESP"
cisco-avpair = "ipsec:key-exchange=ike"
cisco-avpair = "ipsec:tunnel-password=lab"
cisco-avpair = "ipsec:addr-pool=pool1"
cisco-avpair = "ipsec:default-domain=cisco"
cisco-avpair = "ipsec:inac1=101"
cisco-avpair = "ipsec:access-restrict=fastethernet 0/0"
cisco-avpair = "ipsec:group-lock=1"
cisco-avpair = "ipsec:dns-servers=10.1.1.1 10.2.2.2"
cisco-avpair = "ipsec:firewall=1"
cisco-avpair = "ipsec:include-local-lan=1"
cisco-avpair = "ipsec:save-password=1"
cisco-avpair = "ipsec:wins-servers=10.3.3.3 10.4.4.4"
cisco-avpair = "ipsec:split-dns=green.com"
cisc-avpair = "ipsec:ipsec-backup-gateway=10.1.1.1"

```

```

ciscoc-vpair = "ipsec:ipsec-backup-gateway=10.1.1.2"
ciscoc-vpair = "ipsec:pfs=1"
ciscoc-vpair = "ipsec:cpp-policy="Enterprise Firewall"
ciscoc-vpair = "ipsec:auto-update="Win http://abc.com 4.0.1"
ciscoc-vpair = "ipsec:browser-proxy=bproxy_profile_A"
ciscoc-vpair = "ipsec:xauth-banner="Xauth banner text here"

```

## RADIUS User Profile with IPsec AV Pairs: Example

The following is an example of a standard RADIUS user profile that includes RADIUS IPsec AV pairs. These user attributes will be obtained during Xauth.

```

ualluall Password = "uall1234"
 cisco-vpair = "ipsec:user-vpn-group=unity"
 cisco-vpair = "ipsec:user-include-local-lan=1"
 cisco-vpair = "ipsec:user-save-password=1"
 Framed-IP-Address = 10.10.10.10

```

## Backup Gateway with Maximum Logins and Maximum Users: Example

The following example shows that five backup gateways have been configured, that the maximum users have been set to 250, and that maximum logins have been set to 2:

```

crypto isakmp client configuration group sdm
 key 6 RMZPPMRQMSdiZNJg`EBbCWTkSTi\d[
 pool POOL1
 acl 150
 backup-gateway 172.16.12.12
 backup-gateway 172.16.12.13
 backup-gateway 172.16.12.14
 backup-gateway 172.16.12.130
 backup-gateway 172.16.12.131
 max-users 250
 max-logins 2

```

## Easy VPN with an IPsec Virtual Tunnel Interface: Example

The following output shows that Easy VPN has been configured with an IPsec virtual tunnel interface.

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization network default local
!

```

```
aaa session-id common
!
resource policy
!
clock timezone IST 0
ip subnet-zero
ip cef
no ip domain lookup
no ip dhcp use vrf connected
!
username lab password 0 lab
!
crypto isakmp policy 3
 authentication pre-share
 group 2
crypto isakmp xauth timeout 90

!
crypto isakmp client configuration group easy
 key cisco
 domain foo.com
 pool dpool
 acl 101
crypto isakmp profile vi
 match identity group easy
 isakmp authorization list default
 client configuration address respond
 client configuration group easy
 virtual-template 1
!
!
crypto ipsec transform-set set esp-3des esp-sha-hmac
!
crypto ipsec profile vi
 set transform-set set
 set isakmp-profile vi
!
!
interface Loopback0
 ip address 10.4.0.1 255.255.255.0
!
interface Ethernet0/0
 ip address 10.3.0.2 255.255.255.0
 no keepalive
 no cdp enable
interface Ethernet1/0
 no ip address
 no keepalive
 no cdp enable
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi
!
ip local pool dpool 10.5.0.1 10.5.0.10
!
ip classless
ip route 10.2.0.0 255.255.255.0 10.3.0.1
no ip http server
no ip http secure-server
!
!
access-list 101 permit ip 10.4.0.0 0.0.0.255 any
```

```

no cdp run
!
!
line con 0
line aux 0
line vty 0 4
!
end

```

## Pushing a Configuration URL Through a Mode-Configuration Exchange: Examples

The following **show crypto ipsec client ezvpn** command output displays the mode configuration URL location and version:

```
Router# show crypto ipsec client ezvpn
```

```

Easy VPN Remote Phase: 5

Tunnel name : branch
Inside interface list: Vlan1
Outside interface: FastEthernet0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 172.16.1.209
Mask: 255.255.255.255
Default Domain: cisco.com
Save Password: Allowed
Configuration URL [version]: tftp://172.16.30.2/branch.cfg [11]
Config status: applied, Last successfully applied version: 11
Current EzVPN Peer: 192.168.10.1

```

The following **show crypto isakmp peers config** command output displays all manageability information that is sent by the remote device.

```
Router# show crypto isakmp peers config
```

```

Client-Public-Addr=192.168.10.2:500; Client-Assigned-Addr=172.16.1.209;
Client-Group=branch; Client-User=branch; Client-Hostname=branch.; Client-Platform=Cisco
1711; Client-Serial=FOC080210E2 (412454448); Client-Config-Version=11;
Client-Flash=33292284; Client-Available-Flash=10202680; Client-Memory=95969280;
Client-Free-Memory=14992140; Client-Image=flash:c1700-advipservicesk9-mz.ef90241;
Client-Public-Addr=192.168.10.3:500; Client-Assigned-Addr=172.16.1.121;
Client-Group=store; Client-User=store; Client-Hostname=831-storerouter.;
Client-Platform=Cisco C831; Client-Serial=FOC08472UXR (1908379618);
Client-Config-Version=2; Client-Flash=24903676; Client-Available-Flash=5875028;
Client-Memory=45298688; Client-Free-Memory=6295596;
Client-Image=flash:c831-k9o3y6-mz.ef90241

```

## Per User AAA Policy Download with PKI: Example

The following output shows that the Per User AAA Policy Download with PKI feature has been configured on the Easy VPN server.

```
Router# show running-config
```

```
Building configuration...
```

```
Current configuration : 7040 bytes
```



```

!
! Last configuration change at 21:06:51 UTC Tue Jun 28 2005
!
version 12.4
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname GEN
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa group server radius usrgppki
 server 10.76.248.201 auth-port 1645 acct-port 1646
!
aaa authentication login xauth group usrgppki
aaa authentication login usrgp group usrgppki
aaa authorization network usrgp group usrgppki
!
aaa session-id common
!
resource policy
!
ip subnet-zero
!
!
ip cef
!
!
ip address-pool local
!
!
crypto pki trustpoint ca-server
 enrollment url http://10.7.7.2:80
 revocation-check none
 rsa-keypair rsa-pair
 ! Specify the field within the certificate that will be used as a username to do a
 per-user AAA lookup into the RADIUS database. In this example, the contents of the
 commonname will be used to do a AAA lookup. In the absence of this statement, by default
 the contents of the "unstructured name" field in the certificate is used for AAA lookup.
 authorization username subjectname commonname
!
!
crypto pki certificate map CERT-MAP 1
 subject-name co yourname
 name co yourname
!
crypto pki certificate chain ca-server
 certificate 02
 308201EE 30820157 A0030201 02020102 300D0609 2A864886 F70D0101 04050030
 14311230 10060355 04031309 63612D73 65727665 72301E17 0D303530 36323832
 30303731 345A170D 30363036 32383230 30373134 5A301531 13301106 092A8648
 86F70D01 09021604 47454E2E 30819F30 0D06092A 864886F7 0D010101 05000381
 8D003081 89028181 00ABF8F0 FDFDF8D F22098D6 A48EE0C3 F505DD96 C0022EA4
 EAB95EE8 1F97F450 990BB0E6 F2B7151F C5C79391 93822FE4 DEE5B00C A03412BB
 9B715AAD D6C31F93 D8802658 AF9A8866 63811942 913D0C02 C3E328CC 1C046E94
 F73B7C1A 4497F86E 74A627BC B809A3ED 293C15F2 8DCFA217 5160F9A4 09D52044
 350F85AF 08B357F5 D7020301 0001A34F 304D300B 0603551D 0F040403 0205A030

```

```

1F060355 1D230418 30168014 F9BC4498 3DA4D51D 451EFEFD 5B1F5F73 8D7B1C9B
301D0603 551D0E04 1604146B F6B2DFD1 1FE237FF 23294129 E55D9C48 CCB04630
0D06092A 864886F7 0D010104 05000381 81004AFF 2BE300C1 15D0B191 C20D06E0
260305A6 9DF610BB 24211516 5AE73B62 78E01FE4 0785776D 3ADFA3E2 CE064432
1C93E82D 93B5F2AB 9661EDD3 499C49A8 F87CA553 9132F239 1D50187D 21CC3148
681F5043 2F2685BC F544F4FF 8DF535CB E55B5F36 31FFF025 8969D9F8 418C8AB7
C569B022 46C3C63A 22DD6516 C503D6C8 3D81
quit
certificate ca 01
30820201 3082016A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
14311230 10060355 04031309 63612D73 65727665 72301E17 0D303530 36323832
30303535 375A170D 30383036 32373230 30353537 5A301431 12301006 03550403
13096361 2D736572 76657230 819F300D 06092A86 4886F70D 01010105 0003818D
00308189 02818100 BA1A4413 96339C6B D36BD720 D25C9A44 E0627A29 97E06F2A
69B268ED 08C7144E 7058948D BEA512D4 40588B87 322C5D79 689427CA 5C54B3BA
82FAEC53 F6AC0B5C 615D032C 910CA203 AC6AB681 290D9EED D31EB185 8D98E1E7
FF73613C 32290FD6 A0CBDC40 6E4D6B39 DE1D86BA DE77A55E F15299FF 97D7C185
919F81C1 30027E0F 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D 23041830 168014F9
BC44983D A4D51D45 1EFEFD5B 1F5F738D 7B1C9B30 1D060355 1D0E0416 0414F9BC
44983DA4 D51D451E FEFD5B1F 5F738D7B 1C9B300D 06092A86 4886F70D 01010405
00038181 003EF397 F4D98BDE A4322FAF 4737800F 1671F77E BD6C45AE FB91B28C
F04C98F0 135A40C6 635FDC29 63C73373 5D5BBC9A F1BBD235 F66CE1AD 6B4BFC7A
AB18C8CC 1AB93AF3 7AC67436 930E9C81 F43F7570 A8FE09AE 3DEA01D1 DA6BD0CB
83F9A77F 1DFAFE5E 2F1F206B F1FDD8BE 6BB57A3C 8D03115D B1F64A3F 7A7557C1
09B0A34A DB
quit
!
!
crypto isakmp policy 10
group 2
crypto isakmp keepalive 10
crypto isakmp profile ISA-PROF
match certificate CERT-MAP
isakmp authorization list usrgrp
client pki authorization list usrgrp
client configuration address respond
client configuration group pkuser
virtual-template 2
!
!
crypto ipsec transform-set trans2 esp-3des esp-sha-hmac
!
crypto ipsec profile IPSEC_PROF
set transform-set trans2
!
crypto ipsec profile ISC_IPSEC_PROFILE_1
set transform-set trans2
!
!
crypto call admission limit ike sa 40
!
!
interface Loopback0
ip address 10.3.0.1 255.255.255.255
no ip route-cache cef
no ip route-cache
!
interface Loopback1
ip address 10.76.0.1 255.255.255.255
no ip route-cache cef
no ip route-cache
!
interface Ethernet3/0

```

```
ip address 10.76.248.209 255.255.255.255
no ip route-cache cef
no ip route-cache
duplex half
!
!
interface Ethernet3/2
ip address 10.2.0.1 255.255.255.0
no ip route-cache cef
no ip route-cache
duplex half
!
!
interface Serial4/0
no ip address
no ip route-cache cef
no ip route-cache
shutdown
serial restart-delay 0
!
interface Serial4/1
no ip address
no ip route-cache cef
no ip route-cache
shutdown
serial restart-delay 0
!
interface Serial4/2
no ip address
no ip route-cache cef
no ip route-cache
shutdown
serial restart-delay 0
!
interface Serial4/3
no ip address
no ip route-cache cef
no ip route-cache
shutdown
serial restart-delay 0
!
interface FastEthernet5/0
ip address 10.9.4.77 255.255.255.255
no ip route-cache cef
no ip route-cache
duplex half
!
interface FastEthernet6/0
ip address 10.7.7.1 255.255.255.0
no ip route-cache cef
no ip route-cache
duplex full
!
interface Virtual-Template1
no ip address
!
interface Virtual-Template2 type tunnel
ip unnumbered Loopback0
tunnel source Ethernet3/2
tunnel mode ipsec ipv4
tunnel protection ipsec profile IPSEC_PROF
!
router eigrp 20
network 172.16.0.0
```

```

 auto-summary
 !
ip local pool ourpool 10.6.6.6
ip default-gateway 10.9.4.1
ip classless
ip route 10.1.0.1 255.255.255.255 10.0.0.2
ip route 10.2.3.0 255.255.0.0 10.2.4.4
ip route 10.9.1.0 255.255.0.0 10.4.0.1
ip route 10.76.0.0 255.255.0.0 10.76.248.129
ip route 10.11.1.1 255.255.255.0 10.7.7.2
 !
no ip http server
no ip http secure-server
 !
 !
logging alarm informational
arp 10.9.4.1 0011.bcb4.d40a ARPA
 !
 !
radius-server host 10.76.248.201 auth-port 1645 acct-port 1646 key cisco
 !
control-plane
 !
 !
gatekeeper
shutdown
 !
 !
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 !
 !
end

```

## Per-User Attributes on an Easy VPN Server: Example

The following example shows that per-user attributes have been configured on an Easy VPN server.

```

!

aaa new-model
!
!
aaa authentication login default local
aaa authentication login noAAA none
aaa authorization network default local
!
aaa attribute list per-group
 attribute type inacl "per-group-acl" service ike protocol ip mandatory
!
aaa session-id common
!
resource policy
!
ip subnet-zero
!
!
ip cef
!

```

```
!
username example password 0 example
!
!
crypto isakmp policy 3
 authentication pre-share
 group 2
crypto isakmp xauth timeout 90
!
crypto isakmp client configuration group PerUserAAA
 key cisco
 pool dpool
 crypto aaa attribute list per-group
!
crypto isakmp profile vi
 match identity group PerUserAAA
 isakmp authorization list default
 client configuration address respond
 client configuration group PerUserAAA
 virtual-template 1
!
!
crypto ipsec transform-set set esp-3des esp-sha-hmac
!
crypto ipsec profile vi
 set transform-set set
 set isakmp-profile vi
!
!
interface GigabitEthernet0/0
 description 'EzVPN Peer'
 ip address 192.168.1.1 255.255.255.128
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto

interface Virtual-Template1 type tunnel
 ip unnumbered GigabitEthernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi
!
ip local pool dpool 10.5.0.1 10.5.0.10
ip classless
!
no ip http server
no ip http secure-server
!
!
ip access-list extended per-group-acl
 permit tcp any any
 deny icmp any any
logging alarm informational
logging trap debugging
!
control-plane
```

```

!
gatekeeper
 shutdown
!
line con 0
line aux 0
 stopbits 1
line vty 0 4
!
!
end

```

## Network Admission Control: Example

The following is output for an Easy VPN server that has been enabled with Network Admission Control.



### Note

Network Admission Control is supported on an Easy VPN server only when the server uses IPsec virtual interfaces. Network Admission Control is enabled on the virtual template interface and applies to all PC clients that use this virtual template interface.

```
Router# show running-config
```

```
Building configuration...
```

```
Current configuration : 5091 bytes
```

```

!
version 12.4
!
hostname Router
!

```

```
aaa new-model
```

```

!
!
aaa authentication login userlist local
!

```

```

aaa authentication eou default group radius
aaa authorization network hw-client-groupname local
aaa accounting update newinfo
aaa accounting network acclist start-stop broadcast group radius
aaa session-id common
!

```

```

! Note 1: EAPoUDP packets will use the IP address of the loopback interface when sending
the EAPoUDP hello to the Easy VPN client. Using the IP address ensures that the returning
EAPoUDP packets come back encrypted and are associated with the correct virtual access
interface. The ip admission (ip admission source-interface Loopback10) command is
optional. Instead of using this command, you can specify the IP address of the virtual
template to be an address in the inside network space as shown in the configuration of the
virtual template below in Note 2.

```

```

ip admission source-interface Loopback10
ip admission name test eapoudp inactivity-time 60
!
!
eou clientless username cisco
eou clientless password cisco
eou allow ip-station-id
eou logging
!

```

```

username lab password 0 lab
username lab@easy password 0 lab
!
!
crypto isakmp policy 3
 encr 3des
 authentication pre-share
 group 2
!
!
crypto isakmp key 0 cisco address 10.53.0.1
crypto isakmp client configuration group easy
 key cisco
 domain cisco.com
 pool dynpool
 acl split-acl
 group-lock
 configuration url tftp://10.13.0.9/Config-URL_TFTP.cfg
 configuration version 111
!
crypto isakmp profile vi
 match identity group easy
 client authentication list userlist
 isakmp authorization list hw-client-groupname
 client configuration address respond
 client configuration group easy
 accounting acclist
 virtual-template 2
!
crypto ipsec security-association lifetime seconds 120
crypto ipsec transform-set set esp-3des esp-sha-hmac
crypto ipsec transform-set aes-trans esp-aes esp-sha-hmac
crypto ipsec transform-set transform-1 esp-des esp-sha-hmac
crypto ipsec profile vi
 set security-association lifetime seconds 3600
 set transform-set set aes-trans transform-1
 set isakmp-profile vi
!
!
crypto dynamic-map dynmap 1
 set transform-set aes-trans transform-1
 reverse-route
!

interface Loopback10
 ip address 10.61.0.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 10.13.11.173 255.255.255.255
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.55.0.1 255.255.255.255
 duplex auto
 speed auto
!
!
interface Virtual-Template2 type tunnel
! Note2: Use the IP address of the loopback10. This ensures that the EAPoUDP packets that
are attached to virtual-access interfaces that are cloned from this virtual template carry
the source address of the loopback address and that response packets from the VPN client
come back encrypted.
!

```

```

ip unnumbered Loopback10
! Enable Network Admission Control for remote VPN clients.
ip admission test
tunnel mode ipsec ipv4
tunnel protection ipsec profile vi
!
!
ip local pool dynpool 172.16.2.65 172.16.2.70
ip classless
ip access-list extended ClientException
 permit ip any host 10.61.0.1
ip access-list extended split-acl
 permit ip host 10.13.11.185 any
 permit ip 10.61.0.0 255.255.255.255 any
 permit ip 10.71.0.0 255.255.255.255 any
 permit ip 10.71.0.0 255.255.255.255 10.52.0.0 0.255.255.255
 permit ip 10.55.0.0 255.255.255.255 any
!
ip radius source-interface FastEthernet0/0
access-list 102 permit esp any any
access-list 102 permit ahp any any
access-list 102 permit udp any any eq 21862
access-list 102 permit ospf any any
access-list 102 deny ip any any
access-list 195 deny ospf any any
access-list 195 permit ip 10.61.0.0 255.255.255.255 10.51.0.0 255.255.255.255
!
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server host 10.13.11.185 auth-port 1645 acct-port 1646 key cisco
radius-server vsa send accounting
radius-server vsa send authentication
!
end

```

## Configuring Password Aging: Example

The following example shows that password aging has been configured so that if the password expires, the Easy VPN client is notified.

```

Current configuration : 4455 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname xinl-gateway
!
boot-start-marker
boot system flash c2800nm-advsecurityk9-mz.124-7.9.T
boot-end-marker
!
!
aaa new-model
!
!
aaa authentication login USERAUTH passwd-expiry group radius aaa authorization network
branch local !
aaa session-id common
!

```



```
ip cef

username cisco privilege 15 secret 5 1A3HU$bCWj1krEztDJx6JJzSnMV1 !
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp client configuration address-pool local dynpool !
crypto isakmp client configuration group branch
 key cisco
 domain cisco.com
 pool dynpool
!
!
crypto ipsec transform-set transform-1 esp-3des esp-sha-hmac !
crypto isakmp profile profile2
 client authentication list USERAUTH
 match identity group branch
 isakmp authorization list branch
 client configuration address respond
 virtual-template 1

crypto ipsec profile vi
 set transform-set transform-1

interface GigabitEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
 ip address 192.168.1.100 255.255.255.0
 duplex auto
 speed auto
 crypto map dynmap
!
interface GigabitEthernet0/1
 description ES_LAN
 ip address 172.19.217.96 255.255.255.0
 duplex auto
 speed auto

!
!interface Virtual-Templat1 type tunnel
 ip unnumbered Ethernet0/0
 no clns route-cache
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi
!
ip local pool dpool 10.0.0.1 10.0.0.3

!
radius-server host 172.19.220.149 auth-port 1645 acct-port 1646 key cisco radius-server
vsa send authentication !
control-plane
!
!
end
```

## Split DNS: Examples

In the following example, the split tunnel list named “101” contains the 10.168.0.0/16 network. It is necessary to include this network information so that the DNS requests to the internal DNS server of 10.168.1.1 are encrypted.

```
crypto isakmp client configuration group home
 key abcd
 acl 101
 dns 10.168.1.1. 10.168.1.2
```

### show Output

The following **show** command output example shows that `www.ciscoexample1.com` and `www.ciscoexample2.com` have been added to the policy group:

```
Router# show running-config | security group

crypto isakmp client configuration group 831server
key abcd
dns 10.104.128.248
split-dns www.ciscoexample1.com
split-dns www.ciscoexample2.com
group home2 key abcd
```

The following **show** command output example displays currently configured DNS views:

```
Router# show ip dns view

DNS View default parameters:
Logging is off
DNS Resolver settings:
 Domain lookup is enabled
 Default domain name: cisco.com
 Domain search list:
 Lookup timeout: 3 seconds
 Lookup retries: 2
 Domain name-servers:
 172.16.168.183
DNS Server settings:
 Forwarding of queries is enabled
 Forwarder addresses:

DNS View ezvpn-internal-view parameters:
Logging is off
DNS Resolver settings:
 Domain lookup is enabled
 Default domain name:
 Domain search list:
 Lookup timeout: 3 seconds
 Lookup retries: 2
 Domain name-servers:
 10.104.128.248
DNS Server settings:
 Forwarding of queries is enabled
 Forwarder addresses:
```

The following **show** command output example displays currently configured DNS view lists.

```
Router# show ip dns view-list

View-list ezvpn-internal-viewlist:
View ezvpn-internal-view:
 Evaluation order: 10
```

```

Restrict to ip dns name-list: 1
View default:
Evaluation order: 20

```

The following **show** command output displays DNS name lists.

```
Router# show ip dns name-list
```

```

ip dns name-list 1
 permit www.ciscoexample1.com
 permit www.ciscoexample2.com

```

## DHCP Client Proxy: Examples

The following examples display DHCP client proxy output information using **show** and **debug** commands.

### show Output



#### Note

To use the **show ip dhcp** command, the DHCP server must be a Cisco IOS server.

The following **show ip dhcp pool** command output provides information about the DHCP parameters:

```
Router# show ip dhcp pool
```

```

Pool dynpool :
 Utilization mark (high/low) : 100 / 0
 Subnet size (first/next) : 0 / 0
 Total addresses : 254
 Leased addresses : 1
 Pending event : none
 1 subnet is currently in the pool:
 Current index IP address range Leased addresses
 10.3.3.1 - 10.3.3.254 1
 No relay targets associated with class aclass

```

The following **show ip dhcp** command output provides information about the DHCP bindings:

```
Router# show ip dhcp binding
```

```

Bindings from all pools not associated with VRF:
IP address Client-ID/ Lease expiration Type
 Hardware address/User name
10.3.3.5 0065.7a76.706e.2d63. Apr 04 2006 06:01 AM Automatic
6c69.656e.74

```

### debug Output

The following example shows how the **debug crypto isakmp** and **debug ip dhcp server events** commands can be used to troubleshoot your DHCP client proxy support configuration:

```

*Apr 3 06:01:32.047: ISAKMP: Config payload REQUEST *Apr 3 06:01:32.047:
ISAKMP:(1002):checking request:
*Apr 3 06:01:32.047: ISAKMP: IP4_ADDRESS
*Apr 3 06:01:32.047: ISAKMP: IP4_NETMASK
*Apr 3 06:01:32.047: ISAKMP: MODECFG_CONFIG_URL
*Apr 3 06:01:32.047: ISAKMP: MODECFG_CONFIG_VERSION
*Apr 3 06:01:32.047: ISAKMP: IP4_DNS
*Apr 3 06:01:32.047: ISAKMP: IP4_DNS
*Apr 3 06:01:32.047: ISAKMP: IP4_NBNS

```

```

*Apr 3 06:01:32.047: ISAKMP: IP4_NBNS
*Apr 3 06:01:32.047: ISAKMP: SPLIT_INCLUDE
*Apr 3 06:01:32.047: ISAKMP: SPLIT_DNS
*Apr 3 06:01:32.047: ISAKMP: DEFAULT_DOMAIN
*Apr 3 06:01:32.047: ISAKMP: MODECFG_SAVEPWD
*Apr 3 06:01:32.047: ISAKMP: INCLUDE_LOCAL_LAN
*Apr 3 06:01:32.047: ISAKMP: PFS
*Apr 3 06:01:32.047: ISAKMP: BACKUP_SERVER
*Apr 3 06:01:32.047: ISAKMP: APPLICATION_VERSION
*Apr 3 06:01:32.047: ISAKMP: MODECFG_BANNER
*Apr 3 06:01:32.047: ISAKMP: MODECFG_IPSEC_INT_CONF
*Apr 3 06:01:32.047: ISAKMP: MODECFG_HOSTNAME
*Apr 3 06:01:32.047: ISAKMP/author: Author request for group homesuccessfully sent to AAA
*Apr 3 06:01:32.047: ISAKMP:(1002):Input = IKE_MSG_FROM_PEER, IKE_CFG_REQUEST

*Apr 3 06:01:32.047: ISAKMP:(1002):Old State = IKE_P1_COMPLETE New State =
IKE_CONFIG_AUTHOR_AAA_AWAIT

*Apr 3 06:01:32.047: ISAKMP:(1002):attributes sent in message:
*Apr 3 06:01:32.047: Address: 10.2.0.0
*Apr 3 06:01:32.047: Requesting DHCP Server0 address 10.3.3.3 *Apr 3 06:01:32.047:
DHCPD: Sending notification of DISCOVER:
*Apr 3 06:01:32.047: DHCPD: htype 1 chaddr aabb.cc00.6600
*Apr 3 06:01:32.047: DHCPD: circuit id 00000000
*Apr 3 06:01:32.047: DHCPD: Seeing if there is an internally specified pool class:
*Apr 3 06:01:32.047: DHCPD: htype 1 chaddr aabb.cc00.6600
*Apr 3 06:01:32.047: DHCPD: circuit id 00000000

*Apr 3 06:01:34.063: DHCPD: Adding binding to radix tree (10.3.3.5) *Apr 3 06:01:34.063:
DHCPD: Adding binding to hash tree *Apr 3 06:01:34.063: DHCPD: assigned IP address
10.3.3.5 to client 0065.7a76.706e.2d63.6c69.656e.74.
*Apr 3 06:01:34.071: DHCPD: Sending notification of ASSIGNMENT:
*Apr 3 06:01:34.071: DHCPD: address 10.3.3.5 mask 255.255.255.0
*Apr 3 06:01:34.071: DHCPD: htype 1 chaddr aabb.cc00.6600
*Apr 3 06:01:34.071: DHCPD: lease time remaining (secs) = 86400
*Apr 3 06:01:34.183: Obtained DHCP address 10.3.3.5 *Apr 3 06:01:34.183:
ISAKMP:(1002):allocating address 10.3.3.5 *Apr 3 06:01:34.183: ISAKMP: Sending private
address: 10.3.3.5 *Apr 3 06:01:34.183: ISAKMP: Sending subnet mask: 255.255.255.0

```

## cTCP Session: Example

The following **debug crypto ctcp** command output displays information about a cTCP session, and it includes comments about the output:

```
Router# debug crypto ctcp
```

```

! In the following two lines, a cTCP SYN packet is received from the client, and the cTCP
connection is created.
*Sep 26 11:14:37.135: cTCP: Connection[648B50C0] 10.76.235.21:3519 10.76.248.239:10000:
created
*Sep 26 11:14:37.135: cTCP: SYN from 10.76.235.21:3519
! In the following line, the SYN acknowledgement is sent to the client.
*Sep 26 11:14:37.135: cTCP: Sending SYN(680723B2)ACK(100C637) to 10.76.235.21:3519
! In the following two lines, an acknowledgement is received, and connection setup is
complete. IKE packets should now be received on this newly created cTCP session.
*Sep 26 11:14:37.135: cTCP: Connection[648B50C0] 10.76.235.21:3519 10.76.248.239:10000:
found
*Sep 26 11:14:37.135: cTCP: ACK from 10.76.235.21:3519
*Sep 26 11:14:37.727: cTCP: Connection[648B50C0] 10.76.235.21:3519 10.76.248.239:10000:
found

```

```

*Sep 26 11:14:37.731: cTCP: updating PEER Seq number to 168288031
*Sep 26 11:14:37.731: cTCP: Pak with contiguous buffer
*Sep 26 11:14:37.731: cTCP: mangling IKE packet from peer: 10.76.235.21:500->3519
 10.76.248.239:500->500
*Sep 26 11:14:37.731: cTCP: Connection[648B50C0] 10.76.235.21:3519 10.76.248.239:10000:
found
*Sep 26 11:14:37.799: cTCP: demangling outbound IKE packet: 10.76.248.239:500->500
 10.76.235.21:3519->500
*Sep 26 11:14:37.799: cTCP: encapsulating IKE packet
*Sep 26 11:14:37.799: cTCP: updating LOCAL Seq number to 17452987271
! The above lines show that after the required number of IKE packets are exchanged, IKE
and IPsec SAs are created.
*Sep 26 11:14:40.335: cTCP: updating PEER Seq number to 168304311
*Sep 26 11:14:40.335: cTCP: Pak with particles
*Sep 26 11:14:40.335: cTCP: encapsulating pak
*Sep 26 11:14:40.339: cTCP: datagramstart 0xF2036D8, network_start 0xF2036D8, size 112
*Sep 26 11:14:40.339: cTCP: Pak with contiguous buffer
*Sep 26 11:14:40.339: cTCP: allocated new buffer
*Sep 26 11:14:40.339: cTCP: updating LOCAL Seq number to 17452995351
*Sep 26 11:14:40.339: IP: s=10.76.248.239 (local), d=10.76.235.21 (FastEthernet1/1), len
148, cTCP
! The above lines show that Encapsulating Security Payload (ESP) packets are now being
sent and received.

```

## Additional References

The following sections provide references related to Easy VPN Server.

## Related Documents

| Related Topic                         | Document Title                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuring a router as a VPN client  | <a href="#">Easy VPN Remote Enhancements</a> , Cisco IOS Release 12.4(4)T feature module                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| General information on IPsec and VPN  | Refer to the following information in the product literature and in IP technical tips sections on Cisco.com: <ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Security Configuration Guide</a></li> <li>• <a href="#">Cisco IOS Security Command Reference</a>, Release 12.4</li> <li>• <a href="#">An Introduction to IP Security (IPSec) Encryption</a></li> <li>• <a href="#">Deploying IPSec</a></li> <li>• <a href="#">Certificate Authority Support for IPSec Overview</a></li> <li>• <a href="#">Cisco Secure VPN Client</a></li> <li>• <a href="#">IPSec VPN High Availability Enhancements</a>, Cisco IOS Release 12.2(8)T feature module</li> <li>• <a href="#">Cisco Easy VPN</a></li> <li>• <a href="#">Configuring NAC with IPSec Dynamic Virtual Tunnel Interface</a></li> </ul> |
| IPsec Protocol options and attributes | “Configuring Internet Key Exchange Security Protocol” chapter in the <a href="#">Cisco IOS Security Configuration Guide</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Related Topic             | Document Title                                                                                       |
|---------------------------|------------------------------------------------------------------------------------------------------|
| IPsec virtual tunnels     | <a href="#">IPSec Virtual Tunnel Interface</a> , Cisco IOS Release 12.3(14)T feature module          |
| Network Admission Control | <a href="#">Network Admission Control</a> , Cisco IOS Release 12.3(8)T                               |
| RRI                       | <a href="#">IPSec VPN High Availability Enhancements</a> , Cisco IOS Release 12.2(8)T feature module |
| Split DNS                 | <a href="#">Configuring Split and Dynamic DNS on the Cisco VPN 3000</a>                              |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features.

- **aaa authentication login**
- **access-restrict**
- **acl (ISAKMP)**
- **auto-update client**
- **backup-gateway**
- **banner**
- **browser-proxy**
- **clear crypto ctp**
- **clear crypto session**
- **client authentication list**
- **client pki authorization list**
- **configuration url**
- **configuration version**
- **crypto aaa attribute list**
- **crypto ctp**
- **crypto ipsec server send-update**
- **crypto isakmp client configuration browser-proxy**
- **crypto isakmp client configuration group**
- **crypto isakmp client firewall**
- **crypto logging ezvpn**
- **debug crypto ctp**
- **debug crypto condition**

- **debug ip dns name-list**
- **debug ip dns view**
- **debug ip dns view-list**
- **dhcp server (isakmp)**
- **dhcp timeout**
- **domain (isakmp-group)**
- **firewall are-u-there**
- **firewall policy**
- **group-lock**
- **include-local-lan**
- **key (isakmp-group)**
- **max-logins**
- **max-users**
- **pfs**
- **policy**
- **pool (isakmp-group)**
- **proxy**
- **save-password**
- **show crypto ctp**
- **show crypto debug-condition**
- **show crypto isakmp peers**
- **show crypto isakmp profile**
- **show crypto isakmp sa**
- **show crypto session**
- **show crypto session group**
- **show crypto session summary**
- **show ip dns name-list**
- **show ip dns view**
- **show ip dns view-list**
- **split-dns**
- **wins**
- **Glossary**

For information about these commands, see the Cisco IOS Security Command Reference at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.



# Feature Information for Easy VPN Server

Table 3 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



## Note

Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 3** Feature Information for Easy VPN Server

| Feature Name    | Releases                | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Easy VPN Server | 12.2(8)T                | The Easy VPN Server feature introduces server support for the Cisco VPN Client Release 3.x and later software clients and Cisco VPN hardware clients (such as the Cisco 800, Cisco 900, Cisco 1700, VPN 3002, and PIX 501 devices). This feature allows a remote end user to communicate using IP Security (IPsec) with any Cisco IOS Virtual Private Network (VPN) gateway. Centrally managed IPsec policies are “pushed” to the client device by the server, minimizing configuration by the end user. |
|                 | 12.3(2)T                | RADIUS support for user profiles, user-based policy control, session monitoring for VPN group access, backup-gateway list, and PFS were added.                                                                                                                                                                                                                                                                                                                                                           |
|                 | 12.4(2)T<br>12.2(33)SXH | The following feature was added in this release: <ul style="list-style-type: none"> <li>Banner, Auto-Update, and Browser Proxy Enhancements</li> </ul>                                                                                                                                                                                                                                                                                                                                                   |
|                 | 12.4(4)T<br>12.2(33)SXH | The following features were added in this release: <ul style="list-style-type: none"> <li>Configuration Management Enhancements (Pushing a Configuration URL Through a Mode-Configuration Exchange)</li> <li>Per User AAA Policy Download with PKI</li> <li>Syslog Message Enhancements</li> <li>Network Admission Control for Easy VPN</li> <li>Password Aging</li> <li>Virtual IPsec Interface Support</li> </ul>                                                                                      |
|                 | 12.4(6)T                | The Central Policy Push Firewall Policy Push feature was added.                                                                                                                                                                                                                                                                                                                                                                                                                                          |

**Table 3** *Feature Information for Easy VPN Server (continued)*

| Feature Name | Releases    | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | 12.2(33)SRA | This feature was integrated into Cisco IOS Release 12.2(33)SRA.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|              | 12.4(9)T    | <p>The following features were added in this release:</p> <ul style="list-style-type: none"> <li>• DHCP Client Proxy<br/>The following section provides information about this feature: <ul style="list-style-type: none"> <li>– <a href="#">DHCP Client Proxy, page 11</a></li> </ul> </li> <li>• Virtual Tunnel Interface Per-User Attribute Support for Easy VPN Servers. <ul style="list-style-type: none"> <li>– <a href="#">Virtual Tunnel Interface Per-User Attribute Support, page 13</a></li> </ul> </li> <li>• Split DNS<br/>The following section provides information about this feature: <ul style="list-style-type: none"> <li>– <a href="#">Split DNS, page 18</a></li> </ul> </li> <li>• cTCP<br/>The following sections provide information about this feature: <ul style="list-style-type: none"> <li>– <a href="#">cTCP, page 18</a></li> <li>– <a href="#">Configuring cTCP, page 50</a></li> <li>– <a href="#">cTCP Session: Example, page 70</a></li> </ul> </li> <li>• Per-User Attribute Support for Easy VPN Servers<br/>The following sections provide information about this feature: <ul style="list-style-type: none"> <li>– <a href="#">Per-User Attribute Support for Easy VPN Servers, page 15</a></li> <li>– <a href="#">Configuring Per-User Attributes on a Local Easy VPN AAA Server, page 38</a></li> <li>– <a href="#">Per-User Attributes on an Easy VPN Server: Example, page 62</a></li> </ul> </li> </ul> <p>The following new commands were introduced: <b>crypto aaa attribute list</b>, <b>debug ip dns</b>, <b>dhcp-server (isakmp)</b>, <b>dhcp-timeout</b>, <b>show ip dns name-list</b>, <b>show ip dns view</b>, and <b>show ip dns view-list</b></p> <p>The following commands were modified: <b>crypto isakmp client configuration group</b></p> |

**Table 3**      *Feature Information for Easy VPN Server (continued)*

| Feature Name                | Releases                 | Feature Information                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                             | 12.4(11)T                | The DHCP Client Proxy feature was updated to include manageability enhancements for remote access VPNs.<br><br>The following commands were modified: <b>clear crypto session, crypto isakmp client configuration group, debug crypto condition, show crypto debug-condition, show crypto isakmp peers, show crypto isakmp profile, show crypto isakmp sa, show crypto session</b> |
| EasyVPN Server Enhancements | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                     |

# Glossary

**AAA**—authentication, authorization, and accounting. Framework of security services that provides the method for identifying users (authentication), for remote access control (authorization), and for collecting and sending security server information used for billing, auditing, and reporting (accounting).

**aggressive mode (AM)**—Mode during Internet Key Exchange negotiation. Compared to main mode (MM), AM eliminates several steps, which makes it faster but less secure than MM. Cisco IOS software will respond in aggressive mode to an Internet Key Exchange (IKE) peer that initiates aggressive mode.

**AV pair**—attribute-value pair. Additional authentication and authorization information in the following format: Cisco:AVPair=“protocol:attribute=value”.

**IKE**—Internet Key Exchange. Hybrid protocol that implements Oakley key exchange and Skeme key exchange inside the ISAKMP framework. Although IKE can be used with other protocols, its initial implementation is with IPsec. IKE provides authentication of the IPsec peers, negotiates IPsec keys, and negotiates IPsec security associations.

**IPsec**—IP Security Protocol. Framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer. IPsec uses IKE to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPsec. IPsec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

**ISAKMP**—Internet Security Association Key Management Protocol. Protocol framework that defines payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of a security association.

**MM**—main mode. Mode that is slower than aggressive mode but more secure and more flexible than aggressive mode because it can offer an IKE peer more security proposals. The default action for IKE authentication (Rivest, Shamir, and Adelman signature (rsa-sig), RSA encryption (rsa-encr), or preshared) is to initiate main mode.

**policy push**—Allows administrators to push policies that enforce security to the Cisco Easy VPN (software) Client and related firewall software.

**reverse route injection (RRI)**—Simplified network design for VPNs on which there is a requirement for redundancy or load balancing. RRI works with both dynamic and static crypto maps.

In the dynamic case, as remote peers establish IPsec security associations with an RRI enabled router, a static route is created for each subnet or host protected by that remote peer. For static crypto maps, a static route is created for each destination of an extended access-list rule.

**SA**—security association. Description of how two or more entities will utilize security services to communicate securely. For example, an IPsec SA defines the encryption algorithm (if used), the authentication algorithm, and the shared session key to be used during the IPsec connection.

Both IPsec and IKE require and use SAs to identify the parameters of their connections. IKE can negotiate and establish its own SA. The IPsec SA is established either by IKE or by manual user configuration.

**VPN**—Virtual Private Network. Framework that consists of multiple peers transmitting private data securely to one another over an otherwise public infrastructure. In this framework, inbound and outbound network traffic is protected using protocols that tunnel and encrypt all data. This framework permits networks to extend beyond their local topology, while remote users are provided with the appearance and functionality of a direct network connection.

**Note**

---

Refer to *[Internetworking Terms and Acronyms](#)* for terms not included in this glossary.

---

---

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

---

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

---

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.





# Invalid Security Parameter Index Recovery

---

When an invalid security parameter index error (shown as “Invalid SPI”) occurs in IP Security (IPSec) packet processing, the feature allows for an Internet Key Exchange (IKE) security association (SA) to be established. The “IKE” module sends notification of the “Invalid SPI” error to the originating IPSec peer so that Security Association Databases (SADB) can be resynchronized and successful packet processing can be resumed.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all of the features documented in this module.* To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for](#)” [section on page 17](#).

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for](#), page 2
- [Restrictions for](#), page 2
- [Information About](#), page 2
- [How to Configure](#), page 3
- [Configuration Examples for](#), page 10
- [Additional References](#), page 16
- [Command Reference](#), page 17
- [Feature Information for](#), page 17



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

## Prerequisites for

Before configuring the feature, you must have enabled Internet Key Exchange (IKE) and IPsec on your router.

## Restrictions for

If an IKE SA is being initiated to notify an IPsec peer of an “Invalid SPI” error, there is the risk that a denial-of-service (DoS) attack can occur. The feature has a built-in mechanism to minimize such a risk, but because there is a risk, the feature is not enabled by default. You must enable the command using command-line interface (CLI).

## Information About

To use the feature, you should understand the following concept.

- [How the Feature Works, page 2](#)

## How the Feature Works

An IPsec “black hole” occurs when one IPsec peer “dies” (for example, a peer can “die” if a reboot occurs or if an IPsec peer somehow gets reset). Because one of the peers (the receiving peer) is completely reset, it loses its IKE SA with the other peer. Generally, when an IPsec peer receives a packet for which it cannot find an SA, it tries to send an IKE “INVALID SPI NOTIFY” message to the data originator. This notification is sent using the IKE SA. If there is no IKE SA available, the receiving peer drops the packet.



### Note

---

A single security association (SA) has only two peers. However, a SADB can have multiple SAs, whereby each SA has an association with a different peer.

---

When an invalid security parameter index (SPI) is encountered, the Invalid Security Parameter Index feature provides for the setting up of an IKE SA with the originator of the data, and the IKE “INVALID SPI NOTIFY” message is sent. The peer that originated the data “sees” the “INVALID SPI NOTIFY” message and deletes the IPsec SA that has the invalid SPI. If there is further traffic from the originating peer, there will not be any IPsec SAs, and new SAs will be set up. Traffic will flow again. The default behavior (that is, without configuring the feature) is that the data packet that caused the invalid SPI error is dropped. The originating peer keeps on sending the data using the IPsec SA that has the invalid SPI, and the receiving peer keeps dropping the traffic (thus creating the “black hole”).

The IPsec module uses the IKE module to send an IKE “INVALID SPI NOTIFY” message to the other peer. Once the invalid SPI recovery is in place, there should not be any significant dropping of packets although the IPsec SA setup can itself result in the dropping of a few packets.

To configure your router for the feature, use the **crypto isakmp invalid-spi-recovery** command. The IKE SA will not be initiated unless you have configured this command.



# How to Configure

This section contains the following procedure.

- [Configuring, page 3](#)

## Configuring

To configure the feature, perform the following steps.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `crypto isakmp invalid-spi-recovery`

### DETAILED STEPS

|        | Command or Action                                                                                                                          | Purpose                                                                                                                       |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br>Router> <code>enable</code>                                                                  | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>              |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br>Router# <code>configure terminal</code>                                          | Enters global configuration mode.                                                                                             |
| Step 3 | <code>crypto isakmp invalid-spi-recovery</code><br><br><b>Example:</b><br>Router (config)# <code>crypto isakmp invalid-spi-recovery</code> | Initiates the IKE module process whereby the IKE module notifies the receiving peer that an “Invalid SPI” error has occurred. |

## Verifying an Configuration

To determine the status of the IPsec SA for traffic between two peers, you can use the **show crypto ipsec sa** command. If the IPsec SA is available on one peer and not on the other, there is a “black hole” situation, in which case you will see the invalid SPI errors being logged for the receiving peer. If you turn console logging on or check the syslog server, you will see that these errors are also being logged.

Figure 1 shows the topology of a typical preshared configuration setup. Host 1 is the initiating peer (initiator), and Host 2 is the receiving peer (responder).

**Figure 1** Preshared Configuration Topology



### SUMMARY STEPS

To verify the preshared configuration, perform the following steps.

1. Initiate the IKE and IPsec SAs between Host 1 and Host 2
2. Clear the IKE and IPsec SAs on Router B
3. Send traffic from Host 1 to Host 2 and ensure that IKE and IPsec SAs are correctly established
4. Check for an invalid SPI message on Router B

### DETAILED STEPS

#### Step 1 Initiate the IKE and IPsec SAs between Host 1 and Host 2

##### Router A

```
Router# show crypto isakmp sa
```

| f_vrf/i_vrf | dst      | src      | state   | conn-id | slot |
|-------------|----------|----------|---------|---------|------|
| /           | 10.2.2.2 | 10.1.1.1 | QM_IDLE | 1       | 0    |

##### Router B

```
Router# show crypto isakmp sa
```

| f_vrf/i_vrf | dst      | src      | state   | conn-id | slot |
|-------------|----------|----------|---------|---------|------|
| /           | 10.1.1.1 | 10.2.2.2 | QM_IDLE | 1       | 0    |

##### Router A

```
Router# show crypto ipsec sa interface fastethernet0/0
```

```
interface: FastEthernet0/0
 Crypto map tag: testtag1, local addr. 10.1.1.1

protected vrf:
 local ident (addr/mask/prot/port): (10.0.0.1/255.255.255.255/0/0)
 remote ident (addr/mask/prot/port): (10.0.2.2/255.255.255.255/0/0)
```

```

current_peer: 10.2.2.2:500
 PERMIT, flags={origin_is_acl,}
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.2.2.2
path mtu 1500, media mtu 1500
current outbound spi: 7AA69CB7

inbound esp sas:
 spi: 0x249C5062(614223970)
 transform: esp-des esp-sha-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 5123, flow_id: 1, crypto map: testtag1
 crypto engine type: Hardware
 sa timing: remaining key lifetime (k/sec): (4537831/3595)
 IV size: 8 bytes
 replay detection support: Y

inbound ah sas:
 spi: 0xB16D1587(2976716167)
 transform: ah-sha-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 5121, flow_id: 1, crypto map: testtag1
 crypto engine type: Hardware
 sa timing: remaining key lifetime (k/sec): (4537831/3595)
 replay detection support: Y

inbound pcp sas:

outbound esp sas:
 spi: 0x7AA69CB7(2057739447)
 transform: esp-des esp-sha-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 5124, flow_id: 2, crypto map: testtag1
 crypto engine type: Hardware
 sa timing: remaining key lifetime (k/sec): (4537835/3595)
 IV size: 8 bytes
 replay detection support: Y

outbound ah sas:
 spi: 0x1214F0D(18960141)
 transform: ah-sha-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 5122, flow_id: 2, crypto map: testtag1
 crypto engine type: Hardware
 sa timing: remaining key lifetime (k/sec): (4537835/3594)
 replay detection support: Y

outbound pcp sas:

```

## Router B

```
Router# show crypto ipsec sa interface ethernet1/0
```

```

interface: Ethernet1/0
 Crypto map tag: testtag1, local addr. 10.2.2.2

protected vrf:
 local ident (addr/mask/prot/port): (10.0.2.2/255.255.255.255/0/0)

```

```

remote ident (addr/mask/prot/port): (10.0.0.1/255.255.255.255/0/0)
current_peer: 10.1.1.1:500
 PERMIT, flags={origin_is_acl,}
 #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
 #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 10.2.2.2, remote crypto endpt.: 10.1.1.1
path mtu 1500, media mtu 1500
current outbound spi: 249C5062

inbound esp sas:
 spi: 0x7AA69CB7(2057739447)
 transform: esp-des esp-sha-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 5123, flow_id: 1, crypto map: testtag1
 crypto engine type: Hardware
 sa timing: remaining key lifetime (k/sec): (4421281/3593)
 IV size: 8 bytes
 replay detection support: Y

inbound ah sas:
 spi: 0x1214F0D(18960141)
 transform: ah-sha-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 5121, flow_id: 1, crypto map: testtag1
 crypto engine type: Hardware
 sa timing: remaining key lifetime (k/sec): (4421281/3593)
 replay detection support: Y

inbound pcg sas:

outbound esp sas:
 spi: 0x249C5062(614223970)
 transform: esp-des esp-sha-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 5124, flow_id: 2, crypto map: testtag1
 crypto engine type: Hardware
 sa timing: remaining key lifetime (k/sec): (4421285/3593)
 IV size: 8 bytes
 replay detection support: Y

outbound ah sas:
 spi: 0xB16D1587(2976716167)
 transform: ah-sha-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 5122, flow_id: 2, crypto map: testtag1
 crypto engine type: Hardware
 sa timing: remaining key lifetime (k/sec): (4421285/3592)
 replay detection support: Y

outbound pcg sas:

```

## Step 2 Clear the IKE and IPSec SAs on Router B

```
Router# clear crypto isakmp
```

```
Router# clear crypto sa
```

```

Router# show crypto isakmp sa

 f_vrf/i_vrf dst src state conn-id slot
 / 10.2.2.2 10.1.1.1 MM_NO_STATE 1 0 (deleted)

Router# show crypto ipsec sa

interface: Ethernet1/0
 Crypto map tag: testtag1, local addr. 10.2.2.2

protected vrf:
local ident (addr/mask/prot/port): (10.0.2.2/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (10.0.0.1/255.255.255.255/0/0)
current_peer: 10.1.1.1:500
 PERMIT, flags={origin_is_acl,}
 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
 #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 0, #recv errors 0

 local crypto endpt.: 10.2.2.2, remote crypto endpt.: 10.1.1.1
 path mtu 1500, media mtu 1500
 current outbound spi: 0

inbound esp sas:

inbound ah sas:

inbound pcg sas:

outbound esp sas:

outbound ah sas:

outbound pcg sas:

```

### Step 3 Send traffic from Host 1 to Host 2 and ensure that new IKE and IPSec SAs are correctly established

```

ping
Protocol [ip]: ip
Target IP address: 10.0.2.2
Repeat count [5]: 30
Datagram size [100]: 100
Timeout in seconds [2]:
Extended commands [n]: no
Sweep range of sizes [n]: n
Type escape sequence to abort.
Sending 30, 100-byte ICMP Echos to 10.0.2.2, timeout is 2 seconds:
..!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 93 percent (28/30), round-trip min/avg/max = 1/3/8 ms

```

```

RouterB# show crypto isakmp sa

 f_vrf/i_vrf dst src state conn-id slot
 / 10.1.1.1 10.2.2.2 QM_IDLE 3 0
 / 10.1.1.1 10.2.2.2 MM_NO_STATE 1 0 (deleted)

RouterB# show crypto ipsec sa

interface: Ethernet1/0
 Crypto map tag: testtag1, local addr. 10.2.2.2

```

```

protected vrf:
local ident (addr/mask/prot/port): (10.0.2.2/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (10.0.0.1/255.255.255.255/0/0)
current_peer: 10.1.1.1:500
 PERMIT, flags={origin_is_acl,}
#pkts encaps: 28, #pkts encrypt: 28, #pkts digest: 28
#pkts decaps: 28, #pkts decrypt: 28, #pkts verify: 28
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.2.2.2, remote crypto endpt.: 10.1.1.1
path mtu 1500, media mtu 1500
current outbound spi: D763771F

inbound esp sas:
 spi: 0xE7AB4256(3886760534)
 transform: esp-des esp-sha-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 5127, flow_id: 3, crypto map: testtag1
 crypto engine type: Hardware
 sa timing: remaining key lifetime (k/sec): (4502463/3596)
 IV size: 8 bytes
 replay detection support: Y

inbound ah sas:
 spi: 0xF9205CED(4179647725)
 transform: ah-sha-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 5125, flow_id: 3, crypto map: testtag1
 crypto engine type: Hardware
 sa timing: remaining key lifetime (k/sec): (4502463/3596)
 replay detection support: Y

inbound pcg sas:

outbound esp sas:
 spi: 0xD763771F(3613619999)
 transform: esp-des esp-sha-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 5128, flow_id: 4, crypto map: testtag1
 crypto engine type: Hardware
 sa timing: remaining key lifetime (k/sec): (4502468/3596)
 IV size: 8 bytes
 replay detection support: Y

outbound ah sas:
 spi: 0xEB95406F(3952427119)
 transform: ah-sha-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 5126, flow_id: 4, crypto map: testtag1
 crypto engine type: Hardware
 sa timing: remaining key lifetime (k/sec): (4502468/3595)
 replay detection support: Y

outbound pcg sas:

```

RouterA# **show crypto isakmp sa**

| f_vrf/i_vrf | dst      | src      | state       | conn-id | slot |           |
|-------------|----------|----------|-------------|---------|------|-----------|
| /           | 10.2.2.2 | 10.1.1.1 | MM_NO_STATE | 1       | 0    | (deleted) |

```

/ 10.2.2.2 10.1.1.1 QM_IDLE 2 0

```

Check for an invalid SPI message on Router B

Router# **show logging**

```

Syslog logging: enabled (10 messages dropped, 13 messages rate-limited, 0 flushes, 0
overruns, xml disabled)
 Console logging: disabled
 Monitor logging: level debugging, 0 messages logged, xml disabled
 Buffer logging: level debugging, 43 messages logged, xml disabled
 Logging Exception size (8192 bytes)
 Count and timestamp logging messages: disabled
 Trap logging: level informational, 72 message lines logged

Log Buffer (8000 bytes):

*Mar 24 20:55:45.739: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid
spi for
 destaddr=10.2.2.2, prot=51, spi=0x1214F0D(18960141), srcaddr=10.1.1.1
*Mar 24 20:55:47.743: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 10.2.2.2, remote= 10.1.1.1,
 local_proxy= 10.0.2.2/255.255.255.255/0/0 (type=1),
 remote_proxy= 10.0.0.1/255.255.255.255/0/0 (type=1),
 protocol= AH, transform= ah-sha-hmac ,
 lifedur= 0s and 0kb,
 spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
*Mar 24 20:55:47.743: IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 10.2.2.2, remote= 10.1.1.1,
 local_proxy= 10.0.2.2/255.255.255.255/0/0 (type=1),
 remote_proxy= 10.0.0.1/255.255.255.255/0/0 (type=1),
 protocol= ESP, transform= esp-des esp-sha-hmac ,
 lifedur= 0s and 0kb,
 spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
*Mar 24 20:55:47.743: IPSEC(kei_proxy): head = testtag1, map->ivrf = , kei->ivrf =
*Mar 24 20:55:47.743: IPSEC(key_engine): got a queue event with 2 kei messages
*Mar 24 20:55:47.743: IPSEC(spi_response): getting spi 4179647725 for SA
 from 10.2.2.2 to 10.1.1.1 for prot 2
*Mar 24 20:55:47.747: IPSEC(spi_response): getting spi 3886760534 for SA
 from 10.2.2.2 to 10.1.1.1 for prot 3
*Mar 24 20:55:48.071: IPsec: Flow_switching Allocated flow for flow_id 939524099
*Mar 24 20:55:48.071: IPsec: Flow_switching Allocated flow for flow_id 939524100
*Mar 24 20:55:48.135: IPSEC(key_engine): got a queue event with 4 kei messages
*Mar 24 20:55:48.135: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 10.2.2.2, remote= 10.1.1.1,
 local_proxy= 10.0.2.2/0.0.0.0/0/0 (type=1),
 remote_proxy= 10.0.0.1/0.0.0.0/0/0 (type=1),
 protocol= AH, transform= ah-sha-hmac ,
 lifedur= 3600s and 4608000kb,
 spi= 0xF9205CED(4179647725), conn_id= 939529221, keysize= 0, flags= 0x2
*Mar 24 20:55:48.135: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 10.2.2.2, remote= 10.1.1.1,
 local_proxy= 10.0.2.2/0.0.0.0/0/0 (type=1),
 remote_proxy= 10.0.0.1/0.0.0.0/0/0 (type=1),
 protocol= AH, transform= ah-sha-hmac ,
 lifedur= 3600s and 4608000kb,
 spi= 0xEB95406F(3952427119), conn_id= 939529222, keysize= 0, flags= 0xA
*Mar 24 20:55:48.135: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 10.2.2.2, remote= 10.1.1.1,
 local_proxy= 10.0.2.2/0.0.0.0/0/0 (type=1),
 remote_proxy= 10.0.0.1/0.0.0.0/0/0 (type=1),
 protocol= ESP, transform= esp-des esp-sha-hmac ,
 lifedur= 3600s and 4608000kb,

```

```

spi= 0xE7AB4256(3886760534), conn_id= 939529223, keysize= 0, flags= 0x2
*Mar 24 20:55:48.135: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 10.2.2.2, remote= 10.1.1.1,
local_proxy= 10.0.2.2/0.0.0.0/0/0 (type=1),
remote_proxy= 10.0.0.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-sha-hmac ,

lifedur= 3600s and 4608000kb,
spi= 0xD763771F(3613619999), conn_id= 939529224, keysize= 0, flags= 0xA
*Mar 24 20:55:48.139: IPSEC(kei_proxy): head = testtag1, map->ivrf = , kei->ivrf =
*Mar 24 20:55:48.139: IPSEC(mtree_add_ident): src 10.2.2.2, dest 10.1.1.1, dest_port 0

*Mar 24 20:55:48.139: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.1.1.1, sa_prot= 51,
sa_spi= 0xF9205CED(4179647725),
sa_trans= ah-sha-hmac , sa_conn_id= 939529221
*Mar 24 20:55:48.139: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.2.2.2, sa_prot= 51,
sa_spi= 0xEB95406F(3952427119),
sa_trans= ah-sha-hmac , sa_conn_id= 939529222
*Mar 24 20:55:48.139: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.1.1.1, sa_prot= 50,
sa_spi= 0xE7AB4256(3886760534),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 939529223
*Mar 24 20:55:48.139: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.2.2.2, sa_prot= 50,
sa_spi= 0xD763771F(3613619999),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 939529224
ipseca-72a#

```

## Configuration Examples for

This section provides the following configuration example.

- [: Example, page 10](#)

### : Example

The following example shows that invalid security parameter index recovery has been configured on Router A and Router B. [Figure 1](#) shows the topology used for this example.

#### Router A

```
Router# show running-config
```

```
Building configuration...
```

```

Current configuration : 2048 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service tcp-small-servers
!
hostname ipseca-71a
!
logging queue-limit 100

```



```
no logging console
enable secret 5 $1$4GZB$L2Y0mnenOCNAu0jgFxebT/
enable password lab
!
clock timezone PST -8

clock summer-time PDT recurring
ip subnet-zero
!
!
no ip domain lookup
!
ip cef
ip audit notify log
ip audit po max-events 100
mpls ldp logging neighbor-changes
no ftp-server write-enable
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 180
crypto isakmp key 0 1234 address 10.2.2.2
crypto isakmp invalid-spi-recovery
!
!
crypto ipsec transform-set auth2 ah-sha-hmac esp-des esp-sha-hmac
!
crypto map testtag1 10 ipsec-isakmp
 set peer 10.2.2.2
 set transform-set auth2
 match address 150
!
!
controller ISA 5/1
!
!
interface FastEthernet0/0
 ip address 10.1.1.1 255.0.0.0
 no ip route-cache cef
 duplex full
 speed 100
 crypto map testtag1
!
interface FastEthernet0/1
 ip address 10.0.0.1 255.0.0.0
 no ip route-cache cef
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 serial restart_delay 0
 clockrate 128000
!
interface Serial1/1
 no ip address
```

```

no ip route-cache
no ip mroute-cache
shutdown
serial restart_delay 0
clockrate 128000
!

interface Serial1/2
no ip address
no ip route-cache
no ip mroute-cache
shutdown
serial restart_delay 0
!
interface Serial1/3
no ip address
no ip route-cache
no ip mroute-cache
shutdown
no keepalive
serial restart_delay 0
clockrate 128000
!
ip classless
ip route 10.3.3.3 255.0.0.0 10.2.0.1
no ip http server
no ip http secure-server
!
!
access-list 150 permit ip host 10.0.0.1 host 10.0.2.2
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
!
call rsvp-sync
!
!
mgcp profile default
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
password lab
login
!
!
end

ipseca-71a#

```

### Router B

Router# **show running-config**

Building configuration...

Current configuration : 2849 bytes

```

!
version 12.3
no service pad
service timestamps debug datetime msec localtime

```

```
service timestamps log datetime msec localtime
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname ipseca-72a
!

logging queue-limit 100
no logging console
enable secret 5 1kKqL$5Th5Qhw1ubDkkK90KWFxi1
enable password lab
!
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
!
!
no ip domain lookup
!
ip cef
ip audit notify log
ip audit po max-events 100
mpls ldp logging neighbor-changes
no ftp-server write-enable
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
mta receive maximum-recipients 0
!
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 180
crypto isakmp key 0 1234 address 10.1.1.1
crypto isakmp invalid-spi-recovery
!
!
crypto ipsec transform-set auth2 ah-sha-hmac esp-des esp-sha-hmac
!
crypto map testtag1 10 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set auth2
 match address 150
!
!
controller ISA 5/1
!
!
interface FastEthernet0/0
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface Ethernet1/0
 ip address 10.2.2.2 255.0.0.0
 no ip route-cache cef
 duplex half
 crypto map testtag1
```

```
!
interface Ethernet1/1
 ip address 10.0.2.2 255.0.0.0
 no ip route-cache cef
 duplex half
!
interface Ethernet1/2
 no ip address

 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface Ethernet1/3
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface Ethernet1/4
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface Ethernet1/5
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface Ethernet1/6
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface Ethernet1/7
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
!
interface Serial3/0
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 serial restart_delay 0
!
interface Serial3/1
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 serial restart_delay 0
 clockrate 128000
!
```

```
interface Serial3/2
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
 serial restart_delay 0
!
interface Serial3/3
 no ip address

 no ip route-cache
 no ip mroute-cache
 shutdown
 no keepalive
 serial restart_delay 0
 clockrate 128000
!
ip classless
ip route 10.0.0.0 255.0.0.0 10.2.0.1
no ip http server
no ip http secure-server
!
!
access-list 150 permit ip host 10.0.2.2 host 10.0.0.1
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password lab
 login
!
!
end
```

# Additional References

The following sections provide references related to .

## Related Documents

| Related Topic      | Document Title                                                                                                                       |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Configuring IKE    | “ <a href="#">Configuring Internet Key Exchange Security Protocol</a> ” section of the <i>Cisco IOS Security Configuration Guide</i> |
| Configuring IPSec  | “ <a href="#">Part 4: IP Security and Encryption</a> ” of the <i>Cisco IOS Security Configuration Guide</i>                          |
| Interface commands | The <i>Cisco IOS Interface and Hardware Component Command Reference</i> , Release 12.3                                               |

## Standards

| Standards                                      | Title |
|------------------------------------------------|-------|
| This feature has no new or modified standards. | —     |

## MIBs

| MIBs                                      | MIBs Link                                                                                                                                                                                                              |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| This feature has no new or modified MIBs. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                      | Title |
|-------------------------------------------|-------|
| This feature has no new or modified RFCs. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

# Command Reference

The following commands are introduced or modified in the feature or features

- **crypto isakmp invalid-spi-recovery**

For information about these commands, see the Cisco IOS Security Command Reference at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

## Feature Information for

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1**      **Feature Information for**

| Feature Name                                   | Releases                 | Feature Information                                             |
|------------------------------------------------|--------------------------|-----------------------------------------------------------------|
|                                                | 12.3(2)T                 | This feature was introduced.                                    |
|                                                | 12.2(18)SXE              | This feature was integrated into Cisco IOS Release 12.2(18)SXE. |
| Invalid Special Parameter Index (SPI) Recovery | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.   |



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





# IP Security VPN Monitoring

---

The IP Security VPN Monitoring feature provides VPN session monitoring enhancements that will allow you to troubleshoot the Virtual Private Network (VPN) and monitor the end-user interface. Session monitoring enhancements include the following:

- Ability to specify an Internet Key Exchange (IKE) peer description in the configuration file
- Summary listing of crypto session status
- Syslog notification for crypto session up or down status
- Ability to clear both IKE and IP Security (IPSec) security associations (SAs) using one command-line interface (CLI)

## Feature History for IP Security VPN Monitoring

| Release                  | Modification                                                  |
|--------------------------|---------------------------------------------------------------|
| 12.3(4)T                 | This feature was introduced.                                  |
| Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for IP Security VPN Monitoring, page 2](#)
- [Restrictions for IP Security VPN Monitoring, page 2](#)
- [Information About IPSec VPN Monitoring, page 2](#)
- [How to Configure IP Security VPN Monitoring, page 4](#)
- [Configuration Examples for IP Security VPN Monitoring, page 6](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

- [Additional References, page 7](#)
- [Command Reference, page 8](#)

## Prerequisites for IP Security VPN Monitoring

- You should be familiar with IPSec and encryption.
- Your router must support IPSec, and before using the IP Security VPN Monitoring feature, you must have configured IPSec on your router.

## Restrictions for IP Security VPN Monitoring

- You must be running Cisco IOS k8 or k9 crypto images on your router.

## Information About IPSec VPN Monitoring

To troubleshoot the IPSec VPN and monitor the end-user interface, you should understand the following concepts:

- [Background: Crypto Sessions, page 2](#)
- [Per-IKE Peer Description, page 2](#)
- [Summary Listing of Crypto Session Status, page 3](#)
- [Syslog Notification for Crypto Session Up or Down Status, page 3](#)
- [IKE and IPSec Security Exchange Clear Command, page 3](#)

## Background: Crypto Sessions

A crypto session is a set of IPSec connections (flows) between two crypto endpoints. If the two crypto endpoints use IKE as the keying protocol, they are IKE peers to each other. Typically, a crypto session consists of one IKE security association (for control traffic) and at least two IPSec security associations (for data traffic—one per each direction). There may be duplicated IKE security associations (SAs) and IPSec SAs or duplicated IKE SAs or IPSec SAs for the same session in the duration of rekeying or because of simultaneous setup requests from both sides.

## Per-IKE Peer Description

The Per-IKE Peer Description function allows you to enter a description of your choosing for an IKE peer. (Before Cisco IOS Release 12.3(4)T, you could use only the IP address or fully qualified domain name [FQDN] to identify the peer; there was no way to configure a description string.) The unique peer description, which can include up to 80 characters, can be used whenever you are referencing that particular IKE peer. To add the peer description, use the **description** command.

**Note**

IKE peers that “sit” behind a Network Address Translation (NAT) device cannot be uniquely identified; therefore, they have to share the same peer description.

The primary application of this description field is for monitoring purposes (for example, when using **show** commands or for logging [syslog messages]). The description field is purely informational (for example, it cannot act as a substitute for the peer address or FQDN when defining crypto maps).

## Summary Listing of Crypto Session Status

You can get a list of all the active VPN sessions by entering the **show crypto session** command. The listing will include the following:

- Interface
- IKE peer description, if available
- IKE SAs that are associated with the peer by whom the IPsec SAs are created
- IPsec SAs serving the flows of a session

Multiple IKE or IPsec SAs may be established for the same peer (for the same session), in which case IKE peer descriptions will be repeated with different values for the IKE SAs that are associated with the peer and for the IPsec SAs that are serving the flows of the session.

You can also use the **show crypto session detail** variant of this command to obtain more detailed information about the sessions.

## Syslog Notification for Crypto Session Up or Down Status

The Syslog Notification for Crypto Session Up or Down Status function provides syslog notification every time the crypto session comes up or goes down.

The following is a sample syslog notification showing that a crypto session is up:

```
%CRYPTO-5-SESSION_STATUS: Crypto session is UP. Peer 10.6.6.1:500 fvrf=name10 ivrf=name20
Description: SJC24-2-VPN-Gateway Id: 10.5.5.2
```

The following is a sample syslog notification showing that a crypto session is down:

```
%CRYPTO-5-SESSION_STATUS: Crypto session is DOWN. Peer 10.6.6.1:500 fvrf=name10
ivrf=name20 Description: SJC24-2-VPN-Gateway Id: 10.5.5.2
```

## IKE and IPsec Security Exchange Clear Command

In previous IOS versions, there was no single command to clear both IKE and IPsec connections (that is, SAs). Instead, you had to use the **clear crypto isakmp** command to clear IKE and the **clear crypto ipsec** command to clear IPsec. The new **clear crypto session** command allows you to clear both IKE and IPsec with a single command. To clear a specific crypto session or a subset of all the sessions (for example, a single tunnel to one remote site), you need to provide session-specific parameters, such as a local or remote IP address, a local or remote port, a front door VPN routing and forwarding (FVRF) name, or an inside VRF (IVRF) name. Typically, the remote IP address will be used to specify a single tunnel to be deleted.

If a local IP address is provided as a parameter when you use the **clear crypto session** command, all the sessions (and their IKE SAs and IPSec SAs) that share the IP address as a local crypto endpoint (IKE local address) will be cleared. If you do not provide a parameter when you use the **clear crypto session** command, all IPSec SAs and IKE SAs that are in the router will be deleted.

## How to Configure IP Security VPN Monitoring

See the following sections for configuration tasks for this feature. Each task in the list is identified as either required or optional.

- [Adding the Description of an IKE Peer, page 4](#) (optional)
- [Verifying Peer Descriptions, page 5](#) (optional)
- [Clearing a Crypto Session, page 6](#) (optional)

### Adding the Description of an IKE Peer

To add the description of an IKE peer to an IPSec VPN session, perform the following steps.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp peer {ip-address ip-address}**
4. **description**

#### DETAILED STEPS

|        | Command or Action                                                              | Purpose                                                                                                               |
|--------|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                     |

|        | Command or Action                                                                                                                       | Purpose                                                                                                                                                                           |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>crypto isakmp peer</b> {ip-address ip-address}<br><br><b>Example:</b><br>Router (config)# <b>crypto isakmp peer</b> address 10.2.2.9 | Enables an IPSec peer for IKE querying of authentication, authorization, and accounting (AAA) for tunnel attributes in aggressive mode and enters ISAKMP peer configuration mode. |
| Step 4 | <b>description</b><br><br><b>Example:</b><br>Router (config-isakmp-peer)# <b>description</b> connection from site A                     | Adds a description for an IKE peer.                                                                                                                                               |

## Verifying Peer Descriptions

To verify peer descriptions, use the **show crypto isakmp peer** command.

### SUMMARY STEPS

1. **enable**
2. **show crypto isakmp peer**

### DETAILED STEPS

|        | Command or Action                                                                               | Purpose                                                                                                            |
|--------|-------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> <b>enable</b>                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>show crypto isakmp peer</b><br><br><b>Example:</b><br>Router# <b>show crypto isakmp peer</b> | Displays peer descriptions.                                                                                        |

## Examples

The following output example verifies that the description “connection from site A” has been added for IKE peer 10.2.2.9:

```
Router# show crypto isakmp peer

Peer: 10.2.2.9 Port: 500
Description: connection from site A
flags: PEER_POLICY
```

When the peer at address 10.2.2.9 connects and the session comes up, the syslog status will be shown as follows:

```
%CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP. Peer 10.2.2.9:500 Description: connection from site A Id: ezvpn
```

## Clearing a Crypto Session

To clear a crypto session, use the **clear crypto session** command from the router command line. No configuration statements are required in the configuration file to use this command.

### SUMMARY STEPS

1. **enable**
2. **clear crypto session**

### DETAILED STEPS

|        | Command or Action                                                                  | Purpose                                                                                                             |
|--------|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                             | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>clear crypto session</b><br><br><b>Example:</b><br>Router# clear crypto session | Deletes crypto sessions (IPSec and IKE SAs).                                                                        |

## Configuration Examples for IP Security VPN Monitoring

This section provides the following configuration example:

- [show crypto session Command Output: Examples, page 6](#)

### show crypto session Command Output: Examples

The following is sample output for the **show crypto session** output without the **detail** keyword:

```
Router# show crypto session

Crypto session current status

Interface: FastEthernet0/1
Session status: UP-ACTIVE
Peer: 172.0.0.2/500
 IKE SA: local 172.0.0.1/500 remote 172.0.0.2/500 Active
 IPSEC FLOW: permit ip 10.10.10.0/255.255.255.0 10.30.30.0/255.255.255.0
 Active SAs: 2, origin: crypto map
```

The following is sample output using the **show crypto session command and the detail** keyword:

```
Router# show crypto session detail

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.1.1.3 port 500 fvrf: (none) ivrf: (none)
 Desc: this is my peer at 10.1.1.3:500 Green
```

```
Phase1_id: 10.1.1.3
IKE SA: local 10.1.1.4/500 remote 10.1.1.3/500 Active
 Capabilities:(none) connid:3 lifetime:22:03:24
IPSEC FLOW: permit 47 host 10.1.1.4 host 10.1.1.3
 Active SAs: 0, origin: crypto map
 Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
 Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0
IPSEC FLOW: permit ip host 10.1.1.4 host 10.1.1.3
 Active SAs: 4, origin: crypto map
 Inbound: #pkts dec'ed 4 drop 0 life (KB/Sec) 4605665/2949
 Outbound: #pkts enc'ed 4 drop 1 life (KB/Sec) 4605665/2949
```

## Additional References

The following sections provide references related to IP Security VPN Monitoring.

## Related Documents

| Related Topic                    | Document Title                                                                                            |
|----------------------------------|-----------------------------------------------------------------------------------------------------------|
| IP security, encryption, and IKE | <a href="#">“IP Security and Encryption”</a> section of the <i>Cisco IOS Security Configuration Guide</i> |
| Security commands                | <a href="#">Cisco IOS Security Command Reference</a> , Release 12.3 T                                     |

## Standards

| Standards                                                   | Title |
|-------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature. | —     |

## MIBs

| MIBs                                                   | MIBs Link                                                                                                                                                                                                                  |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                                   | Title |
|--------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following commands are introduced or modified in the feature or features

- **clear crypto session**



- **description (isakmp peer)**
- **show crypto isakmp peer**
- **show crypto session**

For information about these commands, see the Cisco IOS Security Command Reference at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





# IPsec and IKE MIB Support for Cisco VRF-Aware IPsec

The IPsec and IKE MIB Support for Cisco VRF-Aware IPsec feature provides manageability of Virtual Private Network routing and forwarding- (VRF-) aware IP security (IPsec) using MIBs. The benefit of this feature is that VRF-aware IPsec MIBs provide the granular details of IPsec statistics and performance metrics on a VRF basis.

## History for the IPsec and IKE MIB Support for Cisco VRF-Aware IPsec Feature

| Release  | Modification                 |
|----------|------------------------------|
| 12.4(4)T | This feature was introduced. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for IPsec and IKE MIB Support for Cisco VRF-Aware IPsec, page 2](#)
- [Information About IPsec and IKE MIB Support for Cisco VRF-Aware IPsec, page 2](#)
- [How to Configure IPsec and IKE MIB Support for Cisco VRF-Aware IPsec, page 2](#)
- [Configuration Examples for IPsec and IKE MIB Support for Cisco VRF-Aware IPsec, page 3](#)
- [Additional References, page 15](#)
- [Command Reference, page 17](#)



**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

# Prerequisites for IPsec and IKE MIB Support for Cisco VRF-Aware IPsec

- You should be familiar with configuring Simple Network Management Protocol (SNMP).

## Information About IPsec and IKE MIB Support for Cisco VRF-Aware IPsec

To configure IPsec and MIB Support for Cisco VRF-Aware IPsec, you should understand the following concepts:

- [MIBs Supported by the IPsec and IKE MIB Support for Cisco VRF-Aware IPsec Feature, page 2](#)

## MIBs Supported by the IPsec and IKE MIB Support for Cisco VRF-Aware IPsec Feature

The following MIBs are supported by the IPsec and IKE MIB Support for Cisco VRF-Aware IPsec feature:

- CISCO-IPSEC-FLOW-MONITOR-MIB
- CISCO-IPSEC-MIB
- The CISCO-IPSEC-POLICY-MAP-MIB continues to be supported. However, because this MIB applies to the entire router rather than to a specific VPN VRF instance, it is not VRF aware; therefore, polling of the object identifiers (OIDs) that belong to this MIB is accomplished with respect to the global VRF context.

## How to Configure IPsec and IKE MIB Support for Cisco VRF-Aware IPsec

No special configuration is needed for this feature. The SNMP framework can be used to manage VRF-aware IPsec using MIBs. See the section “[Configuration Examples for IPsec and IKE MIB Support for Cisco VRF-Aware IPsec](#)” for a reference to configuring SNMP.

The following section provides information about troubleshooting this feature:

- [How to Troubleshoot the IPsec and IKE MIB Support for Cisco VRF-Aware IPsec Feature, page 2](#)

## How to Troubleshoot the IPsec and IKE MIB Support for Cisco VRF-Aware IPsec Feature

The following **debug crypto mib** command and keywords may be used to display information about the IPsec and Internet Key Exchange (IKE) MIB as it relates to Cisco VRF-aware IPsec.

## SUMMARY STEPS

1. `enable`
2. `debug crypto mib detail`
3. `debug crypto mib error`

## DETAILED STEPS

|        | Command or Action                                                                                     | Purpose                                                                                                                                                                                                                                                                  |
|--------|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> <code>enable</code>                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                       |
| Step 2 | <b>debug crypto mib detail</b><br><br><b>Example:</b><br>Router# <code>debug crypto mib detail</code> | Displays different events as they occur in the IPsec MIB subsystem. <ul style="list-style-type: none"> <li>• Due consideration should be given to enabling <b>debug crypto mib detail</b> because the output for the <b>detail</b> keyword can be quite long.</li> </ul> |
| Step 3 | <b>debug crypto mib error</b><br><br><b>Example:</b><br>Router# <code>debug crypto mib error</code>   | Displays error events in the MIB agent.                                                                                                                                                                                                                                  |

# Configuration Examples for IPsec and IKE MIB Support for Cisco VRF-Aware IPsec

This section includes the following example:

- [Configuration That Has Two VRFs: Examples, page 3](#)

## Configuration That Has Two VRFs: Examples

The following output example is for a typical hub configuration that has two VRFs. The output is what you would see if you were to poll for the IPsec security association (SA). Router 3745b is the VRF-aware router.

### Two VRFs Configured

The following output shows that two VRFs have been configured (vrf1 and vrf2).

```
Router3745b# show running-config

Building configuration...

Current configuration : 6567 bytes
!
version 12.4
```

```

service timestamps debug datetime msec localtime
service timestamps log uptime
no service password-encryption
!
hostname ipsecf-3745b
!
boot-start-marker
boot-end-marker
!
no logging console
enable password lab
!
no aaa new-model
!
resource policy
!
memory-size iomem 5
clock timezone PST -8
clock summer-time PDT recurring
ip subnet-zero
ip cef
!
!
ip vrf vrf1
 rd 1:101
 context vrf-vrf1-context
 route-target export 1:101
 route-target import 1:101
!
ip vrf vrf2
 rd 2:101
 context vrf-vrf2-context
 route-target export 2:101
 route-target import 2:101
!
no ip domain lookup
!
!
crypto keyring vrf1-1 vrf vrf1
 pre-shared-key address 10.1.1.1 255.255.255.0 key vrf1-1
crypto keyring vrf2-1 vrf vrf2
 pre-shared-key address 10.1.2.1 255.255.255.0 key vrf2-1
!
!
crypto isakmp policy 1
 authentication pre-share
!
crypto isakmp policy 50
 authentication pre-share
crypto isakmp key global1-1 address 10.1.151.1
crypto isakmp key global2-1 address 10.1.152.1
crypto isakmp profile vrf1-1
 keyring vrf1-1
 match identity address 10.1.1.1 255.255.255.255 vrf1
crypto isakmp profile vrf2-1
 keyring vrf2-1
 match identity address 10.1.2.1 255.255.255.255 vrf2
!
crypto ipsec security-association lifetime kilobytes 99000
crypto ipsec security-association lifetime seconds 5000
!
crypto ipsec transform-set tset ah-sha-hmac esp-des esp-sha-hmac
!
crypto map global1-1 10 ipsec-isakmp

```

```
 set peer 10.1.151.1
 set transform-set tset
 match address 151
 !
crypto map global2-1 10 ipsec-isakmp
 set peer 10.1.152.1
 set transform-set tset
 match address 152
 !
crypto map vrf1-1 10 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set tset
 set isakmp-profile vrf1-1
 match address 101
 !
crypto map vrf2-1 10 ipsec-isakmp
 set peer 10.1.2.1
 set transform-set tset
 set isakmp-profile vrf2-1
 match address 102
 !
 !
interface FastEthernet0/0
 ip address 10.1.38.25 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
 !
interface Serial0/0
 no ip address
 shutdown
 clock rate 2000000
 !
interface FastEthernet0/1
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
 !
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
 !
interface Serial1/0
 no ip address
 encapsulation frame-relay
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 no keepalive
 serial restart-delay 0
 clock rate 128000
 no frame-relay inverse-arp
 !
interface Serial1/0.1 point-to-point
 ip vrf forwarding vrf1
 ip address 10.3.1.1 255.255.255.0
 no ip route-cache
 frame-relay interface-dlci 21
 !
interface Serial1/0.2 point-to-point
 ip vrf forwarding vrf2
```

```

ip address 10.3.2.1 255.255.255.0
no ip route-cache
frame-relay interface-dlci 22
!
interface Serial1/0.151 point-to-point
ip address 10.7.151.1 255.255.255.0
no ip route-cache
frame-relay interface-dlci 151
!
interface Serial1/0.152 point-to-point
ip address 10.7.152.1 255.255.255.0
no ip route-cache
frame-relay interface-dlci 152
!
interface Serial1/1
no ip address
no ip mroute-cache
shutdown
serial restart-delay 0
!
interface Serial1/2
no ip address
encapsulation frame-relay
no ip route-cache cef
no ip route-cache
no ip mroute-cache
no keepalive
serial restart-delay 0
no frame-relay inverse-arp
!
interface Serial1/2.1 point-to-point
ip vrf forwarding vrf1
ip address 10.1.1.2 255.255.255.0
no ip route-cache
frame-relay interface-dlci 21
crypto map vrf1-1
!
interface Serial1/2.2 point-to-point
ip vrf forwarding vrf2
ip address 10.1.2.2 255.255.255.0
no ip route-cache
frame-relay interface-dlci 22
crypto map vrf2-1
!
interface Serial1/2.151 point-to-point
ip address 10.5.151.2 255.255.255.0
no ip route-cache
frame-relay interface-dlci 151
crypto map global1-1
!
interface Serial1/2.152 point-to-point
ip address 10.5.152.2 255.255.255.0
no ip route-cache
frame-relay interface-dlci 152
crypto map global2-1
!
interface Serial1/3
no ip address
no ip mroute-cache
shutdown
serial restart-delay 0
!
ip default-gateway 10.1.38.1
ip classless

```



```

ip route 10.1.1.6 255.255.255.255 10.1.151.1
ip route 10.2.1.6 255.255.255.255 10.1.152.1
ip route 10.6.2.1 255.255.255.255 10.7.151.2
ip route 10.6.2.2 255.255.255.255 10.7.152.2
ip route 172.19.216.110 255.255.255.255 FastEthernet0/0
ip route vrf vrf1 10.20.1.1 255.255.255.255 10.1.1.1
ip route vrf vrf1 10.22.1.1 255.255.255.255 10.30.1.1
ip route vrf vrf2 10.20.2.1 255.255.255.255 10.1.2.1
ip route vrf vrf2 10.22.2.1 255.255.255.255 10.30.1.2
!
!
ip http server
no ip http secure-server
!
ip access-list standard vrf-vrf1-context
ip access-list standard vrf-vrf2-context
!
access-list 101 permit ip host 10.22.1.1 host 10.20.1.1
access-list 102 permit ip host 10.22.2.1 host 10.20.2.1
access-list 151 permit ip host 10.6.2.1 host 10.1.1.6
access-list 152 permit ip host 10.6.2.2 host 10.2.1.6
snmp-server group abc1 v2c context vrf-vrf1-context read view_vrf1 notify
*tv.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.F access vrf-vrf1-context
snmp-server group abc2 v2c context vrf-vrf2-context read view_vrf2 notify
*tv.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.F access vrf-vrf2-context
snmp-server view view_vrf1 iso included
snmp-server view view_vrf2 iso included
snmp-server community abc1 RW
snmp-server community global1 RW
snmp-server community abc2 RW
snmp-server community global2 RW
snmp-server enable traps tty
snmp-server enable traps config
snmp-server host 172.19.216.110 version 2c abc1
snmp-server host 172.19.216.110 vrf vrf1 version 2c abc1 udp-port 2001 ipsec isakmp
snmp-server host 172.19.216.110 version 2c abc2
snmp-server host 172.19.216.110 vrf vrf2 version 2c abc2 udp-port 2002 ipsec isakmp
snmp-server context vrf-vrf1-context
snmp-server context vrf-vrf2-context
!
!
snmp mib community-map abc1 context vrf-vrf1-context
snmp mib community-map abc2 context vrf-vrf2-context
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
!
webvpn context Default_context
 ssl authenticate verify all
!
 no inservice
!
!
end

```

**Both VRFs Cleared**

The following output, for abc1 and abc2, shows that both VRFs have been “cleared” to ensure that all the counters are initialized to a known value.

The following output shows that VRF abc1 has been cleared:

```

orcas:2> setenv SR_MGR_CONF /users/green1
orcas:3> setenv SR_UTIL_SNMP_VERSION v2c
orcas:5> setenv SR_UTIL_COMMUNITY abc1
orcas:6> setenv SR_MGR_CONF_DIR /users/green1

orcas:7> /auto/sw/packages/snmpd/10.14.2.0/solaris2bin/getmany -v2c 10.1.38.25
cipSecMIBObjects

cipSecMibLevel.0 = 1
cikeGlobalActiveTunnels.0 = 0
cikeGlobalPreviousTunnels.0 = 0
cikeGlobalInOctets.0 = 0
cikeGlobalInPkts.0 = 0
cikeGlobalInDropPkts.0 = 0
cikeGlobalInNotifys.0 = 0
cikeGlobalInP2Exchgs.0 = 0
cikeGlobalInP2ExchgInvalids.0 = 0
cikeGlobalInP2ExchgRejects.0 = 0
cikeGlobalInP2SaDelRequests.0 = 0
cikeGlobalOutOctets.0 = 0
cikeGlobalOutPkts.0 = 0
cikeGlobalOutDropPkts.0 = 0
cikeGlobalOutNotifys.0 = 0
cikeGlobalOutP2Exchgs.0 = 0
cikeGlobalOutP2ExchgInvalids.0 = 0
cikeGlobalOutP2ExchgRejects.0 = 0
cikeGlobalOutP2SaDelRequests.0 = 0
cikeGlobalInitTunnels.0 = 0
cikeGlobalInitTunnelFails.0 = 0
cikeGlobalRespTunnelFails.0 = 0
cikeGlobalSysCapFails.0 = 0
cikeGlobalAuthFails.0 = 0
cikeGlobalDecryptFails.0 = 0
cikeGlobalHashValidFails.0 = 0
cikeGlobalNoSaFails.0 = 0
cipSecGlobalActiveTunnels.0 = 0
cipSecGlobalPreviousTunnels.0 = 0
cipSecGlobalInOctets.0 = 0
cipSecGlobalHcInOctets.0 = 0x00
cipSecGlobalInOctWraps.0 = 0
cipSecGlobalInDecompOctets.0 = 0
cipSecGlobalHcInDecompOctets.0 = 0x00
cipSecGlobalInDecompOctWraps.0 = 0
cipSecGlobalInPkts.0 = 0
cipSecGlobalInDrops.0 = 0
cipSecGlobalInReplayDrops.0 = 0
cipSecGlobalInAuths.0 = 0
cipSecGlobalInAuthFails.0 = 0
cipSecGlobalInDecrypts.0 = 0
cipSecGlobalInDecryptFails.0 = 0
cipSecGlobalOutOctets.0 = 0
cipSecGlobalHcOutOctets.0 = 0x00
cipSecGlobalOutOctWraps.0 = 0
cipSecGlobalOutUncompOctets.0 = 0
cipSecGlobalHcOutUncompOctets.0 = 0x00
cipSecGlobalOutUncompOctWraps.0 = 0
cipSecGlobalOutPkts.0 = 0
cipSecGlobalOutDrops.0 = 0

```

```

cipSecGlobalOutAuths.0 = 0
cipSecGlobalOutAuthFails.0 = 0
cipSecGlobalOutEncrypts.0 = 0
cipSecGlobalOutEncryptFails.0 = 0
cipSecGlobalProtocolUseFails.0 = 0
cipSecGlobalNoSaFails.0 = 0
cipSecGlobalSysCapFails.0 = 0
cipSecHistTableSize.0 = 200
cipSecHistCheckPoint.0 = ready(1)
cipSecFailTableSize.0 = 200
cipSecTrapCntlIkeTunnelStart.0 = enabled(1)
cipSecTrapCntlIkeTunnelStop.0 = enabled(1)
cipSecTrapCntlIkeSysFailure.0 = disabled(2)
cipSecTrapCntlIkeCertCrlFailure.0 = disabled(2)
cipSecTrapCntlIkeProtocolFail.0 = disabled(2)
cipSecTrapCntlIkeNoSa.0 = disabled(2)
cipSecTrapCntlIpSecTunnelStart.0 = enabled(1)
cipSecTrapCntlIpSecTunnelStop.0 = enabled(1)
cipSecTrapCntlIpSecSysFailure.0 = disabled(2)
cipSecTrapCntlIpSecSetUpFailure.0 = disabled(2)
cipSecTrapCntlIpSecEarlyTunTerm.0 = disabled(2)
cipSecTrapCntlIpSecProtocolFail.0 = disabled(2)
cipSecTrapCntlIpSecNoSa.0 = disabled(2)

```

The following output shows that VRF abc2 has been cleared:

```

orcas:8> setenv SR_UTIL_COMMUNITY abc2
orcas:9> /auto/sw/packages/snmpr/14.2.0.0/solaris2bin/getmany -v2c 10.1.38.25
cipSecMIBObjects
cipSecMibLevel.0 = 1
cikeGlobalActiveTunnels.0 = 0
cikeGlobalPreviousTunnels.0 = 0
cikeGlobalInOctets.0 = 0
cikeGlobalInPkts.0 = 0
cikeGlobalInDropPkts.0 = 0
cikeGlobalInNotifys.0 = 0
cikeGlobalInP2Exchgs.0 = 0
cikeGlobalInP2ExchgInvalids.0 = 0
cikeGlobalInP2ExchgRejects.0 = 0
cikeGlobalInP2SaDelRequests.0 = 0
cikeGlobalOutOctets.0 = 0
cikeGlobalOutPkts.0 = 0
cikeGlobalOutDropPkts.0 = 0
cikeGlobalOutNotifys.0 = 0
cikeGlobalOutP2Exchgs.0 = 0
cikeGlobalOutP2ExchgInvalids.0 = 0
cikeGlobalOutP2ExchgRejects.0 = 0
cikeGlobalOutP2SaDelRequests.0 = 0
cikeGlobalInitTunnels.0 = 0
cikeGlobalInitTunnelFails.0 = 0
cikeGlobalRespTunnelFails.0 = 0
cikeGlobalSysCapFails.0 = 0
cikeGlobalAuthFails.0 = 0
cikeGlobalDecryptFails.0 = 0
cikeGlobalHashValidFails.0 = 0
cikeGlobalNoSaFails.0 = 0
cipSecGlobalActiveTunnels.0 = 0
cipSecGlobalPreviousTunnels.0 = 0
cipSecGlobalInOctets.0 = 0
cipSecGlobalHcInOctets.0 = 0x00
cipSecGlobalInOctWraps.0 = 0
cipSecGlobalInDecompOctets.0 = 0
cipSecGlobalHcInDecompOctets.0 = 0x00
cipSecGlobalInDecompOctWraps.0 = 0

```

```

cipSecGlobalInPkts.0 = 0
cipSecGlobalInDrops.0 = 0
cipSecGlobalInReplayDrops.0 = 0
cipSecGlobalInAuths.0 = 0
cipSecGlobalInAuthFails.0 = 0
cipSecGlobalInDecrypts.0 = 0
cipSecGlobalInDecryptFails.0 = 0
cipSecGlobalOutOctets.0 = 0
cipSecGlobalHcOutOctets.0 = 0x00
cipSecGlobalOutOctWraps.0 = 0
cipSecGlobalOutUncompOctets.0 = 0
cipSecGlobalHcOutUncompOctets.0 = 0x00
cipSecGlobalOutUncompOctWraps.0 = 0
cipSecGlobalOutPkts.0 = 0
cipSecGlobalOutDrops.0 = 0
cipSecGlobalOutAuths.0 = 0
cipSecGlobalOutAuthFails.0 = 0
cipSecGlobalOutEncrypts.0 = 0
cipSecGlobalOutEncryptFails.0 = 0
cipSecGlobalProtocolUseFails.0 = 0
cipSecGlobalNoSaFails.0 = 0
cipSecGlobalSysCapFails.0 = 0
cipSecHistTableSize.0 = 200
cipSecHistCheckPoint.0 = ready(1)
cipSecFailTableSize.0 = 200
cipSecTrapCntlIkeTunnelStart.0 = enabled(1)
cipSecTrapCntlIkeTunnelStop.0 = enabled(1)
cipSecTrapCntlIkeSysFailure.0 = disabled(2)
cipSecTrapCntlIkeCertCrlFailure.0 = disabled(2)
cipSecTrapCntlIkeProtocolFail.0 = disabled(2)
cipSecTrapCntlIkeNoSa.0 = disabled(2)
cipSecTrapCntlIpSecTunnelStart.0 = enabled(1)
cipSecTrapCntlIpSecTunnelStop.0 = enabled(1)
cipSecTrapCntlIpSecSysFailure.0 = disabled(2)
cipSecTrapCntlIpSecSetUpFailure.0 = disabled(2)
cipSecTrapCntlIpSecEarlyTunTerm.0 = disabled(2)
cipSecTrapCntlIpSecProtocolFail.0 = disabled(2)
cipSecTrapCntlIpSecNoSa.0 = disabled(2)
orcas:10>
orcas:10>
orcas:10>

```

### VRF abc1 Pinged

The following output shows that VRF abc1 has been pinged:

Router3745a# **ping**

```

Protocol [ip]:
Target IP address: 10.22.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.20.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.22.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.20.1.1

```

**VRF abc1 Polled**

Polling VRF abc1 results in the following output:

**Note**

After the ping, the counters should show some nonzero values.

```

orcas:10>
orcas:12> setenv SR_UTIL_COMMUNITY abc1
orcas:13> /auto/sw/packages/snmpd/10.14.2.0/solaris2bin/getmany -v2c 10.1.38.25
cipSecMIBObjects
cipSecMibLevel.0 = 1
cikeGlobalActiveTunnels.0 = 1
cikeGlobalPreviousTunnels.0 = 0
cikeGlobalInOctets.0 = 336
cikeGlobalInPkts.0 = 2
cikeGlobalInDropPkts.0 = 0
cikeGlobalInNotifys.0 = 1
cikeGlobalInP2Exchgs.0 = 2
cikeGlobalInP2ExchgInvalids.0 = 0
cikeGlobalInP2ExchgRejects.0 = 0
cikeGlobalInP2SaDelRequests.0 = 0
cikeGlobalOutOctets.0 = 344
cikeGlobalOutPkts.0 = 2
cikeGlobalOutDropPkts.0 = 0
cikeGlobalOutNotifys.0 = 0
cikeGlobalOutP2Exchgs.0 = 1
cikeGlobalOutP2ExchgInvalids.0 = 0
cikeGlobalOutP2ExchgRejects.0 = 0
cikeGlobalOutP2SaDelRequests.0 = 0
cikeGlobalInitTunnels.0 = 0
cikeGlobalInitTunnelFails.0 = 0
cikeGlobalRespTunnelFails.0 = 0
cikeGlobalSysCapFails.0 = 0
cikeGlobalAuthFails.0 = 0
cikeGlobalDecryptFails.0 = 0
cikeGlobalHashValidFails.0 = 0
cikeGlobalNoSaFails.0 = 0
cikePeerLocalAddr.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.50.1.15.48.49.48.46.48.48
.49.46.48.48.49.46.48.48.49.1 = 0a 01 01 02
cikePeerRemoteAddr.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.50.1.15.48.49.48.46.48.4
8.49.46.48.48.49.46.48.48.49.1 = 0a 01 01 01
cikePeerActiveTime.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.50.1.15.48.49.48.46.48.4
8.49.46.48.48.49.46.48.48.49.1 = 13743
cikePeerActiveTunnelIndex.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.50.1.15.48.49.48.
46.48.48.49.46.48.48.49.46.48.48.49.1 = 1
cikeTunLocalType.1 = ipAddrPeer(1)
cikeTunLocalValue.1 = 010.001.001.002
cikeTunLocalAddr.1 = 0a 01 01 02
cikeTunLocalName.1 = ipsecf-3745b
cikeTunRemoteType.1 = ipAddrPeer(1)
cikeTunRemoteValue.1 = 010.001.001.001
cikeTunRemoteAddr.1 = 0a 01 01 01
cikeTunRemoteName.1 =
cikeTunNegoMode.1 = main(1)
cikeTunDiffHellmanGrp.1 = dhGroup1(2)
cikeTunEncryptAlgo.1 = des(2)
cikeTunHashAlgo.1 = sha(3)
cikeTunAuthMethod.1 = preSharedKey(2)
cikeTunLifeTime.1 = 86400
cikeTunActiveTime.1 = 13752
cikeTunSaRefreshThreshold.1 = 0
cikeTunTotalRefreshes.1 = 0

```

```

cikeTunInOctets.1 = 336
cikeTunInPkts.1 = 2
cikeTunInDropPkts.1 = 0
cikeTunInNotifys.1 = 1
cikeTunInP2Exchgs.1 = 2
cikeTunInP2ExchgInvalids.1 = 0
cikeTunInP2ExchgRejects.1 = 0
cikeTunInP2SaDelRequests.1 = 0
cikeTunOutOctets.1 = 344
cikeTunOutPkts.1 = 2
cikeTunOutDropPkts.1 = 0
cikeTunOutNotifys.1 = 0
cikeTunOutP2Exchgs.1 = 1
cikeTunOutP2ExchgInvalids.1 = 0
cikeTunOutP2ExchgRejects.1 = 0
cikeTunOutP2SaDelRequests.1 = 0
cikeTunStatus.1 = active(1)
cikePeerCorrIpSecTunIndex.1.15.48.49.48.46.48.48.49.46.48.48.49.46.48.48.50.1.15.48.49.48.
46.48.48.49.46.48.48.49.46.48.48.49.1.1 = 1
cipSecGlobalActiveTunnels.0 = 1
cipSecGlobalPreviousTunnels.0 = 0
cipSecGlobalInOctets.0 = 400
cipSecGlobalHcInOctets.0 = 0x0190
cipSecGlobalInOctWraps.0 = 0
cipSecGlobalInDecompOctets.0 = 400
cipSecGlobalHcInDecompOctets.0 = 0x0190
cipSecGlobalInDecompOctWraps.0 = 0
cipSecGlobalInPkts.0 = 4
cipSecGlobalInDrops.0 = 0
cipSecGlobalInReplayDrops.0 = 0
cipSecGlobalInAuths.0 = 4
cipSecGlobalInAuthFails.0 = 0
cipSecGlobalInDecrypts.0 = 4
cipSecGlobalInDecryptFails.0 = 0
cipSecGlobalOutOctets.0 = 704
cipSecGlobalHcOutOctets.0 = 0x02c0
cipSecGlobalOutOctWraps.0 = 0
cipSecGlobalOutUncompOctets.0 = 704
cipSecGlobalHcOutUncompOctets.0 = 0x02c0
cipSecGlobalOutUncompOctWraps.0 = 0
cipSecGlobalOutPkts.0 = 4
cipSecGlobalOutDrops.0 = 0
cipSecGlobalOutAuths.0 = 4
cipSecGlobalOutAuthFails.0 = 0
cipSecGlobalOutEncrypts.0 = 4
cipSecGlobalOutEncryptFails.0 = 0
cipSecGlobalProtocolUseFails.0 = 0
cipSecGlobalNoSaFails.0 = 0
cipSecGlobalSysCapFails.0 = 0
cipSecTunIkeTunnelIndex.1 = 1
cipSecTunIkeTunnelAlive.1 = true(1)
cipSecTunLocalAddr.1 = 0a 01 01 02
cipSecTunRemoteAddr.1 = 0a 01 01 01
cipSecTunKeyType.1 = ike(1)
cipSecTunEncapMode.1 = tunnel(1)
cipSecTunLifeSize.1 = 99000
cipSecTunLifeTime.1 = 5000
cipSecTunActiveTime.1 = 13749
cipSecTunSaLifeSizeThreshold.1 = 64
cipSecTunSaLifeTimeThreshold.1 = 10
cipSecTunTotalRefreshes.1 = 0
cipSecTunExpiredSaInstances.1 = 0
cipSecTunCurrentSaInstances.1 = 4
cipSecTunInSaDiffHellmanGrp.1 = dhGroup1(2)

```

```

cipSecTunInSaEncryptAlgo.1 = des(2)
cipSecTunInSaAhAuthAlgo.1 = hmacSha(3)
cipSecTunInSaEspAuthAlgo.1 = hmacSha(3)
cipSecTunInSaDecompAlgo.1 = none(1)
cipSecTunOutSaDiffHellmanGrp.1 = dhGroup1(2)
cipSecTunOutSaEncryptAlgo.1 = des(2)
cipSecTunOutSaAhAuthAlgo.1 = hmacSha(3)
cipSecTunOutSaEspAuthAlgo.1 = hmacSha(3)
cipSecTunOutSaCompAlgo.1 = none(1)
cipSecTunInOctets.1 = 400
cipSecTunHcInOctets.1 = 0x0190
cipSecTunInOctWraps.1 = 0
cipSecTunInDecompOctets.1 = 400
cipSecTunHcInDecompOctets.1 = 0x0190
cipSecTunInDecompOctWraps.1 = 0
cipSecTunInPkts.1 = 4
cipSecTunInDropPkts.1 = 0
cipSecTunInReplayDropPkts.1 = 0
cipSecTunInAuths.1 = 4
cipSecTunInAuthFails.1 = 0
cipSecTunInDecrypts.1 = 4
cipSecTunInDecryptFails.1 = 0
cipSecTunOutOctets.1 = 704
cipSecTunHcOutOctets.1 = 0x02c0
cipSecTunOutOctWraps.1 = 0
cipSecTunOutUncompOctets.1 = 704
cipSecTunHcOutUncompOctets.1 = 0x02c0
cipSecTunOutUncompOctWraps.1 = 0
cipSecTunOutPkts.1 = 4
cipSecTunOutDropPkts.1 = 0
cipSecTunOutAuths.1 = 4
cipSecTunOutAuthFails.1 = 0
cipSecTunOutEncrypts.1 = 4
cipSecTunOutEncryptFails.1 = 0
cipSecTunStatus.1 = active(1)
cipSecEndPtLocalName.1.1 =
cipSecEndPtLocalType.1.1 = singleIpAddr(1)
cipSecEndPtLocalAddr1.1.1 = 16 01 01 01
cipSecEndPtLocalAddr2.1.1 = 16 01 01 01
cipSecEndPtLocalProtocol.1.1 = 0
cipSecEndPtLocalPort.1.1 = 0
cipSecEndPtRemoteName.1.1 =
cipSecEndPtRemoteType.1.1 = singleIpAddr(1)
cipSecEndPtRemoteAddr1.1.1 = 14 01 01 01
cipSecEndPtRemoteAddr2.1.1 = 14 01 01 01
cipSecEndPtRemoteProtocol.1.1 = 0
cipSecEndPtRemotePort.1.1 = 0
cipSecSpiDirection.1.1 = in(1)
cipSecSpiDirection.1.2 = out(2)
cipSecSpiDirection.1.3 = in(1)
cipSecSpiDirection.1.4 = out(2)
cipSecSpiValue.1.1 = 3891970674
cipSecSpiValue.1.2 = 1963217493
cipSecSpiValue.1.3 = 3691920464
cipSecSpiValue.1.4 = 3458912974
cipSecSpiProtocol.1.1 = ah(1)
cipSecSpiProtocol.1.2 = ah(1)
cipSecSpiProtocol.1.3 = esp(2)
cipSecSpiProtocol.1.4 = esp(2)
cipSecSpiStatus.1.1 = active(1)
cipSecSpiStatus.1.2 = active(1)
cipSecSpiStatus.1.3 = active(1)
cipSecSpiStatus.1.4 = active(1)
cipSecHistTableSize.0 = 200

```

```

cipSecHistCheckPoint.0 = ready(1)
cipSecFailTableSize.0 = 200
cipSecTrapCntlIkeTunnelStart.0 = enabled(1)
cipSecTrapCntlIkeTunnelStop.0 = enabled(1)
cipSecTrapCntlIkeSysFailure.0 = disabled(2)
cipSecTrapCntlIkeCertCrlFailure.0 = disabled(2)
cipSecTrapCntlIkeProtocolFail.0 = disabled(2)
cipSecTrapCntlIkeNoSa.0 = disabled(2)
cipSecTrapCntlIpSecTunnelStart.0 = enabled(1)
cipSecTrapCntlIpSecTunnelStop.0 = enabled(1)
cipSecTrapCntlIpSecSysFailure.0 = disabled(2)
cipSecTrapCntlIpSecSetUpFailure.0 = disabled(2)
cipSecTrapCntlIpSecEarlyTunTerm.0 = disabled(2)
cipSecTrapCntlIpSecProtocolFail.0 = disabled(2)
cipSecTrapCntlIpSecNoSa.0 = disabled(2)
orcas:14>
orcas:14>
orcas:14>

```

### VRF abc2 Polled

Polling VRF abc2 results in the following output:



#### Note

The ping was completed for VRF abc1 only. Therefore, the counters of VRF abc2 should remain in the initialized state.

```

setenv SR_UTIL_COMMUNITY abc2
orcas:15>
orcas:15> /auto/sw/packages/snmpr/10.14.2.0/solaris2bin/getmany -v2c 10.1.38.25
cipSecMIBObjects
cipSecMibLevel.0 = 1
cikeGlobalActiveTunnels.0 = 0
cikeGlobalPreviousTunnels.0 = 0
cikeGlobalInOctets.0 = 0
cikeGlobalInPkts.0 = 0
cikeGlobalInDropPkts.0 = 0
cikeGlobalInNotifys.0 = 0
cikeGlobalInP2Exchgs.0 = 0
cikeGlobalInP2ExchgInvalids.0 = 0
cikeGlobalInP2ExchgRejects.0 = 0
cikeGlobalInP2SaDelRequests.0 = 0
cikeGlobalOutOctets.0 = 0
cikeGlobalOutPkts.0 = 0
cikeGlobalOutDropPkts.0 = 0
cikeGlobalOutNotifys.0 = 0
cikeGlobalOutP2Exchgs.0 = 0
cikeGlobalOutP2ExchgInvalids.0 = 0
cikeGlobalOutP2ExchgRejects.0 = 0
cikeGlobalOutP2SaDelRequests.0 = 0
cikeGlobalInitTunnels.0 = 0
cikeGlobalInitTunnelFails.0 = 0
cikeGlobalRespTunnelFails.0 = 0
cikeGlobalSysCapFails.0 = 0
cikeGlobalAuthFails.0 = 0
cikeGlobalDecryptFails.0 = 0
cikeGlobalHashValidFails.0 = 0
cikeGlobalNoSaFails.0 = 0
cipSecGlobalActiveTunnels.0 = 0
cipSecGlobalPreviousTunnels.0 = 0
cipSecGlobalInOctets.0 = 0
cipSecGlobalHcInOctets.0 = 0x00
cipSecGlobalInOctWraps.0 = 0

```



```

cipSecGlobalInDecompOctets.0 = 0
cipSecGlobalHcInDecompOctets.0 = 0x00
cipSecGlobalInDecompOctWraps.0 = 0
cipSecGlobalInPkts.0 = 0
cipSecGlobalInDrops.0 = 0
cipSecGlobalInReplayDrops.0 = 0
cipSecGlobalInAuths.0 = 0
cipSecGlobalInAuthFails.0 = 0
cipSecGlobalInDecrypts.0 = 0
cipSecGlobalInDecryptFails.0 = 0
cipSecGlobalOutOctets.0 = 0
cipSecGlobalHcOutOctets.0 = 0x00
cipSecGlobalOutOctWraps.0 = 0
cipSecGlobalOutUncompOctets.0 = 0
cipSecGlobalHcOutUncompOctets.0 = 0x00
cipSecGlobalOutUncompOctWraps.0 = 0
cipSecGlobalOutPkts.0 = 0
cipSecGlobalOutDrops.0 = 0
cipSecGlobalOutAuths.0 = 0
cipSecGlobalOutAuthFails.0 = 0
cipSecGlobalOutEncrypts.0 = 0
cipSecGlobalOutEncryptFails.0 = 0
cipSecGlobalProtocolUseFails.0 = 0
cipSecGlobalNoSaFails.0 = 0
cipSecGlobalSysCapFails.0 = 0
cipSecHistTableSize.0 = 200
cipSecHistCheckPoint.0 = ready(1)
cipSecFailTableSize.0 = 200
cipSecTrapCntlIkeTunnelStart.0 = enabled(1)
cipSecTrapCntlIkeTunnelStop.0 = enabled(1)
cipSecTrapCntlIkeSysFailure.0 = disabled(2)
cipSecTrapCntlIkeCertCrlFailure.0 = disabled(2)
cipSecTrapCntlIkeProtocolFail.0 = disabled(2)
cipSecTrapCntlIkeNoSa.0 = disabled(2)
cipSecTrapCntlIpSecTunnelStart.0 = enabled(1)
cipSecTrapCntlIpSecTunnelStop.0 = enabled(1)
cipSecTrapCntlIpSecSysFailure.0 = disabled(2)
cipSecTrapCntlIpSecSetUpFailure.0 = disabled(2)
cipSecTrapCntlIpSecEarlyTunTerm.0 = disabled(2)
cipSecTrapCntlIpSecProtocolFail.0 = disabled(2)
cipSecTrapCntlIpSecNoSa.0 = disabled(2)
orcas:16>

```

## Additional References

The following sections provide references related to the IPsec and IKE MIB Support for Cisco VRF-Aware IPsec feature.

## Related Documents

| Related Topic                    | Document Title                                                                                                            |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Cisco IOS commands by technology | <a href="#">Cisco IOS Release Command References</a> , Release 12.4T                                                      |
| Cisco IOS master commands list   | <a href="#">Cisco IOS Master Commands List</a> , Release 12.4                                                             |
| Configuring SNMP                 | The chapter “ <a href="#">Configuring SNMP Support</a> ” in the <i>Cisco IOS Network Management Configuration Guide</i> . |
| Configuring VRF-Aware IPsec      | <a href="#">VRF-Aware IPsec</a> feature module, Release 12.2(15)T                                                         |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC                                                                                                                         | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                         | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Command Reference

The following commands are introduced or modified in the feature or features

- **debug crypto mib**

For information about these commands, see the Cisco IOS Security Command Reference at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

---

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





# IPSec and Quality of Service

---

The IPSec and Quality of Service feature allows Cisco IOS quality of service (QoS) policies to be applied to IP Security (IPSec) packet flows on the basis of a QoS group that can be added to the current Internet Security Association and Key Management Protocol (ISAKMP) profile.

## Feature History for IPSec and Quality of Service

| Release  | Modification                 |
|----------|------------------------------|
| 12.3(8)T | This feature was introduced. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for IPSec and Quality of Service, page 1](#)
- [Restrictions for IPSec and Quality of Service, page 2](#)
- [Information About IPSec and Quality of Service, page 2](#)
- [How to Configure IPSec and Quality of Service, page 2](#)
- [Configuration Examples for IPSec and Quality of Service, page 4](#)
- [Additional References, page 7](#)
- [Command Reference, page 9](#)

## Prerequisites for IPSec and Quality of Service

- You should be familiar with IPSec and the concept of ISAKMP profiles.
- You should be familiar with Cisco IOS QoS.



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

# Restrictions for IPSec and Quality of Service

- This feature can be applied only via the ISAKMP profile. The limit of 128 QoS groups that exists for QoS applications applies to this feature as well.
- You can apply an IPSec QoS group only to outbound service policies.
- QoS is not supported for software encryption.

## Information About IPSec and Quality of Service

To configure the IPSec and Quality of Service feature, you should understand the following concept:

- [IPSec and Quality of Service Overview, page 2](#)

## IPSec and Quality of Service Overview

The IPSec and Quality of Service feature allows you to apply QoS policies, such as traffic policing and shaping, to IPSec-protected packets by adding a QoS group to ISAKMP profiles. After the QoS group has been added, this group value will be mapped to the same QoS group as defined in QoS class maps. Any current QoS method that makes use of this QoS group tag can be applied to IPSec packet flows. Common groupings of packet flows can have specific policy classes applied by having the IPSec QoS group made available to the QoS mechanism. Marking IPSec flows allows QoS mechanisms to be applied to classes of traffic that could provide support for such things as restricting the amount of bandwidth that is available to specific groups or devices or marking the type of service (ToS) bits on certain flows.

The application of the QoS group is applied at the ISAKMP profile level because it is the profile that can uniquely identify devices through its concept of match identity criteria. These criteria are on the basis of the Internet Key Exchange (IKE) identity that is presented by incoming IKE connections and includes such things as IP address, fully qualified domain name (FQDN), and group (that is, the virtual private network [VPN] remote client grouping). The granularity of the match identity criteria will impose the granularity of the specified QoS policy, for example, to mark all traffic belonging to the VPN client group named “Engineering” as “TOS 5”. Another example of having the granularity of a specified QoS policy imposed would be to allocate 30 percent of the bandwidth on an outbound WAN link to a specific group of remote VPN devices.

## How to Configure IPSec and Quality of Service

This section includes the following procedures:

- [Configuring IPSec and Quality of Service, page 2](#) (required)
- [Verifying IPSec and Quality of Service Sessions, page 3](#) (optional)
- [Troubleshooting Tips, page 4](#) (optional)

## Configuring IPSec and Quality of Service

To apply QoS policies to an ISAKMP profile, perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp-profile** *profile-name*
4. **qos-group** *group-number*

## DETAILED STEPS

|        | Command or Action                                                                                                                 | Purpose                                                                                                          |
|--------|-----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                    | Enters global configuration mode.                                                                                |
| Step 3 | <b>crypto isakmp-profile</b> <i>profile-number</i><br><br><b>Example:</b><br>Router (config)# crypto isakmp-profile<br>vpnprofile | Defines an ISAKMP profile, audits IPSec user sessions, and enters ISAKMP profile configuration mode.             |
| Step 4 | <b>qos-group</b> <i>group-number</i><br><br><b>Example:</b><br>Router(config-isa-prof)# qos-group 1                               | Applies a QoS group value to an ISAKMP profile.                                                                  |

## Verifying IPSec and Quality of Service Sessions

To verify your IPSec and QoS sessions, perform the following steps. The **show** commands can be used in any order or independent of each other.

## SUMMARY STEPS

1. **enable**
2. **show crypto isakmp profile**
3. **show crypto ipsec sa**

## DETAILED STEPS

|        | Command or Action                                                                              | Purpose                                                                                                          |
|--------|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>show crypto isakmp profile</b><br><br><b>Example:</b><br>Router# show crypto isakmp profile | Shows that the QoS group is applied to the profile.                                                              |
| Step 3 | <b>show crypto ipsec sa</b><br><br><b>Example:</b><br>Router# show crypto ipsec sa             | Shows that the QoS group is applied to a particular pair of IPSec security associations (SAs).                   |

## Troubleshooting Tips

If you have a problem with your IPSec and QoS sessions, ensure that you have done the following:

- Validated the application of QoS by the QoS service using the QoS-specific commands in the *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.3 T.
- Configured a QoS policy on the router that matches the same QoS group as that specified for the class map match criterion.
- Applied the service policy to the same interface to which a crypto map is applied.

## Configuration Examples for IPSec and Quality of Service

This section provides the following output examples:

- [QoS Policy Applied to Two Groups of Remote Users: Example, page 4](#)
- [show crypto isakmp profile Command: Example, page 6](#)
- [show crypto ipsec sa Command: Example, page 6](#)

## QoS Policy Applied to Two Groups of Remote Users: Example

In the following example, a specific QoS policy is applied to two groups of remote users. Two ISAKMP profiles are configured so that upon initial connection via IKE, remote users are mapped to a specific profile. From that profile, all IPSec SAs that have been created for that remote will be marked with the specific QoS group. As traffic leaves the outbound interface, the QoS service will map the IPSec set QoS group with the QoS group that is specified in the class maps that comprise the service policy that is applied on that outbound interface.

```
version 12.3
!
aaa authentication login group group radius
aaa authorization network autho local
aaa accounting update periodic 1
```



```
aaa session-id common
ip subnet-zero
!
!
ip cef
no ip domain lookup
!
class-map match-all yellow
 match qos-group 3
class-map match-all blue
 match qos-group 2
!
!
policy-map clients
 class blue
 set precedence 5
 class yellow
 set precedence 7
!
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
 lifetime 300
!
crypto isakmp keepalive 10 periodic
crypto isakmp xauth timeout 20
!
crypto isakmp client configuration group blue
 key cisco
 dns 10.2.2.2 10.2.2.3
 wins 10.6.6.6
 pool blue
 save-password
 include-local-lan
 backup-gateway corkyl.cisco.com
!
crypto isakmp client configuration group yellow
 dns 10.2.2.2 10.2.2.3
 wins 10.6.6.5
 pool yellow
!
crypto isakmp profile blue
 match identity group cisco
 client authentication list autho
 isakmp authorization list autho
 client configuration address respond
 qos-group 2
crypto isakmp profile yellow
 match identity group yellow
 match identity address 10.0.0.11 255.255.255.255
 client authentication list autho
 isakmp authorization list autho
 client configuration address respond
 qos-group 3
!
!
crypto ipsec transform-set combo ah-sha-hmac esp-3des esp-sha-hmac
crypto ipsec transform-set client esp-3des esp-sha-hmac comp-lzs
!
crypto dynamic-map mode 1
 set security-association lifetime seconds 180
```

```

set transform-set client
set isakmp-profile blue
reverse-route
crypto dynamic-map mode 2
set transform-set combo
set isakmp-profile yellow
reverse-route
!
crypto map mode 1 ipsec-isakmp dynamic mode
!
interface FastEthernet0/0
ip address 10.0.0.110 255.255.255.0
no ip redirects
no ip proxy-arp
no ip mroute-cache
duplex half
no cdp enable
crypto map mode
service-policy out clients
!
ip local pool yellow 192.168.2.1 192.168.2.10
ip local pool blue 192.168.6.1 192.168.6.6
no ip classless
!
radius-server host 10.0.0.13 auth-port 1645 acct-port 1646
radius-server key XXXXXX
radius-server vsa send accounting
radius-server vsa send authentication

```

## show crypto isakmp profile Command: Example

The following output shows that QoS group “2” has been applied to the ISAKMP profile “blue” and that QoS group “3” has been applied to the ISAKMP profile “yellow”:

```

Router# show crypto isakmp profile

ISAKMP PROFILE blue
 Identities matched are:
 group blue
 QoS Group 2 is applied

ISAKMP PROFILE yellow
 Identities matched are:
 ip-address 10.0.0.13 255.255.255.255
 group yellow
 QoS Group 3 is applied

```

## show crypto ipsec sa Command: Example

The following output shows that the QoS group has been applied to a particular pair of IPsec SAs:

```

Router# show crypto ipsec sa

interface: FastEthernet0/0
 Crypto map tag: mode, local addr. 10.0.0.110

 protected vrf:
 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
 remote ident (addr/mask/prot/port): (10.12.12.0/255.255.255.0/0/0)
 current_peer: 10.0.0.11:500

```

```
PERMIT, flags={}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

qos group is set to 2
```

## Additional References

The following sections provide references related to the IPSec and Quality of Service feature.

## Related Documents

| Related Topic     | Document Title                                                                                                   |
|-------------------|------------------------------------------------------------------------------------------------------------------|
| IPSec             | <a href="#">“IP Security and Encryption” chapter of the Cisco IOS Security Configuration Guide, Release 12.3</a> |
| QoS options       | <a href="#">Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.3</a>                         |
| QoS commands      | <a href="#">Cisco IOS Quality of Service Solutions Command Reference, Release 12.3 T</a>                         |
| Security commands | <a href="#">Cisco IOS Security Command Reference, Release 12.3 T</a>                                             |

## Standards

| Standards                                                   | Title |
|-------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature. | —     |

## MIBs

| MIBs                                                   | MIBs Link                                                                                                                                                                                                              |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                                   | Title |
|--------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

# Command Reference

The following commands are introduced or modified in the feature or features

- **qos-group**

For information about these commands, see the Cisco IOS Security Command Reference at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

---

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





# IPsec Anti-Replay Window: Expanding and Disabling

---

**First Published: February 28, 2005**  
**Last Updated: September 12, 2006**

Cisco IP security (IPsec) authentication provides anti-replay protection against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. The decryptor keeps track of which packets it has seen on the basis of these numbers. Currently, the default window size is 64 packets. Generally, this number (window size) is sufficient, but there are times when you may want to expand this window size. The IPsec Anti-Replay Window: Expanding and Disabling feature allows you to expand the window size, allowing the decryptor to keep track of more than 64 packets.

## History for the IPsec Anti-Replay Window: Expanding and Disabling Feature

| Release                  | Modification                                                     |
|--------------------------|------------------------------------------------------------------|
| 12.3(14)T                | This feature was introduced.                                     |
| 12.2(33)SRA              | This feature was integrated into Cisco IOS Release 12.2(33)SRA.  |
| 12.2(18)SXF6             | This feature was integrated into Cisco IOS Release 12.2(18)SXF6. |
| Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.    |

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for IPsec Anti-Replay Window: Expanding and Disabling, page 2](#)
- [Information About IPsec Anti-Replay Window: Expanding and Disabling, page 2](#)
- [How to Configure IPsec Anti-Replay Window: Expanding and Disabling, page 3](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

- [Configuration Examples for IPsec Anti-Replay Window: Expanding and Disabling, page 5](#)
- [Additional References, page 8](#)
- [Command Reference, page 10](#)

## Prerequisites for IPsec Anti-Replay Window: Expanding and Disabling

- Before configuring this feature, you should have already created a crypto map or crypto profile.

## Information About IPsec Anti-Replay Window: Expanding and Disabling

To configure the IPsec Anti-Replay Window: Expanding and Disabling feature, you should understand the following concept:

- [IPsec Anti-Replay Window, page 2](#)

### IPsec Anti-Replay Window

Cisco IPsec authentication provides anti-replay protection against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. (Security association [SA] anti-replay is a security service in which the receiver can reject old or duplicate packets to protect itself against replay attacks.) The decryptor checks off the sequence numbers that it has seen before. The encryptor assigns sequence numbers in an increasing order. The decryptor remembers the value X of the highest sequence number that it has already seen. N is the window size, and the decryptor also remembers whether it has seen packets having sequence numbers from X-N+1 through X. Any packet with the sequence number X-N is discarded. Currently, N is set at 64, so only 64 packets can be tracked by the decryptor.

At times, however, the 64-packet window size is not sufficient. For example, Cisco quality of service (QoS) gives priority to high-priority packets, which could cause some low-priority packets to be discarded even though they could be one of the last 64 packets received by the decryptor. The IPsec Anti-Replay Window: Expanding and Disabling feature allows you to expand the window size, allowing the decryptor to keep track of more than 64 packets.

Increasing the anti-replay window size has no impact on throughput and security. The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed to store the sequence number on the decryptor. It is recommended that you use the full 1024 window size to eliminate any future anti-replay problems.



# How to Configure IPsec Anti-Replay Window: Expanding and Disabling

This section contains the following procedures:

- [Configuring IPsec Anti-Replay Window: Expanding and Disabling Globally, page 3](#) (optional)
- [Configuring IPsec Anti-Replay Window: Expanding and Disabling on a Crypto Map, page 4](#) (optional)

## Configuring IPsec Anti-Replay Window: Expanding and Disabling Globally

To configure IPsec Anti-Replay Window: Expanding and Disabling globally (so that it affects all SAs that are created— except for those that are specifically overridden on a per-crypto map basis), perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec security-association replay window-size [N]**
4. **crypto ipsec security-association replay disable**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                   | Purpose                                                                                                                                                                                                           |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                              | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                 |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                      | Enters global configuration mode.                                                                                                                                                                                 |
| Step 3 | <b>crypto ipsec security-association replay window-size [N]</b><br><br><b>Example:</b><br>Router (config)# crypto ipsec security-association replay window-size 256 | Sets the size of the SA replay window globally.<br><br><b>Note</b> Configure this command or the <b>crypto ipsec security-association replay disable</b> command. The two commands are not used at the same time. |
| Step 4 | <b>crypto ipsec security-association replay disable</b><br><br><b>Example:</b><br>Router (config)# crypto ipsec security-association replay disable                 | Disables checking globally.<br><br><b>Note</b> Configure this command or the <b>crypto ipsec security-association replay window-size</b> command. The two commands are not used at the same time.                 |

## Configuring IPsec Anti-Replay Window: Expanding and Disabling on a Crypto Map

To configure IPsec Anti-Replay Window: Expanding and Disabling on a crypto map so that it affects those SAs that have been created using a specific crypto map or profile, perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* [**ipsec-isakmp**]
4. **set security-association replay window-size [N]**
5. **set security-association replay disable**

## DETAILED STEPS

|        | Command or Action                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                  |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                        | Enters global configuration mode.                                                                                                                                                                                                                                                        |
| Step 3 | <b>crypto map map-name seq-num [ipsec-isakmp]</b><br><br><b>Example:</b><br>Router (config)# crypto map ETH0 17 ipsec-isakmp                          | Enters crypto map configuration mode and creates a crypto profile that provides a template for configuration of dynamically created crypto maps.                                                                                                                                         |
| Step 4 | <b>set security-association replay window-size [N]</b><br><br><b>Example:</b><br>Router (crypto-map)# set security-association replay window-size 128 | Controls the SAs that are created using the policy specified by a particular crypto map, dynamic crypto map, or crypto profile. <p><b>Note</b> Configure this command or the <b>set security-association replay disable</b> command. The two commands are not used at the same time.</p> |
| Step 5 | <b>set security-association replay disable</b><br><br><b>Example:</b><br>Router (crypto-map)# set security-association replay disable                 | Disables replay checking for a particular crypto map, dynamic crypto map, or crypto profile. <p><b>Note</b> Configure this command or the <b>set security-association replay window-size</b> command. The two commands are not used at the same time.</p>                                |

## Troubleshooting Tips

- If your replay window size has not been set to a number that is high enough for the number of packets received, you will receive a system message such as the following:

```
*Nov 17 19:27:32.279: %CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
connection id=1
```

The above message is generated when a received packet is judged to be outside the anti-replay window.

## Configuration Examples for IPsec Anti-Replay Window: Expanding and Disabling

This section includes the following configuration examples:

- [Global Expanding and Disabling of an Anti-Replay Window: Example, page 6](#)

- [Expanding and Disabling of an Anti-Replay Window for a Particular Crypto Map, Dynamic Crypto Map, or Crypto Profile: Example, page 7](#)

## Global Expanding and Disabling of an Anti-Replay Window: Example

The following example shows that the anti-replay window size has been set globally to 1024:

```

version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN-Gateway1
!

boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!
!
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key cisco123 address 192.165.201.2 !
crypto ipsec security-association replay window-size 1024 !
crypto ipsec transform-set basic esp-des esp-md5-hmac !
crypto map mymap 10 ipsec-isakmp
 set peer 192.165.201.2
 set transform-set basic
 match address 101
!
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Serial1/0
 ip address 192.165.200.2 255.255.255.252 serial restart-delay 0 crypto map mymap !
 ip classless
 ip route 0.0.0.0 0.0.0.0 192.165.200.1
 no ip http server
 no ip http secure-server
!
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 172.16.2.0 0.0.0.255 access-list 101
remark Crypto ACL
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!

```

```
!
end
```

## Expanding and Disabling of an Anti-Replay Window for a Particular Crypto Map, Dynamic Crypto Map, or Crypto Profile: Example

The following example shows that anti-replay checking is disabled for IPsec connections to 172.17.150.2 but enabled (and the default window size is 64) for IPsec connections to 172.17.150.3 and 172.17.150.4:

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname networkserver1
!
enable secret 5 1KxKv$cbqKsZtQTLJLGPn.tErFZ1 enable password ww !
ip subnet-zero
!
cns event-service server

crypto isakmp policy 1
authentication pre-share

crypto isakmp key cisco170 address 172.17.150.2 crypto isakmp key cisco180 address
172.17.150.3 crypto isakmp key cisco190 address 172.17.150.4

crypto ipsec transform-set 170cisco esp-des esp-md5-hmac crypto ipsec transform-set
180cisco esp-des esp-md5-hmac crypto ipsec transform-set 190cisco esp-des esp-md5-hmac

crypto map ETH0 17 ipsec-isakmp
 set peer 172.17.150.2
 set security-association replay disable set transform-set 170cisco match address 170
crypto map ETH0 18 ipsec-isakmp set peer 192.168.1.3 set transform-set 180cisco match
address 180 crypto map ETH0 19 ipsec-isakmp set peer 192.168.1.4 set transform-set
190cisco match address 190 !
interface Ethernet0
 ip address 172.17.150.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 no mop enabled
 crypto map ETH0
!
interface Serial0
 ip address 172.16.160.1 255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 no fair-queue
!
ip classless
ip route 172.18.170.0 255.255.255.0 172.17.150.2 ip route 172.19.180.0 255.255.255.0
172.17.150.3 ip route 172.20.190.0 255.255.255.0 172.17.150.4 no ip http server !

access-list 170 permit ip 172.16.160.0 0.0.0.255 172.18.170.0 0.0.0.255 access-list 180
permit ip 172.16.160.0 0.0.0.255 172.19.180.0 0.0.0.255 access-list 190 permit ip
172.16.160.0 0.0.0.255 172.20.190.0 0.0.0.255 !
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
```

```
line con 0
transport input none
line aux 0
line vty 0 4
password ww
login
end
```

## Additional References

The following sections provide references related to IPsec Anti-Replay Window: Expanding and Disabling.

## Related Documents

| Related Topic              | Document Title                                                                                      |
|----------------------------|-----------------------------------------------------------------------------------------------------|
| Cisco IOS commands         | <i>Cisco IOS Security Command Reference, Release 12.3T</i>                                          |
| IP security and encryption | “IP Security and Encryption” section of <i>Cisco IOS Security Configuration Guide, Release 12.3</i> |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                         | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Command Reference

The following commands are introduced or modified in the feature or features

- **crypto ipsec security-association replay disable**
- **crypto ipsec security-association replay window-size**
- **set security-association replay disable**
- **set security-association replay window-size**

For information about these commands, see the Cisco IOS Security Command Reference at

[http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at

<http://tools.cisco.com/Support/CLILookup> or the Master Command List.



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





# IPSec Dead Peer Detection Periodic Message Option

---

**First Published: May 1, 2004**  
**Last Updated: August 21, 2007**

The IPSec Dead Peer Detection Periodic Message Option feature allows you to configure your router to query the liveliness of its Internet Key Exchange (IKE) peer at regular intervals. The benefit of this approach over the default approach (on-demand dead peer detection) is earlier detection of dead peers.

## History for IPSec Dead Peer Detection Periodic Message Option Feature

| Release                  | Modification                                                    |
|--------------------------|-----------------------------------------------------------------|
| 12.3(7)T                 | This feature was introduced.                                    |
| 12.2(33)SRA              | This feature was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH              | This feature was integrated into Cisco IOS Release 12.2(33)SXH. |
| Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.   |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for IPSec Dead Peer Detection Periodic Message Option, page 2](#)
- [Restrictions for IPSec Dead Peer Detection Periodic Message Option, page 2](#)
- [Information About IPSec Dead Peer Detection Periodic Message Option, page 2](#)
- [How to Configure IPSec Dead Peer Detection Periodic Message Option, page 3](#)
- [Configuration Examples for IPSec Dead Peer Detection Periodic Message Option, page 7](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

- [Additional References, page 11](#)
- [Command Reference, page 13](#)

## Prerequisites for IPSec Dead Peer Detection Periodic Message Option

Before configuring the IPSec Dead Peer Detection Periodic Message Option feature, you should have the following:

- Familiarity with configuring IP Security (IPSec).
- An IKE peer that supports DPD (dead peer detection). Implementations that support DPD include the Cisco VPN 3000 concentrator, Cisco PIX Firewall, Cisco VPN Client, and Cisco IOS software in all modes of operation—site-to-site, Easy VPN remote, and Easy VPN server.

## Restrictions for IPSec Dead Peer Detection Periodic Message Option

Using periodic DPD potentially allows the router to detect an unresponsive IKE peer with better response time when compared to on-demand DPD. However, use of periodic DPD incurs extra overhead. When communicating to large numbers of IKE peers, you should consider using on-demand DPD instead.

## Information About IPSec Dead Peer Detection Periodic Message Option

To configure IPSec Dead Peer Detection Periodic Message Option, you should understand the following concepts:

- [How DPD and Cisco IOS Keepalive Features Work, page 2](#)
- [Using the IPSec Dead Peer Detection Periodic Message Option, page 3](#)
- [Using DPD and Cisco IOS Keepalive Features with Multiple Peers in the Crypto Map, page 3](#)
- [Using DPD in an Easy VPN Remote Configuration, page 3](#)

## How DPD and Cisco IOS Keepalive Features Work

DPD and Cisco IOS keepalives function on the basis of the timer. If the timer is set for 10 seconds, the router will send a “hello” message every 10 seconds (unless, of course, the router receives a “hello” message from the peer). The benefit of IOS keepalives and periodic DPD is earlier detection of dead peers. However, IOS keepalives and periodic DPD rely on periodic messages that have to be sent with considerable frequency. The result of sending frequent messages is that the communicating peers must encrypt and decrypt more packets.

DPD also has an on-demand approach. The contrasting on-demand approach is the default. With on-demand DPD, messages are sent on the basis of traffic patterns. For example, if a router has to send outbound traffic and the liveliness of the peer is questionable, the router sends a DPD message to query the status of the peer. If a router has no traffic to send, it never sends a DPD message. If a peer is dead, and the router never has any traffic to send to the peer, the router will not find out until the IKE or IPSec security association (SA) has to be rekeyed (the liveliness of the peer is unimportant if the router is not trying to communicate with the peer). On the other hand, if the router has traffic to send to the peer, and the peer does not respond, the router will initiate a DPD message to determine the state of the peer.

## Using the IPSec Dead Peer Detection Periodic Message Option

With the IPSec Dead Peer Detection Periodic Message Option feature, you can configure your router so that DPD messages are “forced” at regular intervals. This forced approach results in earlier detection of dead peers. For example, if a router has no traffic to send, a DPD message is still sent at regular intervals, and if a peer is dead, the router does not have to wait until the IKE SA times out to find out.

If you want to configure the DPD periodic message option, you should use the **crypto isakmp keepalive** command with the **periodic** keyword. If you do not configure the **periodic** keyword, the router defaults to the on-demand approach.



### Note

When the **crypto isakmp keepalive** command is configured, the Cisco IOS software negotiates the use of Cisco IOS keepalives or DPD, depending on which protocol the peer supports.

## Using DPD and Cisco IOS Keepalive Features with Multiple Peers in the Crypto Map

DPD and IOS keepalive features can be used in conjunction with multiple peers in the crypto map to allow for stateless failover. DPD allows the router to detect a dead IKE peer, and when the router detects the dead state, the router deletes the IPSec and IKE SAs to the peer. If you configure multiple peers, the router will switch over to the next listed peer for a stateless failover.

## Using DPD in an Easy VPN Remote Configuration

DPD can be used in an Easy VPN remote configuration. See the section [“Configuring DPD for an Easy VPN Remote” section on page 5](#).

## How to Configure IPSec Dead Peer Detection Periodic Message Option

This section contains the following procedures:

- [Configuring a Periodic DPD Message, page 4](#)
- [Configuring DPD and Cisco IOS Keepalives with Multiple Peers in the Crypto Map, page 4](#)
- [Configuring DPD for an Easy VPN Remote, page 5](#)
- [Verifying That DPD Is Enabled, page 6](#)

## Configuring a Periodic DPD Message

To configure a periodic DPD message, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp keepalive *seconds* [*retries*] [**periodic** | **on-demand**]**

### DETAILED STEPS

|        | Command or Action                                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                             | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                          |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                     | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 3 | <b>crypto isakmp keepalive <i>seconds</i> [<i>retries</i>] [<b>periodic</b>   <b>on-demand</b>]</b><br><br><b>Example:</b><br>Router (config)# crypto isakmp keepalive 10 periodic | Allows the gateway to send DPD messages to the peer. <ul style="list-style-type: none"> <li>• <i>seconds</i>—Number of seconds between DPD messages.</li> <li>• <i>retries</i>—(Optional) Number of seconds between DPD retries if the DPD message fails.</li> <li>• <b>periodic</b>—(Optional) DPD messages are sent at regular intervals.</li> <li>• <b>on-demand</b>—(Optional) DPD retries are sent on demand. This is the default behavior.</li> </ul> |

## Configuring DPD and Cisco IOS Keepalives with Multiple Peers in the Crypto Map

To configure DPD and IOS keepalives to be used in conjunction with the crypto map to allow for stateless failover, perform the following steps. This configuration will cause a router to cycle through the peer list when it detects that the first peer is dead.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map *map-name seq-num ipsec-isakmp***
4. **set peer {*host-name* [**dynamic**] | *ip-address*}**

5. **set transform-set** *transform-set-name*
6. **match address** [*access-list-id* | *name*]

## DETAILED STEPS

|        | Command or Action                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                      |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                             |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                         | Enters global configuration mode.                                                                                                                                                                                                                                                            |
| Step 3 | <b>crypto map</b> <i>map-name</i> <i>seq-num</i> <b>ipsec-isakmp</b><br><br><b>Example:</b><br>Router (config)# crypto map green 1 ipsec-isakmp        | Enters crypto map configuration mode and creates or modifies a crypto map entry. <ul style="list-style-type: none"> <li>The <b>ipsec-isakmp</b> keyword indicates that IKE will be used to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.</li> </ul> |
| Step 4 | <b>set peer</b> { <i>host-name</i> [ <b>dynamic</b> ]   <i>ip-address</i> }<br><br><b>Example:</b><br>Router (config-crypto-map)# set peer 10.12.12.12 | Specifies an IPSec peer in a crypto map entry. <ul style="list-style-type: none"> <li>You can specify multiple peers by repeating this command.</li> </ul>                                                                                                                                   |
| Step 5 | <b>set transform-set</b> <i>transform-set-name</i><br><br><b>Example:</b><br>Router (config-crypto-map)# set transform-set txfm                        | Specifies which transform sets can be used with the crypto map entry. <ul style="list-style-type: none"> <li>You can specify more than one transform set name by repeating this command.</li> </ul>                                                                                          |
| Step 6 | <b>match address</b> [ <i>access-list-id</i>   <i>name</i> ]<br><br><b>Example:</b><br>Router (config-crypto-map)# match address 101                   | Specifies an extended access list for a crypto map entry.                                                                                                                                                                                                                                    |

## Configuring DPD for an Easy VPN Remote

To configure DPD in an Easy VPN remote configuration, perform the following steps. This configuration also will cause a router to cycle through the peer list when it detects that the first peer is dead.



### Note

IOS keepalives are not supported for Easy VPN remote configurations.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **crypto ipsec client ezvpn** *name*
4. **connect** {**auto** | **manual**}
5. **group** *group-name* **key** *group-key*
6. **mode** {**client** | **network-extension**}
7. **peer** {*ipaddress* | *hostname*}

## DETAILED STEPS

|               |                                                                                                                                                 |                                                                                                                                                                                                                                                                          |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                          | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                                           |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                  | Enters global configuration mode.                                                                                                                                                                                                                                        |
| <b>Step 3</b> | <b>crypto ipsec client ezvpn</b> <i>name</i><br><br><b>Example:</b><br>Router (config)# crypto ipsec client ezvpn<br>ezvpn-config1              | Creates a Cisco Easy VPN remote configuration and enters the Cisco Easy VPN Remote configuration mode.                                                                                                                                                                   |
| <b>Step 4</b> | <b>connect</b> { <b>auto</b>   <b>manual</b> }<br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# connect manual                           | Manually establishes and terminates an IPSec VPN tunnel on demand. <ul style="list-style-type: none"><li>The <b>auto</b> keyword option is the default setting.</li></ul>                                                                                                |
| <b>Step 5</b> | <b>group</b> <i>group-name</i> <b>key</b> <i>group-key</i><br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# group unity key<br>preshared | Specifies the group name and key value for the Virtual Private Network (VPN) connection.                                                                                                                                                                                 |
| <b>Step 6</b> | <b>mode</b> { <b>client</b>   <b>network-extension</b> }<br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# mode client                    | Specifies the VPN mode of operation of the router.                                                                                                                                                                                                                       |
| <b>Step 7</b> | <b>peer</b> { <i>ipaddress</i>   <i>hostname</i> }<br><br><b>Example:</b><br>Router (config-crypto-ezvpn)# peer 10.10.10.10                     | Sets the peer IP address or host name for the VPN connection. <ul style="list-style-type: none"><li>A hostname can be specified only when the router has a DNS server available for host-name resolution.</li><li>This command can be repeated multiple times.</li></ul> |

## Verifying That DPD Is Enabled

DPD allows the router to clear the IKE state when a peer becomes unreachable. If DPD is enabled and the peer is unreachable for some time, you can use the **clear crypto session** command to manually clear IKE and IPSec SAs.

The **debug crypto isakmp** command can be used to verify that DPD is enabled.

## SUMMARY STEPS

1. **enable**
2. **clear crypto session** [**local** *ip-address* [**port** *local-port*]] [**remote** *ip-address* [**port** *remote-port*]] | [**fvrif** *vrf-name*] [**ivrf** *vrf-name*]
3. **debug crypto isakmp**

## DETAILED STEPS

|        |                                                                                                                                                                                                                                                                                                 |                                                                                                                    |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                          | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>clear crypto session</b> [ <b>local</b> <i>ip-address</i> [ <b>port</b> <i>local-port</i> ]] [ <b>remote</b> <i>ip-address</i> [ <b>port</b> <i>remote-port</i> ]]   [ <b>fvrif</b> <i>vrf-name</i> ] [ <b>ivrf</b> <i>vrf-name</i> ]<br><br><b>Example:</b><br>Router# clear crypto session | Deletes crypto sessions (IPSec and IKE SAs).                                                                       |
| Step 3 | <b>debug crypto isakmp</b><br><br><b>Example:</b><br>Router# debug crypto isakmp                                                                                                                                                                                                                | Displays messages about IKE events.                                                                                |

# Configuration Examples for IPSec Dead Peer Detection Periodic Message Option

This section provides the following configuration examples:

- [Site-to-Site Setup with Periodic DPD Enabled: Example, page 7](#)
- [Easy VPN Remote with DPD Enabled: Example, page 8](#)
- [Verifying DPD Configuration Using the debug crypto isakmp Command: Example, page 8](#)
- [DPD and Cisco IOS Keepalives Used in Conjunction with Multiple Peers in a Crypto Map: Example, page 11](#)
- [DPD Used in Conjunction with Multiple Peers for an Easy VPN Remote: Example, page 11](#)

## Site-to-Site Setup with Periodic DPD Enabled: Example

The following configurations are for a site-to-site setup with no periodic DPD enabled. The configurations are for the IKE Phase 1 policy and for the IKE preshared key.

### IKE Phase 1 Policy

```
crypto isakmp policy 1
 encryption 3des
```

```

authentication pre-share
group 2
!

```

### IKE Preshared Key

```

crypto isakmp key kd94j1ksldz address 10.2.80.209 255.255.255.0
crypto isakmp keepalive 10 periodic
crypto ipsec transform-set esp-3des-sha esp-3des esp-sha-hmac
crypto map test 1 ipsec-isakmp
 set peer 10.2.80.209
 set transform-set esp-3des-sha
 match address 101
!
!
interface FastEthernet0
 ip address 10.1.32.14 255.255.255.0
 speed auto
 crypto map test
!

```

## Easy VPN Remote with DPD Enabled: Example

The following configuration tells the router to send a periodic DPD message every 30 seconds. If the peer fails to respond to the DPD R\_U\_THERE message, the router will resend the message every 20 seconds (four transmissions altogether).

```

crypto isakmp keepalive 30 20 periodic
crypto ipsec client ezvpn ezvpn-config
 connect auto
 group unity key preshared
 mode client
 peer 10.2.80.209
!
!
interface Ethernet0
 ip address 10.2.3.4 255.255.255.0
 half-duplex
 crypto ipsec client ezvpn ezvpn-config inside
!
interface FastEthernet0
 ip address 10.1.32.14 255.255.255.0
 speed auto
 crypto ipsec client ezvpn ezvpn-config outside

```

## Verifying DPD Configuration Using the debug crypto isakmp Command: Example

The following sample output from the **debug crypto isakmp** command verifies that IKE DPD is enabled:

```
*Mar 25 15:17:14.131: ISAKMP:(0:1:HW:2):IKE_DPD is enabled, initializing timers
```



To see that IKE DPD is enabled (and that the peer supports DPD): when periodic DPD is enabled, you should see the following debug messages at the interval specified by the command:

```
*Mar 25 15:18:52.107: ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:18:52.107: ISAKMP:(0:1:HW:2):purging node 899852982 *Mar 25 15:18:52.111:
ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER_IM_ALIVE
*Mar 25 15:18:52.111: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE
```

The above message corresponds to sending the DPD R\_U\_THERE message.

```
*Mar 25 15:18:52.123: ISAKMP (0:268435457): received packet from 10.2.80.209
dport 500 sport 500 Global (I) QM_IDLE
*Mar 25 15:18:52.123: ISAKMP: set new node -443923643 to QM_IDLE *Mar 25 15:18:52.131:
ISAKMP:(0:1:HW:2): processing HASH payload. message ID =
-443923643
*Mar 25 15:18:52.131: ISAKMP:(0:1:HW:2): processing NOTIFY R_U_THERE_ACK protocol 1
spi 0, message ID = -443923643, sa = 81BA4DD4
*Mar 25 15:18:52.135: ISAKMP:(0:1:HW:2): DPD/R_U_THERE_ACK received from peer
10.2.80.209, sequence 0x9
*Mar 25 15:18:52.135: ISAKMP:(0:1:HW:2):deleting node -443923643 error FALSE
reason "informational (in) state 1"
*Mar 25 15:18:52.135: ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_PEER, IKE_INFO_NOTIFY *Mar
25 15:18:52.135: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE
```

The above message corresponds to receiving the acknowledge (ACK) message from the peer.

```
Router#
*Mar 25 15:47:35.335: ISAKMP: set new node -90798077 to QM_IDLE *Mar 25 15:47:35.343:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:35.343: ISAKMP:(0:1:HW:2):purging node -90798077 *Mar 25 15:47:35.347:
ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER_IM_ALIVE
*Mar 25 15:47:35.347: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE

*Mar 25 15:47:36.611: ISAKMP:(0:1:HW:2):purging node 1515050537 *Mar 25 15:47:37.343:
ISAKMP:(0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:37.343: ISAKMP: set new node -1592471565 to QM_IDLE *Mar 25 15:47:37.351:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:37.351: ISAKMP:(0:1:HW:2):purging node -1592471565 *Mar 25 15:47:37.355:
ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:37.355: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE

*Mar 25 15:47:39.355: ISAKMP:(0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:39.355: ISAKMP: set new node 1758739401 to QM_IDLE *Mar 25 15:47:39.363:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:39.363: ISAKMP:(0:1:HW:2):purging node 1758739401 *Mar 25 15:47:39.367:
ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:39.367: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE

*Mar 25 15:47:41.367: ISAKMP:(0:1:HW:2):incrementing error counter on sa:
```

## Configuration Examples for IPSec Dead Peer Detection Periodic Message Option

```

PEERS_ALIVE_TIMER
*Mar 25 15:47:41.367: ISAKMP: set new node 320258858 to QM_IDLE *Mar 25 15:47:41.375:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:41.379: ISAKMP:(0:1:HW:2):purging node 320258858 *Mar 25 15:47:41.379:
ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:41.379: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE

*Mar 25 15:47:43.379: ISAKMP:(0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:43.379: ISAKMP: set new node -744493014 to QM_IDLE *Mar 25 15:47:43.387:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:43.387: ISAKMP:(0:1:HW:2):purging node -744493014 *Mar 25 15:47:43.391:
ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:43.391: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE

*Mar 25 15:47:45.391: ISAKMP:(0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:45.391: ISAKMP:(0:1:HW:2):peer 10.2.80.209 not responding! *Mar 25
15:47:45.391: ISAKMP:(0:1:HW:2):peer does not do paranoid keepalives.

*Mar 25 15:47:45.391: ISAKMP:(0:1:HW:2):deleting SA reason "peers alive" state
(I) QM_IDLE (peer 10.2.80.209) input queue 0
*Mar 25 15:47:45.395: ISAKMP: Unlocking IPSEC struct 0x81E5C4E8 from
delete_siblings, count 0
*Mar 25 15:47:45.395: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN. Peer
10.2.80.209:500 Id: 10.2.80.209
*Mar 25 15:47:45.399: ISAKMP: set new node -2061951065 to QM_IDLE *Mar 25 15:47:45.411:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:45.411: ISAKMP:(0:1:HW:2):purging node -2061951065 *Mar 25 15:47:45.411:
ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:45.411: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_DEST_SA

*Mar 25 15:47:45.415: ISAKMP:(0:1:HW:2):deleting SA reason "peers alive" state
(I) QM_IDLE (peer 10.2.80.209) input queue 0
*Mar 25 15:47:45.415: ISAKMP: Unlocking IKE struct 0x81E5C4E8 for
isadb_mark_sa_deleted(), count 0
*Mar 25 15:47:45.415: ISAKMP: Deleting peer node by peer_reap for 10.2.80.209:
81E5C4E8
*Mar 25 15:47:45.415: ISAKMP:(0:1:HW:2):deleting node -1067612752 error TRUE
reason "peers alive"
*Mar 25 15:47:45.415: ISAKMP:(0:1:HW:2):deleting node -114443536 error TRUE
reason "peers alive"
*Mar 25 15:47:45.419: ISAKMP:(0:1:HW:2):deleting node 2116015069 error TRUE
reason "peers alive"
*Mar 25 15:47:45.419: ISAKMP:(0:1:HW:2):deleting node -1981865558 error TRUE
reason "peers alive"
*Mar 25 15:47:45.419: ISAKMP:(0:1:HW:2):Input = IKE_MSG_INTERNAL, IKE_PHASE1_DEL *Mar 25
15:47:45.419: ISAKMP:(0:1:HW:2):Old State = IKE_DEST_SA New State =
IKE_DEST_SA

*Mar 25 15:47:45.419: ISAKMP: received ke message (4/1)
*Mar 25 15:47:45.419: ISAKMP: received ke message (3/1)
*Mar 25 15:47:45.423: ISAKMP: ignoring request to send delete notify (no ISAKMP
sa) src 10.1.32.14 dst 10.2.80.209 for SPI 0x3A7B69BF
*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting SA reason "" state (I)

```

```
MM_NO_STATE (peer 10.2.80.209) input queue 0
*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting node -1067612752 error FALSE
reason ""
*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting node -114443536 error FALSE
reason ""
*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting node 2116015069 error FALSE
reason ""
*Mar 25 15:47:45.427: ISAKMP:(0:1:HW:2):deleting node -1981865558 error FALSE
reason ""
*Mar 25 15:47:45.427: ISAKMP:(0:1:HW:2):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH *Mar 25
15:47:45.427: ISAKMP:(0:1:HW:2):Old State = IKE_DEST_SA New State =
IKE_DEST_SA
```

The above message shows what happens when the remote peer is unreachable. The router sends one DPD R\_U\_THERE message and four retransmissions before it finally deletes the IPsec and IKE SAs.

## DPD and Cisco IOS Keepalives Used in Conjunction with Multiple Peers in a Crypto Map: Example

The following example shows that DPD and Cisco IOS keepalives are used in conjunction with multiple peers in a crypto map configuration when IKE will be used to establish the security associations (SAs). In this example, an SA could be set up to the IPsec peer at 10.0.0.1, 10.0.0.2, or 10.0.0.3.

```
crypto map green 1 ipsec-isakmp
 set peer 10.0.0.1
 set peer 10.0.0.2
 set peer 10.0.0.3
 set transform-set txfm
 match address 101
```

## DPD Used in Conjunction with Multiple Peers for an Easy VPN Remote: Example

The following example shows that DPD is used in conjunction with multiple peers in an Easy VPN remote configuration. In this example, an SA could be set up to the IPsec peer at 10.10.10.10, 10.2.2.2, or 10.3.3.3.

```
crypto ipsec client ezvpn ezvpn-config
 connect auto
 group unity key preshared
 mode client
 peer 10.10.10.10
 peer 10.2.2.2
 peer 10.3.3.3
```

## Additional References

The following sections provide references related to IPsec Dead Peer Detection Periodic Message Option.

## Related Documents

| Related Topic     | Document Title                                                                                        |
|-------------------|-------------------------------------------------------------------------------------------------------|
| Configuring IPSec | <a href="#">“IP Security and Encryption”</a> section of <i>Cisco IOS Security Configuration Guide</i> |
| IPSec commands    | <a href="#">Cisco IOS Security Command Reference, Release 12.4 T</a>                                  |

## Standards

| Standards                                                   | Title |
|-------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature. | —     |

## MIBs

| MIBs                                                   | MIBs Link                                                                                                                                                                                                                  |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                                                                                                                                         | Title |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| DPD conforms to the Internet draft “draft-ietf-ipsec-dpd-04.txt,” which is pending publication as an Informational RFC (a number has not yet been assigned). | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

## Command Reference

The following commands are introduced or modified in the feature or features

- **crypto isakmp keepalive**

For information about these commands, see the Cisco IOS Security Command Reference at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





# IPsec Diagnostics Enhancement

---

**First Published: June 19, 2006**

**Last Updated: June 19, 2006**

The Cisco IPsec Diagnostics Enhancement feature adds four sets of event statistics and an error history buffer to the Cisco IOS software for use in troubleshooting a virtual private network (VPN) that encrypts the data path.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all of the features documented in this module.*

, use the “Feature Information for the IPsec Diagnostics Enhancement” section on page 16.

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- 
- [Restrictions for the IPsec Diagnostics Enhancement, page 2](#)  
[Information About the IPsec Diagnostics Enhancement, page 2](#)  
[How to Use the IPsec Diagnostics Enhancement, page 3](#)  
[Additional References, page 5](#)  
[Command Reference, page 7](#)

## Prerequisites for the IPsec Diagnostics Enhancement

- You understand the IP security (IPsec) standard for network security.



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.



Note

## Restrictions for the IPsec Diagnostics Enhancement

- 

## Memory and Performance Impact

- 

## Information About the IPsec Diagnostics Enhancement

- [Tracking Packet Processing Within a Switch or Router, page 2](#)

## Tracking Packet Processing Within a Switch or Router

Standard packet analyzers used for troubleshooting network issues capture packets between devices in the network but they cannot capture packet processing events inside a device, such as a router. Beginning with Cisco IOS Release 12.4(9)T, Cisco IOS software includes four sets of event statistics to track packet processing within a switch or router. These statistics help Cisco TAC engineers diagnose and resolve issues in encrypted networks. Each set of statistics tracks a different aspect of packet processing within a switch or router:

Error counters track packet processing errors and associated packet drops. When a packet encounters an error, the first 64 bytes of that packet are stored in a buffer, to facilitate troubleshooting.

Internal counters show the detailed movement of a packet, end to end, across an encryption data path.

Punt counters track instances when the configured packet processing method failed, and an alternative method was used.

Success counters record the data path checkpoints where packets are successfully forwarded.

You can view any one set of statistics, or all of them, or only those that have recorded errors. You must choose the display timeframe for the statistics, either **realtime**

**snapshot**



# How to Use the IPsec Diagnostics Enhancement



Note

- 
- [Displaying the Error History, page 4](#)  
[Clearing the Counters or Error History, page 5](#)

## Displaying the Statistics

`show crypto datapath`

|                       |                       |
|-----------------------|-----------------------|
| <code>realtime</code> | <code>snapshot</code> |
| <code>all</code>      |                       |
| <code>non-zero</code> |                       |

### SUMMARY STEPS

1. `enable`
2. `show crypto datapath {ipv4 | ipv6} {  
punt success} [error internal`

DETAILED STEPS

|        | Command or Action                                                                                                                                                         | Purpose                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                                                                                                                                             | Enables privileged EXEC mode.<br><br>Enter your password if prompted. |
|        | <b>Example:</b><br>Router> enable                                                                                                                                         |                                                                       |
|        | <b>show crypto datapath {ipv4   ipv6} {snapshot   realtime} {all   non-zero} [error   internal   punt   success]</b><br><br>Router# show crypto datapath snapshot success |                                                                       |

Displaying the Error History

**cfd**

example, you can display all events for the last 30 minutes.

For detailed information about the show monitor event-trace command, see the [Cisco IOS Configuration Fundamentals Command Reference](#).

*seconds | latest | parameters}]* *component {all | back time | clock time | from-boot*

DETAILED STEPS

|        | Command or Action                                                                                                              | Purpose                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|
| Step 1 | <b>Example:</b>                                                                                                                | <ul style="list-style-type: none"><li></li></ul> |
| Step 2 | <pre>component      back time      time from-boot seconds      }]</pre><br><pre>Router# show monitor event-trace cfd all</pre> |                                                  |

Clearing the Counters or Error History

SUMMARY STEPS

- 1.
- 2.

DETAILED STEPS

|                                                                 |  |
|-----------------------------------------------------------------|--|
|                                                                 |  |
|                                                                 |  |
| Router> enable                                                  |  |
| <pre>      {             } [                            ]</pre> |  |
| Router# clear crypto datapath success                           |  |

Additional References

| Related Topic | Document Title                                         |
|---------------|--------------------------------------------------------|
|               | <a href="#">Cisco IOS Security Configuration Guide</a> |

| Standard | Title |
|----------|-------|
|          | —     |

## MIBs

| MIB                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC | Title |
|-----|-------|
|     |       |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                         | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

### Feature Information for the IPsec Diagnostics Enhancement

[http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

---

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





# IPSec NAT Transparency

---

The IPSec NAT Transparency feature introduces support for IP Security (IPSec) traffic to travel through Network Address Translation (NAT) or Port Address Translation (PAT) points in the network by addressing many known incompatibilities between NAT and IPSec.

## Feature Specifications for the IPSec NAT Transparency feature

---

### Feature History

| Release                  | Modification                                                  |
|--------------------------|---------------------------------------------------------------|
| 12.2(13)T                | This feature was introduced.                                  |
| Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers. |

---

### Supported Platforms

For platforms supported in Cisco IOS Release 12.2(13)T, consult Cisco Feature Navigator.

---

## Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:



---

### Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

<http://www.cisco.com/go/fn>

#### **Availability of Cisco IOS Software Images**

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

## **Contents**

- [Restrictions for IPSec NAT Transparency, page 2](#)
- [Information About IPSec NAT Transparency, page 2](#)
- [How to Configure NAT and IPSec, page 7](#)
- [Configuration Examples for IPSec and NAT, page 9](#)
- [Additional References, page 9](#)
- [Command Reference, page 11](#)
- [Glossary, page 12](#)

## **Restrictions for IPSec NAT Transparency**

Although this feature addresses many incompatibilities between NAT and IPSec, the following problems still exist:

#### **Internet Key Exchange (IKE) IP Address and NAT**

This incompatibility applies only when IP addresses are used as a search key to find a preshared key. Modification of the IP source or destination addresses by NAT or reverse NAT results in a mismatch between the IP address and the preshared key.

#### **Embedded IP Addresses and NAT**

Because the payload is integrity protected, any IP address enclosed within IPSec packets cannot be translated by NAT. Protocols that use embedded IP addresses include FTP, Internet Relay Chat (IRC), Simple Network Management Protocol (SNMP), Lightweight Directory Access Protocol (LDAP), H.323, and Session Initiation Protocol (SIP).

## **Information About IPSec NAT Transparency**

To configure the IPSec NAT Transparency feature, you must understand the following concepts:

- [Benefit of IPSec NAT Transparency, page 3](#)
- [Feature Design of IPSec NAT Traversal, page 3](#)
- [NAT Keepalives, page 6](#)



## Benefit of IPSec NAT Transparency

Before the introduction of this feature, a standard IPSec virtual private network (VPN) tunnel would not work if there were one or more NAT or PAT points in the delivery path of the IPSec packet. This feature makes NAT IPSec-aware, thereby, allowing remote access users to build IPSec tunnels to home gateways.

## Feature Design of IPSec NAT Traversal

The IPSec NAT Transparency feature introduces support for IPSec traffic to travel through NAT or PAT points in the network by encapsulating IPSec packets in a User Datagram Protocol (UDP) wrapper, which allows the packets to travel across NAT devices. The following sections define the details of NAT traversal:

- [IKE Phase 1 Negotiation: NAT Detection](#)
- [IKE Phase 2 Negotiation: NAT Traversal Decision](#)
- [UDP Encapsulation of IPSec Packets for NAT Traversal](#)
- [UDP Encapsulated Process for Software Engines: Transport Mode and Tunnel Mode ESP Encapsulation](#)

### IKE Phase 1 Negotiation: NAT Detection

During Internet Key Exchange (IKE) phase 1 negotiation, two types of NAT detection occur before IKE Quick Mode begins—NAT support and NAT existence along the network path.

To detect NAT support, you should exchange the vendor identification (ID) string with the remote peer. During Main Mode (MM) 1 and MM 2 of IKE phase 1, the remote peer sends a vendor ID string payload to its peer to indicate that this version supports NAT traversal. Thereafter, NAT existence along the network path can be determined.

Detecting whether NAT exists along the network path allows you to find any NAT device between two peers and the exact location of NAT. A NAT device can translate the private IP address and port to public value (or from public to private). This translation changes the IP address and port if the packet goes through the device. To detect whether a NAT device exists along the network path, the peers should send a payload with hashes of the IP address and port of both the source and destination address from each end. If both ends calculate the hashes and the hashes match, each peer knows that a NAT device does not exist on the network path between them. If the hashes do not match (that is, someone translated the address or port), then each peer needs to perform NAT traversal to get the IPSec packet through the network.

The hashes are sent as a series of NAT discovery (NAT-D) payloads. Each payload contains one hash; if multiple hashes exist, multiple NAT-D payloads are sent. In most environments, there are only two NAT-D payloads—one for the source address and port and one for the destination address and port. The destination NAT-D payload is sent first, followed by the source NAT-D payload, which implies that the receiver should expect to process the local NAT-D payload first and the remote NAT-D payload second. The NAT-D payloads are included in the third and fourth messages in Main Mode and in the second and third messages in Aggressive Mode (AM).

## IKE Phase 2 Negotiation: NAT Traversal Decision

While IKE phase 1 detects NAT support and NAT existence along the network path, IKE phase 2 decides whether or not the peers at both ends will use NAT traversal. Quick Mode (QM) security association (SA) payload in QM1 and QM2 is used to for NAT traversal negotiation.

Because the NAT device changes the IP address and port number, incompatibilities between NAT and IPsec can be created. Thus, exchanging the original source address bypasses any incompatibilities.

## UDP Encapsulation of IPsec Packets for NAT Traversal

In addition to allowing IPsec packets to traverse across NAT devices, UDP encapsulation also addresses many incompatibility issues between IPsec and NAT and PAT. The resolved issues are as follows:

### Incompatibility Between IPsec ESP and PAT—Resolved

If PAT found a legislative IP address and port, it would drop the Encapsulating Security Payload (ESP) packet. To prevent this scenario, UDP encapsulation is used to hide the ESP packet behind the UDP header. Thus, PAT treats the ESP packet as a UDP packet, processing the ESP packet as a normal UDP packet.

### Incompatibility Between Checksums and NAT—Resolved

In the new UDP header, the checksum value is always assigned to zero. This value prevents an intermediate device from validating the checksum against the packet checksum, thereby, resolving the TCP UDP checksum issue because NAT changes the IP source and destination addresses.

### Incompatibility Between Fixed IKE Destination Ports and PAT—Resolved

PAT changes the port address in the new UDP header for translation and leaves the original payload unchanged.

To see how UDP encapsulation helps to send IPsec packets see [Figure 1](#) and [Figure 2](#).

**Figure 1**      ***Standard IPSec Tunnel Through a NAT/PAT Point (No UDP Encapsulation)***



**Figure 2**      ***IPSec Packet with UDP Encapsulation***



## UDP Encapsulated Process for Software Engines: Transport Mode and Tunnel Mode ESP Encapsulation

After the IPsec packet is encrypted by a hardware accelerator or a software crypto engine, a UDP header and a non-IKE marker (which is 8 bytes in length) are inserted between the original IP header and ESP header. The total length, protocol, and checksum fields are changed to match this modification. [Figure 3](#) shows an IPsec packet before and after transport mode is applied; [Figure 4](#) shows an IPsec packet before and after tunnel mode is applied.

**Figure 3**      *Transport Mode—IPsec Packet Before and After ESP Encapsulation*



**Figure 4**      *Tunnel Mode—IPsec Packet Before and After ESP Encapsulation*



## NAT Keepalives

NAT keepalives are enabled to keep the dynamic NAT mapping alive during a connection between two peers. NAT keepalives are UDP packets with an unencrypted payload of 1 byte. Although the current dead peer detection (DPD) implementation is similar to NAT keepalives, there is a slight difference: DPD is used to detect peer status, while NAT keepalives are sent if the IPsec entity did not send or receive the packet at a specified period of time—valid range is between 5 to 3600 seconds.

If NAT keepalives are enabled (via the `crypto isamkp nat keepalive` command), users should ensure that the idle value is shorter than the NAT mapping expiration time, which is 20 seconds.

# How to Configure NAT and IPSec

This section contains the following procedures:

- [Configuring NAT Traversal, page 7](#) (optional)
- [Disabling NAT Traversal, page 7](#) (optional)
- [Configuring NAT Keepalives, page 8](#) (optional)
- [Verifying IPSec Configuration, page 8](#) (optional)

## Configuring NAT Traversal

NAT Traversal is a feature that is auto detected by VPN devices. There are no configuration steps for a router running Cisco IOS Release 12.2(13)T. If both VPN devices are NAT-T capable, NAT Traversal is auto detected and auto negotiated.

## Disabling NAT Traversal

You may wish to disable NAT traversal if you already know that your network uses IPSec-awareness NAT (spi-matching scheme). To disable NAT traversal, use the following commands:

### SUMMARY STEPS:

1. `enable`
2. `configure terminal`
3. `no crypto ipsec nat-transparency udp-encapsulation`

### DETAILED STEPS

|        | Command or Action                                                                                      | Purpose                                                        |
|--------|--------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| Step 1 | <code>enable</code>                                                                                    | Enables higher privilege levels, such as privileged EXEC mode. |
|        | <b>Example:</b><br><code>Router&gt; enable</code>                                                      | Enter your password if prompted.                               |
| Step 2 | <code>configure terminal</code>                                                                        | Enters global configuration mode.                              |
|        | <b>Example:</b><br><code>Router# configure terminal</code>                                             |                                                                |
| Step 3 | <code>no crypto ipsec nat-transparency<br/>udp-encapsulation</code>                                    | Disables NAT traversal.                                        |
|        | <b>Example:</b><br><code>Router(config)# no crypto ipsec nat-transparency<br/>udp-encapsulation</code> |                                                                |

## Configuring NAT Keepalives

To configure your router to send NAT keepalives, use the following commands:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp nat keepalive *seconds***

### DETAILED STEPS

|        | Command or Action                                                 | Purpose                                                                                                                                                  |
|--------|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                                     | Enables higher privilege levels, such as privileged EXEC mode.                                                                                           |
|        | <b>Example:</b><br>Router> enable                                 | Enter your password if prompted.                                                                                                                         |
| Step 2 | <b>configure terminal</b>                                         | Enters global configuration mode.                                                                                                                        |
|        | <b>Example:</b><br>Router# configure terminal                     |                                                                                                                                                          |
| Step 3 | <b>crypto isakmp nat keepalive <i>seconds</i></b>                 | Allows an IPSec node to send NAT keepalive packets.                                                                                                      |
|        | <b>Example:</b><br>Router(config)# crypto isakmp nat keepalive 20 | <ul style="list-style-type: none"> <li>• <i>seconds</i>—The number of seconds between keepalive packets; range is between 5 to 3,600 seconds.</li> </ul> |

## Verifying IPSec Configuration

To verify your configuration, perform the following optional steps:

### SUMMARY STEPS

1. **enable**
2. **show crypto ipsec sa [map *map-name* | address | identity] [detail]**

## DETAILED STEPS

|        | Command or Action                                                                                               | Purpose                                                        |
|--------|-----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| Step 1 | <b>enable</b>                                                                                                   | Enables higher privilege levels, such as privileged EXEC mode. |
|        | <b>Example:</b><br>Router> enable                                                                               | Enter your password if prompted.                               |
| Step 2 | <b>show crypto ipsec sa</b> [ <b>map</b> <i>map-name</i>   <b>address</b>   <b>identity</b> ] [ <b>detail</b> ] | Displays the settings used by current SAs.                     |
|        | <b>Example:</b><br>Router# show crypto ipsec sa                                                                 |                                                                |

# Configuration Examples for IPSec and NAT

This section provides the following configuration example:

- [NAT Keepalives Configuration Example, page 9](#)

## NAT Keepalives Configuration Example

The following example shows how to enable NAT keepalives to be sent every 20 seconds:

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key 1234 address 56.0.0.1
crypto isakmp nat keepalive 20
!
!
crypto ipsec transform-set t2 esp-des esp-sha-hmac
!
crypto map test2 10 ipsec-isakmp
 set peer 56.0.0.1
 set transform-set t2
 match address 101
```

## Additional References

The following sections provide additional references related to IPSec NAT Transparency:

- [Related Documents, page 10](#)
- [Standards, page 10](#)
- [MIBs, page 10](#)
- [RFCs, page 11](#)
- [Technical Assistance, page 11](#)

## Related Documents

| Related Topic                                                           | Document Title                                                                                                                          |
|-------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Additional NAT configuration tasks.                                     | <i>The chapter “Configuring IP Addressing” in the Cisco IOS IP Configuration Guide, Release 12.2</i>                                    |
| Additional NAT commands                                                 | <i>The chapter “IP Addressing Commands” in the Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2</i> |
| Additional IPSec configuration tasks                                    | <i>The chapter “Configuring IPSec Network Security” in the Cisco IOS Security Configuration Guide, Release 12.2</i>                     |
| Additional IPSec commands                                               | <i>The chapter “IPSec Network Security Commands” in the Cisco IOS Security Command Reference, Release 12.2</i>                          |
| Information on IKE phase 1 and phase 2, Aggressive Mode, and Main Mode. | <i>The chapter “Configuring Internet Key Exchange Security Protocol” in the Cisco IOS Security Configuration Guide, Release 12.2</i>    |
| Additional information on IKE dead peer detection.                      | <i>Easy VPN Server, Cisco IOS Release 12.2(8)T feature module</i>                                                                       |

## Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

## MIBs

| MIBs | MIBs Link                                                                                                                                                                                                                                                                                                                |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | <p>To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:</p> <p><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></p> |

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>



## RFCs

| RFCs <sup>1</sup> | Title                                   |
|-------------------|-----------------------------------------|
| RFC 2402          | IP Authentication Header                |
| RFC 2406          | IP Encapsulating Security Payload (ESP) |

1. Not all supported RFCs are listed.

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following commands are introduced or modified in the feature or features

- **crypto isamkp nat keepalive**
- **access-list (IP extended)**
- **show crypto ipsec sa**

For information about these commands, see the Cisco IOS Security Command Reference at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

# Glossary

**IKE**—Internet Key Exchange. Hybrid protocol that implements Oakley key exchange and Skeme key exchange inside the Internet Security Association Key Management Protocol (ISAKMP) framework. Although IKE can be used with other protocols, its initial implementation is with IPSec. IKE provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations (SAs).

**IPSec**—IP Security. Framework of open standards developed by the Internet Engineering Task Force (IETF). IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices (“peers”), such as Cisco routers.

**NAT**—Network Address Translation. Translates a private IP address used inside the corporation to a public, routable address for use on the outside of the corporation, such as the Internet. NAT is considered a one-to-one mapping of addresses from private to public.

**PAT**—Port Address Translation. Like NAT, PAT also translated private IP address to public, routable addresses. Unlike NAT, PAT provides a many-to-one mapping of private addresses to a public address; each instance of the public address is associated with a particular port number to provide uniqueness. PAT can be used in environments where the cost of obtaining a range of public addresses is too expensive for an organization.

**Note**

---

Refer to the [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

---

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



# IPsec Preferred Peer

---

**First Published: March 28, 2005**  
**Last Updated: August 21, 2007**

The IP Security (IPsec) Preferred Peer feature allows you to control the circumstances by which multiple peers on a crypto map are tried in a failover scenario.

This feature includes the following capabilities:

- Default peer configuration
- IPsec idle-timer usage with default peer

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all of the features documented in this module.* To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for IPsec Preferred Peer” section on page 9](#).

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for IPsec Preferred Peer, page 2](#)
- [Restrictions for IPsec Preferred Peer, page 2](#)
- [Information About IPsec Preferred Peer, page 2](#)
- [How to Configure IPsec Preferred Peer, page 4](#)
- [Configuration Examples for IPsec Preferred Peer, page 6](#)
- [Additional References, page 7](#)
- [Command Reference, page 9](#)
- [Feature Information for IPsec Preferred Peer, page 9](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

- [Glossary, page 10](#)

## Prerequisites for IPsec Preferred Peer

- You must have a properly defined, complete crypto map.

## Restrictions for IPsec Preferred Peer

Default peer:

- This feature must be used in conjunction with Dead Peer Detection (DPD). It is most effective on a remote site running DPD in periodic mode. DPD detects the failure of a device quickly and resets the peer list so that the default peer is tried for the next attempted connection.
- Only one peer can be designated as the default peer in a crypto map.
- The default peer must be the first peer in the peer list.

IPsec idle-timer usage with default peer:

- This feature works only on the crypto map for which it is configured. You cannot configure the capability globally for all crypto maps.
- If there is a global idle timer, the crypto map idle-timer value must be different from the global value; otherwise, the idle timer is not added to the crypto map.

## Information About IPsec Preferred Peer

To configure IPsec Preferred Peer, you need to understand the following concepts:

- [IPsec, page 2](#)
- [Dead Peer Detection, page 3](#)
- [Default Peer Configuration, page 3](#)
- [Idle Timers, page 4](#)
- [IPsec Idle-Timer Usage with Default Peer, page 4](#)
- [Peers on Crypto Maps, page 4](#)

## IPsec

IPsec is a framework of open standards developed by the Internet Engineering Task Force (IETF). IPsec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating Internet Protocol (IP) packets between participating IPsec devices (peers), such as Cisco routers.

IPsec provides the following network security services. These services are optional. In general, local security policy dictates the use of one or more of these services:

- **Data Confidentiality**—The IPsec sender can encrypt packets before transmitting them across a network.

- **Data Integrity**—The IPsec receiver can authenticate packets sent by the IPsec sender to ensure that the data has not been altered during transmission.
- **Data Origin Authentication**—The IPsec receiver can authenticate the source of the IPsec packets sent.
- **Anti-Replay**—The IPsec receiver can detect and reject replayed packets.

With IPsec, data can be transmitted across a public network without fear of observation, modification, or spoofing. This enables applications such as Virtual Private Networks (VPNs), including intranets, extranets, and remote user access.

IPsec provides secure tunnels between two peers, such as two routers. You define which packets are considered sensitive and should be sent through these secure tunnels, and you define the parameters that should be used to protect these sensitive packets, by specifying characteristics of these tunnels. When the IPsec peer sees such a sensitive packet, it sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer.

## Dead Peer Detection

The VPN Client uses a keepalive mechanism called Dead Peer Detection (DPD) to check the availability of the VPN device on the other side of an IPsec tunnel. If the network is unusually busy or unreliable, you can increase the number of seconds that the VPN Client will wait before deciding whether the peer is no longer active.

Keepalive packets are not sent if traffic is received. This lowers the overhead associated with DPD, because on a heavily loaded network very few keepalive packets will be sent because traffic is being received on the tunnels. In addition, DPD sends keepalive packets only if there is user traffic to send (and no user traffic is received).

You can configure Internet Key Exchange (IKE) DPD so that DPD sends the keepalive packets whether or not there is outbound user data. That is, as long as there is no inbound user data, the keepalive packets are sent at the configured keepalive interval.

## Default Peer Configuration

If a connection timeout occurs, the connection to the current peer is closed. The **set peer** command allows you to configure the first peer as the default peer. If there is a default peer, the next time a connection is initiated, the connection is directed to the default peer instead of to the next peer in the peer list. If the default peer is unresponsive, the next peer in the peer list becomes the current peer and future connections through the crypto map try that peer.

This capability is useful when traffic on a physical link stops due to the failure of a remote peer. DPD indicates that the remote peer is unavailable, but that peer remains the current peer.

A default peer facilitates the failover to a preferred peer that was previously unavailable, but has returned to service. Users can give preference to certain peers in the event of a failover. This is useful if the original failure was due to a network connectivity problem rather than failure of the remote peer.

## Idle Timers

When a router running Cisco IOS software creates an IPsec security association (SA) for a peer, resources must be allocated to maintain the SA. The SA requires both memory and several managed timers. For idle peers, these resources are wasted. If enough resources are wasted by idle peers, the router could be prevented from creating new SAs with other peers.

IPsec SA idle timers increase the availability of resources by deleting SAs associated with idle peers. Because IPsec SA idle timers prevent the wasting of resources by idle peers, more resources are available to create new SAs when required.

If IPsec SA idle timers are not configured, only the global lifetimes for IPsec SAs are applied. SAs are maintained until the global timers expire, regardless of peer activity.

## IPsec Idle-Timer Usage with Default Peer

If all connections to the current peer time out, the next time a connection is initiated it is directed to the default peer configured in the **set peer** command. If a default peer is not configured and there is a connection timeout, the current peer remains the one that timed out.

This enhancement helps facilitate a failover to a preferred peer that was previously unavailable but is in service now.

## Peers on Crypto Maps

A crypto map set can contain multiple entries, each with a different access list. The router searches the crypto map entries in order, and attempts to match the packet to the access list specified in that entry.

When a packet matches a **permit** entry in a particular access list, and the corresponding crypto map entry is tagged as Cisco, connections are established with the remote peer as specified in the set peer statements within the crypto map.

## How to Configure IPsec Preferred Peer

This section contains the following procedures:

- [Configuring a Default Peer, page 4](#) (required)
- [Configuring the Idle Timer, page 5](#) (optional)

## Configuring a Default Peer

To configure a default peer, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*]

4. **set peer** {*host-name* [dynamic] [default] | *ip-address* [default] }
5. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                       | Purpose                                                                                                                                                                                                                       |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                  | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                              |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                          | Enters global configuration mode.                                                                                                                                                                                             |
| Step 3 | <b>crypto map</b> <i>map-name</i> <i>seq-num</i> [ipsec-isakmp] [dynamic <i>dynamic-map-name</i> ] [discover] [profile <i>profile-name</i> ]<br><br><b>Example:</b><br>Router(config)# crypto map mymap 10 ipsec-isakmp | Enters crypto map configuration mode. Creates or modifies a crypto map entry, creates a crypto profile that provides a template for configuration of dynamically created crypto maps, or configures a client accounting list. |
| Step 4 | <b>set peer</b> { <i>host-name</i> [dynamic] [default]   <i>ip-address</i> [default] }<br><br><b>Example:</b><br>Router(config-crypto-map)# set peer 10.0.0.2 default                                                   | Specifies an IPsec peer in a crypto map entry. Ensures that the first peer specified is defined as the default peer.                                                                                                          |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-crypto-map)# exit                                                                                                                                                   | Exits crypto map configuration mode and returns to global configuration mode.                                                                                                                                                 |

## Configuring the Idle Timer

To configure the idle timer, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name* *seq-num* [ipsec-isakmp] [dynamic *dynamic-map-name*] [discover] [profile *profile-name*]
4. **set security-association idletime** *seconds* [default]
5. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                  | Purpose                                                                                                                                                                                                                       |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                             | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                              |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                     | Enters global configuration mode.                                                                                                                                                                                             |
| Step 3 | <b>crypto map</b> <i>map-name seq-num</i> [ <b>ipsec-isakmp</b> ] [ <b>dynamic</b> <i>dynamic-map-name</i> ] [ <b>discover</b> ] [ <b>profile</b> <i>profile-name</i> ]<br><br><b>Example:</b><br>Router(config)# crypto map mymap 10 ipsec-isakmp | Enters crypto map configuration mode. Creates or modifies a crypto map entry, creates a crypto profile that provides a template for configuration of dynamically created crypto maps, or configures a client accounting list. |
| Step 4 | <b>set security-association idletime</b> <i>seconds</i> [ <b>default</b> ]<br><br><b>Example:</b><br>Router(config-crypto-map)# set security-association idletime 120 default                                                                      | Specifies the maximum amount of time for which the current peer can be idle before the default peer is used.                                                                                                                  |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-crypto-map)# exit                                                                                                                                                                              | Exits crypto map configuration mode and returns to global configuration mode.                                                                                                                                                 |

## Configuration Examples for IPsec Preferred Peer

- [Configuring a Default Peer: Example, page 6](#)
- [Configuring the IPsec Idle Timer: Example, page 6](#)

### Configuring a Default Peer: Example

The following example shows that the first peer, at IP address 10.1.1.1, is the default peer:

```
crypto map tohub 1 ipsec-isakmp
 set peer 10.1.1.1 default
 set peer 10.2.2.2
```

### Configuring the IPsec Idle Timer: Example

In the following example, if the current peer is idle for 120 seconds, the default peer 10.1.1.1 (which was specified in the **set peer** command) is used for the next attempted connection:

```
crypto map tohub 1 ipsec-isakmp
```



```
set peer 10.1.1.1 default
set peer 10.2.2.2
set security-association idletime 120 default
```

## Additional References

The following sections provide references related to IPsec Preferred Peer.

## Related Documents

| Related Topic | Document Title                                                                                                                            |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| IPsec         | <i>Cisco IOS Security Configuration Guide, Release 12.4</i><br><i>Cisco IOS Security Command Reference, Release 12.4T</i>                 |
| Crypto map    | <i>Cisco IOS Security Configuration Guide, Release 12.4</i><br><i>Cisco IOS Security Command Reference, Release 12.4T</i>                 |
| DPD           | <i>IPSec Dead Peer Detection Periodic Message Option, Release 12.3(7)T</i><br><i>Cisco IOS Security Configuration Guide, Release 12.4</i> |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features

- **set peer (IPsec)**
- **set security-association idle-time**

For information about these commands, see the Cisco IOS Security Command Reference at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

## Feature Information for IPsec Preferred Peer

[Table 1](#) lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



### Note

[Table 1](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** *Feature Information for IPsec Preferred Peer*

| Feature Name         | Releases                                | Feature Information                                                                                                                                                                                                                                                                                                                                                         |
|----------------------|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IPsec Preferred Peer | 12.3(14)T<br>12.2(33)SRA<br>12.2(33)SXH | The IPsec Preferred Peer feature allows you to control the circumstances by which multiple peers on a crypto map are tried in a failover scenario.<br><br>In 12.3(14)T, this feature was introduced.<br><br>In 12.2(33)SRA, this feature, the <b>set peer</b> (IPsec) command, and the <b>set security-association idle-time</b> command were integrated into this release. |
| IPSEC Preferred Peer | Cisco IOS XE Release 2.1                | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                               |

## Glossary

**crypto access list**—A list that defines which IP traffic will be protected by crypto and which traffic will not be protected by crypto.

**crypto map**—A map that specifies which traffic should be protected by IPsec, where IPsec-protected traffic should be sent, and what IPsec transform sets should be applied to this traffic.

**dead peer detection**—A feature that allows the router to detect an unresponsive peer.

**keepalive message**—A message sent by one network device to inform another network device that the virtual circuit between the two is still active.

**peer**—Router or other device that participates in IPsec and IKE. In IPsec, peers are devices or entities that communicate securely either through the exchange of keys or the exchange of digital certificates.

**SA**—security association. An instance of security policy and keying material applied to a data flow. Both IKE and IPsec use SAs, although SAs are independent of one another. IPsec SAs are unidirectional and are unique in each security protocol. An IKE SA is used by IKE only, and unlike the IPsec SA, it is bidirectional. IKE negotiates and establishes SAs on behalf of IPsec. A user also can establish IPsec SAs manually. A set of SAs are needed for a protected data pipe, one per direction per protocol. For example, if you have a pipe that supports Encapsulating Security Payload (ESP) between peers, one ESP SA is required for each direction. SAs are identified uniquely by destination (IPsec endpoint) address, security protocol (AH or ESP), and security parameter index (SPI).

**transform set**—An acceptable combination of security protocols, algorithms, and other settings to apply to IPsec-protected traffic. During the IPsec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow.



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





# IPSec Security Association Idle Timers

When a router running the Cisco IOS software creates an IPsec security association (SA) for a peer, resources must be allocated to maintain the SA. The SA requires both memory and several managed timers. For idle peers, these resources are wasted. If enough resources are wasted by idle peers, the router could be prevented from creating new SAs with other peers. The IPsec Security Association Idle Timers feature introduces a configurable idle timer to monitor SAs for activity, allowing SAs for idle peers to be deleted. Benefits of this feature include:

- Increased availability of resources
- Improved scalability of Cisco IOS IPsec deployments

## Feature Specifications for IPsec Security Association Idle Timers

### Feature History

| Release                  | Modification                                                                                                                                       |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.2(15)T                | This feature was introduced.                                                                                                                       |
| 12.3(14)T                | The <b>set security-association idle-time</b> command was added, allowing for the configuration of an IPsec idle timer for a specified crypto map. |
| Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                      |

### Supported Platforms

Cisco 1700 series access routers, Cisco 2400 series integrated access devices, Cisco 2600 series multiservice platforms, Cisco 3600 series multiservice platforms, Cisco 3700 series multiservice access routers, Cisco 7100 series VPN routers, Cisco 7200 series routers, Cisco 7400 series routers, Cisco 7500 series routers, Cisco 801–804 ISDN routers, Cisco 805 serial router, Cisco 806 broadband router, Cisco 811, Cisco 813, Cisco 820, Cisco 827 ADSL router, Cisco 828 G.SHDSL router, Cisco 8850-RPM, Cisco 950, Cisco AS5350 universal gateway, Cisco AS5400 series universal gateways, Cisco integrated communications system 7750, Cisco MC3810 series multiservice access concentrators, Cisco ubr7200, Cisco ubr900 series cable access routers

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



### Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

# Contents

- [Prerequisites for IPsec Security Association Idle Timers, page 2](#)
- [Information About IPsec Security Association Idle Timers, page 2](#)
- [Information About IPsec Security Association Idle Timers, page 2](#)
- [How to Configure IPsec Security Association Idle Timers, page 3](#)
- [Configuration Examples for IPsec Security Association Idle Timers, page 5](#)
- [Additional References, page 5](#)
- [Command Reference, page 7](#)

## Prerequisites for IPsec Security Association Idle Timers

You must configure Internet Key Exchange (IKE) as described in the “[Configuring Internet Key Exchange Security Protocol](#)” chapter of the *Cisco IOS Security Configuration Guide*, Release 12.2.

## Information About IPsec Security Association Idle Timers

To configure the IPsec Security Association Idle Timers feature, you must understand the following concepts:

- [Lifetimes for IPsec Security Associations, page 2](#)
- [IPsec Security Association Idle Timers, page 2](#)
- [Benefits of IPsec Security Association Idle Timers, page 3](#)

## Lifetimes for IPsec Security Associations

The Cisco IOS software currently allows the configuration of lifetimes for IPsec SAs. Lifetimes can be configured globally or per crypto map. There are two lifetimes: a “timed” lifetime and a “traffic-volume” lifetime. A security association expires after the first of these lifetimes is reached.

## IPsec Security Association Idle Timers

The IPsec SA idle timers are different from the global lifetimes for IPsec SAs. The expiration of the global lifetime is independent of peer activity. The IPsec SA idle timer allows SAs associated with inactive peers to be deleted before the global lifetime has expired.

If the IPsec SA idle timers are not configured, only the global lifetimes for IPsec SAs are applied. SAs are maintained until the global timers expire, regardless of peer activity.

**Note**

If the last IPsec SA to a given peer is deleted due to idle timer expiration, the Internet Key Exchange (IKE) SA to that peer will also be deleted.



## Benefits of IPSec Security Association Idle Timers

### Increased Availability of Resources

Configuring the IPSec Security Association Idle Timers feature increases the availability of resources by deleting SAs associated with idle peers.

### Improved Scalability of Cisco IOS IPSec Deployments

Because the IPSec Security Association Idle Timers feature prevents the wasting of resources by idle peers, more resources will be available to create new SAs as required.

## How to Configure IPSec Security Association Idle Timers

- [Configuring the IPSec SA Idle Timer Globally, page 3](#)
- [Configuring the IPSec SA Idle Timer per Crypto Map, page 4](#)

### Configuring the IPSec SA Idle Timer Globally

This task configures the IPSec SA idle timer globally. The idle timer configuration will be applied to all SAs.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec security-association idle-time *seconds***

#### DETAILED STEPS

|        | Command or Action                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                      | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                                          |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                              | Enters global configuration mode.                                                                                                                                                                                                                                                         |
| Step 3 | <b>crypto ipsec security-association idle-time <i>seconds</i></b><br><br><b>Example:</b><br>Router(config)# crypto ipsec security-association idle-time 600 | Configures the IPSec SA idle timer. <ul style="list-style-type: none"><li>• The <i>seconds</i> argument specifies the time, in seconds, that the idle timer will allow an inactive peer to maintain an SA. Valid values for the <i>seconds</i> argument range from 60 to 86400.</li></ul> |

# Configuring the IPsec SA Idle Timer per Crypto Map

This task configures the IPsec SA idle timer for a specified crypto map. The idle timer configuration will be applied to all SAs under the specified crypto map.



Note

This configuration task was available effective with Cisco IOS Release 12.3(14)T.

## SUMMARY STEPS

- 1. **enable**
- 2. **configure terminal**
- 3. **crypto map** *map-name seq-number ipsec-isakmp*
- 4. **set security-association idle-time** *seconds*

## DETAILED STEPS

|        | Command or Action                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                   |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                                                                          |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                       | Enters global configuration mode.                                                                                                                                                                                                                                                                                         |
| Step 3 | <b>crypto map</b> <i>map-name seq-number ipsec-isakmp</i><br><br><b>Example:</b><br>Router(config)# crypto map test 1 ipsec-isakmp                   | Creates or modifies a crypto map entry and enters crypto map configuration mode.                                                                                                                                                                                                                                          |
| Step 4 | <b>set security-association idle-time</b> <i>seconds</i><br><br><b>Example:</b><br>Router(config-crypto-map)# set security-association idle-time 600 | Specifies the maximum amount of time for which the current peer can be idle before the default peer is used. <ul style="list-style-type: none"><li>• The <i>seconds</i> argument is the number of seconds for which the current peer can be idle before the default peer is used. Valid values are 60 to 86400.</li></ul> |

# Configuration Examples for IPSec Security Association Idle Timers

- [Configuring the IPSec SA Idle Timer Globally Example, page 5](#)
- [Configuring the IPSec SA Idle Timer per Crypto Map Example, page 5](#)

## Configuring the IPSec SA Idle Timer Globally Example

The following example globally configures the IPSec SA idle timer to drop SAs for inactive peers after 600 seconds:

```
crypto ipsec security-association idle-time 600
```

## Configuring the IPSec SA Idle Timer per Crypto Map Example

The following example configures the IPSec SA idle timer for the crypto map named test to drop SAs for inactive peers after 600 seconds:

```
crypto map test 1 ipsec-isakmp
set security-association idle-time 600
```

**Note**

---

The above configuration was not available until Cisco IOS Release 12.3(14)T.

---

## Additional References

For additional information related to IPSec Security Association Idle Timers, see the following sections:

- [Related Documents, page 6](#)
- [Standards, page 6](#)
- [MIBs, page 6](#)
- [RFCs, page 7](#)
- [Technical Assistance, page 7](#)

## Related Documents

| Related Topic                                                           | Document Title                                                                                                                    |
|-------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Additional information about configuring IKE                            | “Configuring Internet Key Exchange Security Protocol” chapter of the <i>Cisco IOS Security Configuration Guide</i> , Release 12.2 |
| Additional information about configuring global lifetimes for IPsec SAs | “Configuring IPsec Network Security” chapter of the <i>Cisco IOS Security Configuration Guide</i> , Release 12.2                  |
| Additional Security commands                                            | <i>Cisco IOS Security Command Reference</i> , Release 12.2 T                                                                      |

## Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

## MIBs

| MIBs | MIBs Link                                                                                                                                                                                                                                                                                                         |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:<br><br><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a> |

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

## RFCs

| RFCs | Title |
|------|-------|
| None | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following commands are introduced or modified in the feature or features

- **crypto ipsec security-association idle-time**
- **set security-association idle-time**

For information about these commands, see the Cisco IOS Security Command Reference at

[http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at

<http://tools.cisco.com/Support/CLILookup> or the Master Command List.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





# IPSec—SNMP Support

## Feature History

| Release                  | Modification                                                                                                                                                                                                                                                                           |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.1(4)E                 | This feature was introduced on the Cisco 7100, 7200, and 7500 series.                                                                                                                                                                                                                  |
| 12.1(5a)E                | Support for CISCO-IPSEC-FLOW-MONITOR-MIB notifications was added.                                                                                                                                                                                                                      |
| 12.2(4)T                 | Support for this feature was added for platforms in Release 12.2 T.                                                                                                                                                                                                                    |
| 12.2(8)T, 12.1(11b)E     | The following Command Line Interface (CLI) commands were added to enable and disable IP Security (IPSec) MIB notifications: <ul style="list-style-type: none"><li>• <a href="#">snmp-server enable traps ipsec</a></li><li>• <a href="#">snmp-server enable traps isakmp</a></li></ul> |
| 12.2(14)S                | This feature was integrated into Cisco IOS Release 12.2(14)S.                                                                                                                                                                                                                          |
| Cisco IOS XE Release 2.1 | This feature was introduced on the Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                      |

This document describes the IPSec—SNMP Support feature in Cisco IOS Release 12.1 E, 12.2 T, and 12.2 S and includes the following sections:

- [Feature Overview, page 2](#)
- [Supported Platforms, page 3](#)
- [Supported Standards, MIBs, and RFCs, page 5](#)
- [Configuration Tasks, page 5](#)
- [Monitoring and Maintaining IPSec MIB, page 7](#)
- [Configuration Examples, page 7](#)
- [Command Reference, page 8](#)
- [Glossary, page 9](#)



**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

**Note**

This document focuses on Cisco IOS CLI support for the Cisco IPSec MIBs. This document also lists which elements of the MIBs are currently supported. This document does not describe SNMP configuration (from a Network Management Station) of the Cisco IPSec MIBs.

## Feature Overview

The IP Security (IPSec) - SNMP Support feature introduces support for industry-standard IPSec MIBs and Cisco IOS-software specific IPSec MIBs.

The IPSec MIBs allow IPSec configuration monitoring and IPSec status monitoring using SNMP, and can be integrated in a variety of Virtual Private Network (VPN) management solutions.

For example, this feature allows you to specify the desired size of a tunnel history table or a tunnel failure table using the Cisco IOS CLI. The history table archives attribute and statistic information about the tunnel; the failure table archives tunnel failure reasons along with the time failure occurred. A failure history table can be used as a simple method to distinguish between a normal and an abnormal tunnel termination. That is, if a tunnel entry in the tunnel history table has no associated failure record, the tunnel must have terminated normally. However, a tunnel history table does not accompany every failure table because every failure does not correspond to a tunnel. Thus, supported setup failures are recorded in the failure table, but an associated history table is not recorded because a tunnel was never set up.

This feature also provides IPSec Simple Network Management Protocol (SNMP) notifications for use with network management systems.

## Benefits

The commands in this feature allow you to examine the version of the IPSec MIB feature, to enable and disable SNMP traps, and to monitor and control the size of the buffers used by this feature.

## Restrictions

Only the following tunnel setup failure logs are supported with the IPSec - SNMP Support feature:

- NOTIFY\_MIB\_IPSEC\_PROPOSAL\_INVALID  
“A tunnel could not be established because the peer did not supply an acceptable proposal.”
- NOTIFY\_MIB\_IPSEC\_ENCRYPT\_FAILURE  
“A tunnel could not be established because it failed to encrypt a packet to be sent to a peer.”
- NOTIFY\_MIB\_IPSEC\_SYSCAP\_FAILURE  
“A tunnel could not be established because the system ran out of resources.”
- NOTIFY\_MIB\_IPSEC\_LOCAL\_FAILURE  
“A tunnel could not be established because of an internal error.”

Note that these failure notices are recorded in the failure tables, but are not available as SNMP notifications (traps).



The following functions are not supported with the IPSec MIB feature:

- Checkpointing
- The Dynamic Cryptomap table of the CISCO-IPSEC-MIB

**Note**

CISCO-IPSEC-FLOW-MONITOR-MIB notifications are not supported before Cisco IOS Release 12.1(5a)E.

The CISCO-IPSEC-POLICY-MAP-MIB (ciscoIpSecPolMap) defines no notifications (the “IPSec Policy Map Notifications Group” is empty).

## Related Features and Technologies

The IPSec—SNMP Support feature was designed to support the VPN Device Manager (VDM). VDM enables network administrators to manage and configure site-to-site VPNs on a single device from a web browser and to see the effects of changes in real time. VDM implements a wizard-based graphical user interface (GUI) to simplify the process of configuring site-to-site VPNs using the IPSec protocol. VDM software is installed directly on Cisco VPN routers, and is designed for use and compatibility with future Device Manager products.

For more information on Cisco VDM, refer to the following URL:

<http://www.cisco.com/warp/public/cc/pd/nemnsw/vpdvmn/>

## Related Documents

### IPSec and Related Security Information

- Cisco IOS Security Configuration Guide
- Cisco IOS Security Command Reference

### SNMP Configuration Information

- Cisco IOS Configuration Fundamentals Configuration Guide
- *Cisco IOS Configuration Fundamentals Command Reference*

For the Cisco IOS Release 12.1 E implementation of security and SNMP features, refer to the Cisco IOS Release 12.1 versions of these documents. For Cisco IOS Release 12.2 T and 12.2 S implementation of these features, refer to the Cisco IOS Release 12.2 versions of these documents.

## Supported Platforms

The IPSec MIB feature is supported on the following platforms in Cisco IOS Release 12.1(4)E:

- Cisco 7100 series
- Cisco 7200 series
- Cisco 7500 series (RSP7000 and 7500)

The IPSec MIB feature is supported on the following platforms in Cisco IOS Release 12.2(4)T:

- Cisco 800 series (800, 805, 806, 820, 827, 828)

- Cisco 900 series
- Cisco 1600 and 1600R series
- Cisco 1700 series (1710, 1720, 1750, 1751, 1760)
- Cisco 2400 series
- Cisco 2600 and 2600XM series
- Cisco 3600 series (Cisco 3620, 3640, and 3660)
- Cisco 3745
- Cisco 4000
- Cisco 4500
- Cisco 5300 series
- Cisco 5400 series
- Cisco 5800 series
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7400 series
- Cisco 7500 series (Cisco IOS Release 12.2(4)T2 and later releases)
- Cisco 7700 series
- Cisco MC3810
- Cisco uBR900 series (uBR900, uBR904, uBR905, uBR910, uBR920, uBR925)
- Cisco uBR7200

The IPSec MIB feature is supported on the following platforms in Cisco IOS Release 12.2(14)S:

- Cisco 7200 series
- Cisco 7400 series
- Cisco 7500 series

#### **Determining Platform Support Through Cisco Feature Navigator**

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

#### **Availability of Cisco IOS Software Images**

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

## **Supported Standards, MIBs, and RFCs**

### **Standards**

No new or modified standards are supported by this feature.

### **MIBs**

The following MIBs are supported by the IPSec—SNMP Support feature:

- CISCO-IPSEC-FLOW-MONITOR- MIB
- CISCO-IPSEC-MIB
- CISCO-IPSEC-POLICY-MAP-MIB

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

### **RFCs**

No new or modified RFCs are supported by this feature.

## **Configuration Tasks**

See the following sections for configuration tasks for the IPSec—SNMP Support feature. Each task in the list is identified as either required or optional:

- [Enabling IPSec SNMP Notifications](#) (required)

- [Configuring IPSec Failure History Table Size](#) (optional)
- [Configuring IPSec Tunnel History Table Size](#) (optional)

## Enabling IPSec SNMP Notifications

To enable a router to send IPSec trap or inform notifications to a specified host, use the following commands in global configuration mode:

|               | Command                                                                                                | Purpose                                                        |
|---------------|--------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>snmp-server enable traps ipsec cryptomap</b> [add   delete   attach   detach]       | Enables a router to send IPSec SNMP notifications.             |
| <b>Step 2</b> | Router(config)# <b>snmp-server enable traps isakmp</b> [policy {add   delete}   tunnel {start   stop}] | Enables a router to send IPSec ISAKMP SNMP notifications.      |
| <b>Step 3</b> | Router(config)# <b>snmp-server host</b> host-address <b>traps</b> community-string <b>ipsec</b>        | Specifies the recipient of IPSec SNMP notification operations. |

For more information on configuring SNMP, refer to the chapter “Configuring SNMP Support” in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

## Configuring IPSec Failure History Table Size

The default failure history table size is 200. To change the size of the failure history table, use the following command in global configuration mode:

| Command                                                                     | Purpose                                              |
|-----------------------------------------------------------------------------|------------------------------------------------------|
| Router(config)# <b>crypto mib ipsec flowmib history failure size</b> number | Changes the size of the IPSec failure history table. |

## Configuring IPSec Tunnel History Table Size

The default tunnel history table size is 200. To change the size of the tunnel history table, use the following command in global configuration mode:

| Command                                                                    | Purpose                                             |
|----------------------------------------------------------------------------|-----------------------------------------------------|
| Router(config)# <b>crypto mib ipsec flowmib history tunnel size</b> number | Changes the size of the IPSec tunnel history table. |

## Verifying IPSec MIB Configuration

To verify that the IPSec MIB feature is configured properly, perform the following tasks:

- Enter the **show crypto mib ipsec flowmib history failure size** privileged EXEC command to display the size of the failure history table:

```
Router# show crypto mib ipsec flowmib history failure size
```

```
IPSec Failure Window Size: 140
```

- Enter the **show crypto mib ipsec flowmib history tunnel size** privileged EXEC command to display the size of the tunnel history table:

```
Router# show crypto mib ipsec flowmib history tunnel size
IPSec History Window Size: 130
```

- Enter the **show crypto mib ipsec flowmib version** privileged EXEC command to display the MIB version used by the management applications to identify the feature set:

```
Router# show crypto mib ipsec flowmib version
IPSec Flow MIB version: 1
```

- Enter the **debug crypto mib** command to display the IPSec MIB debug message notifications:

```
Router# debug crypto mib
Crypto IPSec Mgmt Entity debugging is on
```

## Monitoring and Maintaining IPSec MIB

To monitor the status of IPSec MIB information, use any of the following commands in EXEC mode:

| Command                                                           | Purpose                                                 |
|-------------------------------------------------------------------|---------------------------------------------------------|
| Router# <b>show crypto mib ipsec flowmib history failure size</b> | Displays the size of the IPSec failure history table.   |
| Router# <b>show crypto mib ipsec flowmib history tunnel size</b>  | Displays the size of the IPSec tunnel history table.    |
| Router# <b>show crypto mib ipsec flowmib version</b>              | Displays the IPSec Flow MIB version used by the router. |

## Configuration Examples

This section provides the following configuration examples:

- [Enabling IPSec Notifications Examples](#)
- [Specifying History Table Size Examples](#)

### Enabling IPSec Notifications Examples

In the following example, IPSec notifications are enabled:

```
snmp-server enable traps ipsec isakmp
```

In the following example, the router is configured to send IPSec notifications to the host nms1.cisco.com:

```
snmp-server host nms1.cisco.com public ipsec isakmp
Translating "nms1.cisco.com"...domain server (171.00.0.01) [OK]
```

## Specifying History Table Size Examples

In the following example, the specified failure history table size is 140:

```
crypto mib ipsec flowmib history failure size 140
```

In the following example, the specified tunnel history table size is 130:

```
crypto mib ipsec flowmib history tunnel size 130
```

## Command Reference

The following commands are introduced or modified in the feature or features

- **crypto mib ipsec flowmib history failure size**
- **crypto mib ipsec flowmib history tunnel size**
- **debug crypto mib**
- **show crypto mib ipsec flowmib history failure size**
- **show crypto mib ipsec flowmib history tunnel size**
- **show crypto mib ipsec flowmib version**
- **snmp-server enable traps ipsec**
- **snmp-server enable traps isakmp**
- **snmp-server host**

For information about these commands, see the *Cisco IOS Security Command Reference* at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

# Glossary

**CA**—certificate authority. A certificate authority (CA) is an entity in a network that issues and manages security credentials and public keys (in the form of X509v3 certificates) for message encryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate. Certificates generally include the owner's public key, the expiration date of the certificate, the owner's name, and other information about the public key owner.

**IP Security**—See IPSec.

**IPSec**—Internet Protocol Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses Internet Key Exchange (IKE) to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

**Management Information Base**—See MIB.

**MIB**—Management Information Base. Database of network management information that is used and maintained by a network management protocol such as Simple Network Management Protocol (SNMP) or Common Management Information Protocol (CMIP). The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a graphical user interface (GUI) network management system (NMS). MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

**Simple Network Management Protocol**—See SNMP.

**SNMP**—Simple Network Management Protocol. An application-layer protocol that provides a message format for communication between SNMP managers and agents.

**trap**—Message sent by an SNMP agent to a network management system, console, or terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached.

---

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.







# IPsec Virtual Tunnel Interface

---

**First Published: October 18, 2004**

**Last Updated: June 11, 2008**

IP security (IPsec) virtual tunnel interfaces (VTIs) provide a routable interface type for terminating IPsec tunnels and an easy way to define protection between sites to form an overlay network. IPsec VTIs simplify configuration of IPsec for protection of remote links, support multicast, and simplify network management and load balancing.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for IPsec Virtual Tunnel Interface”](#) section on page 24.

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Restrictions for IPsec Virtual Tunnel Interface, page 2](#)
- [Information About IPsec Virtual Tunnel Interface, page 2](#)
- [How to Configure IPsec Virtual Tunnel Interface, page 7](#)
- [Configuration Examples for IPsec Virtual Tunnel Interface, page 10](#)
- [Additional References, page 21](#)
- [Command Reference, page 23](#)
- [Feature Information for IPsec Virtual Tunnel Interface, page 24](#)



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2008 Cisco Systems, Inc. All rights reserved.

# Restrictions for IPsec Virtual Tunnel Interface

## IPsec Transform Set

The IPsec transform set must be configured in tunnel mode only.

## IKE Security Association

The Internet Key Exchange (IKE) security association (SA) is bound to the VTI. Because IKE SA is bound to the VTI, the same IKE SA cannot be used for a crypto map.

## IPsec SA Traffic Selectors

Static VTIs support only a single IPsec SA that is attached to the VTI interface. The traffic selector for the IPsec SA is always “IP any any.”

A dynamic VTI also is a point-point interface that supports only a single IPsec SA, but the dynamic VTI is flexible in that it can accept the IPsec selectors that are proposed by the initiator.

## Proxy

Static VTIs support only the “IP any any” proxy.

Dynamic VTIs support only one proxy, which can be “IP any any” or any subset of it.

## QoS Traffic Shaping

The shaped traffic is process switched.

## Stateful Failover

IPsec stateful failover is not supported with IPsec VTIs.

## Tunnel Protection

The **shared** keyword is not required and must not be configured when using the **tunnel mode ipsec ipv4** command for IPsec IPv4 mode.

## Static VTIs Versus GRE Tunnels

The IPsec VTI is limited to IP unicast and multicast traffic only, as opposed to GRE tunnels, which have a wider application for IPsec implementation.

## VRF-Aware IPsec Configuration

In VRF-aware IPsec configurations with either static or dynamic VTIs (DVTIs), the VRF must *not* be configured in the Internet Security Association and Key Management Protocol (ISAKMP) profile.

Instead, the VRF must be configured on the tunnel interface for static VTIs. For DVTIs, you must apply VRF to the vtemplate using the **ip vrf forwarding** command.

# Information About IPsec Virtual Tunnel Interface

The use of IPsec VTIs both greatly simplifies the configuration process when you need to provide protection for remote access and provides a simpler alternative to using generic routing encapsulation (GRE) or Layer 2 Tunneling Protocol (L2TP) tunnels for encapsulation and crypto maps with IPsec. A major benefit associated with IPsec VTIs is that the configuration does not require a static mapping of

IPsec sessions to a physical interface. The IPsec tunnel endpoint is associated with an actual (virtual) interface. Because there is a routable interface at the tunnel endpoint, many common interface capabilities can be applied to the IPsec tunnel.

The IPsec VTI allows for the flexibility of sending and receiving both IP unicast and multicast encrypted traffic on any physical interface, such as in the case of multiple paths. Traffic is encrypted or decrypted when it is forwarded from or to the tunnel interface and is managed by the IP routing table. Using IP routing to forward the traffic to the tunnel interface simplifies the IPsec VPN configuration compared to the more complex process of using access control lists (ACLs) with the crypto map in native IPsec configurations. DVTIs function like any other real interface so that you can apply quality of service (QoS), firewall, and other security services as soon as the tunnel is active.

Without Virtual Private Network (VPN) Acceleration Module2+ (VAM2+) accelerating virtual interfaces, the packet traversing an IPsec virtual interface is directed to the router processor (RP) for encapsulation. This method tends to be slow and has limited scalability. In hardware crypto mode, all the IPsec VTIs are accelerated by the VAM2+ crypto engine, and all traffic going through the tunnel is encrypted and decrypted by the VAM2+.

The following sections provide details about the IPsec VTI:

- [Benefits of Using IPsec Virtual Tunnel Interfaces, page 3](#)
- [Routing with IPsec Virtual Tunnel Interfaces, page 5](#)
- [Static Virtual Tunnel Interfaces, page 3](#)
- [Dynamic Virtual Tunnel Interfaces, page 4](#)
- [Dynamic Virtual Tunnel Interface Life Cycle, page 5](#)
- [Traffic Encryption with the IPsec Virtual Tunnel Interface, page 6](#)

## Benefits of Using IPsec Virtual Tunnel Interfaces

IPsec VTIs allow you to configure a virtual interface to which you can apply features. Features for clear-text packets are configured on the VTI. Features for encrypted packets are applied on the physical outside interface. When IPsec VTIs are used, you can separate the application of features such as NAT, ACLs, and QoS and apply them to clear-text or encrypted text, or both. When crypto maps are used, there is no simple way to apply encryption features to the IPsec tunnel.

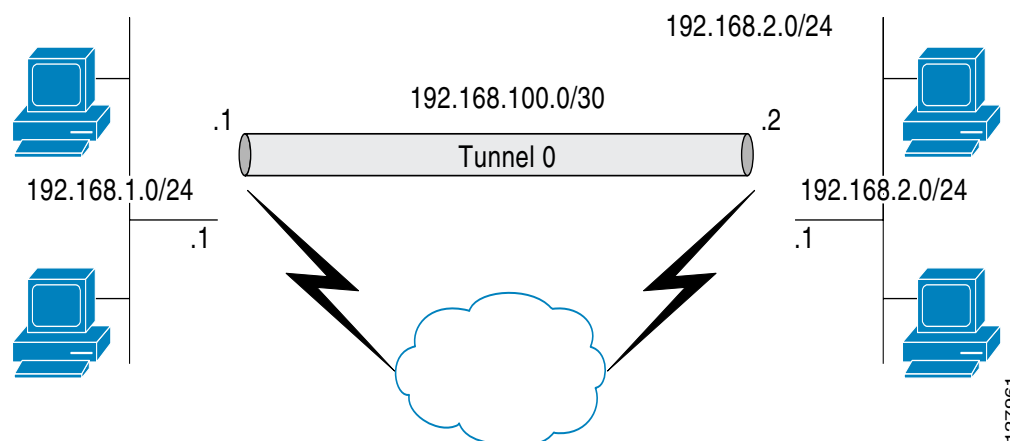
There are two types of VTI interfaces: static VTIs (SVTIs) and dynamic VTIs (DVTIs).

## Static Virtual Tunnel Interfaces

SVTI configurations can be used for site-to-site connectivity in which a tunnel provides always-on access between two sites. The advantage of using SVTIs as opposed to crypto map configurations is that users can enable dynamic routing protocols on the tunnel interface without the extra 4 bytes required for GRE headers, thus reducing the bandwidth for sending encrypted data.

Additionally, multiple Cisco IOS software features can be configured directly on the tunnel interface and on the physical egress interface of the tunnel interface. This direct configuration allows users to have solid control on the application of the features in the pre- or post-encryption path.

[Figure 1](#) illustrates how a static VTI is used.

**Figure 1** *IPsec Static VTI*

The IPsec VTI supports native IPsec tunneling and exhibits most of the properties of a physical interface.

## Dynamic Virtual Tunnel Interfaces

DVTIs can provide highly secure and scalable connectivity for remote-access VPNs. The DVTI technology replaces dynamic crypto maps and the dynamic hub-and-spoke method for establishing tunnels.

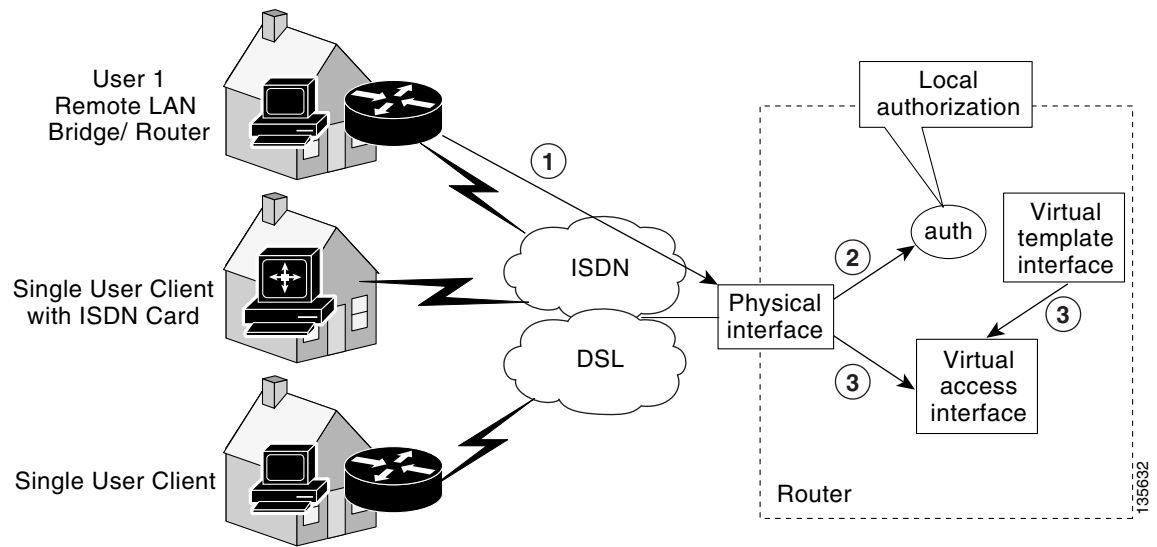
Dynamic VTIs can be used for both the server and remote configuration. The tunnels provide an on-demand separate virtual access interface for each VPN session. The configuration of the virtual access interfaces is cloned from a virtual template configuration, which includes the IPsec configuration and any Cisco IOS software feature configured on the virtual template interface, such as QoS, NetFlow, or ACLs.

Dynamic VTIs function like any other real interface so that you can apply QoS, firewall, other security services as soon as the tunnel is active. QoS features can be used to improve the performance of various applications across the network. Any combination of QoS features offered in Cisco IOS software can be used to support voice, video, or data applications.

Dynamic VTIs provide efficiency in the use of IP addresses and provide secure connectivity. Dynamic VTIs allow dynamically downloadable per-group and per-user policies to be configured on a RADIUS server. The per-group or per-user definition can be created using extended authentication (Xauth) User or Unity group, or it can be derived from a certificate. Dynamic VTIs are standards based, so interoperability in a multiple-vendor environment is supported. IPsec DVTIs allow you to create highly secure connectivity for remote access VPNs and can be combined with Cisco Architecture for Voice, Video, and Integrated Data (AVVID) to deliver converged voice, video, and data over IP networks. The DVTI simplifies Virtual Private Network (VRF) routing and forwarding- (VRF-) aware IPsec deployment. The VRF is configured on the interface.

A DVTI requires minimal configuration on the router. A single virtual template can be configured and cloned.

The DVTI creates an interface for IPsec sessions and uses the virtual template infrastructure for dynamic instantiation and management of dynamic IPsec VTIs. The virtual template infrastructure is extended to create dynamic virtual-access tunnel interfaces. Dynamic VTIs are used in hub-and-spoke configurations. A single DVTI can support several static VTIs. [Figure 2](#) illustrates the DVTI authentication path.

**Figure 2**      **Dynamic IPsec VTI**

The authentication shown in [Figure 2](#) follows this path:

1. User 1 calls the router.
2. Router 1 authenticates User 1.
3. IPsec clones virtual access interface from virtual template interface.

## Dynamic Virtual Tunnel Interface Life Cycle

IPsec profiles define policy for dynamic VTIs. The dynamic interface is created at the end of IKE Phase 1 and IKE Phase 1.5. The interface is deleted when the IPsec session to the peer is closed. The IPsec session is closed when both IKE and IPsec SAs to the peer are deleted.

## Routing with IPsec Virtual Tunnel Interfaces

Because VTIs are routable interfaces, routing plays an important role in the encryption process. Traffic is encrypted only if it is forwarded out of the VTI, and traffic arriving on the VTI is decrypted and routed accordingly. VTIs allow you to establish an encryption tunnel using a real interface as the tunnel endpoint. You can route to the interface or apply services such as QoS, firewalls, network address translation, and Netflow statistics as you would to any other interface. You can monitor the interface, route to it, and it has an advantage over crypto maps because it is a real interface and provides the benefits of any other regular Cisco IOS interface.



### Note

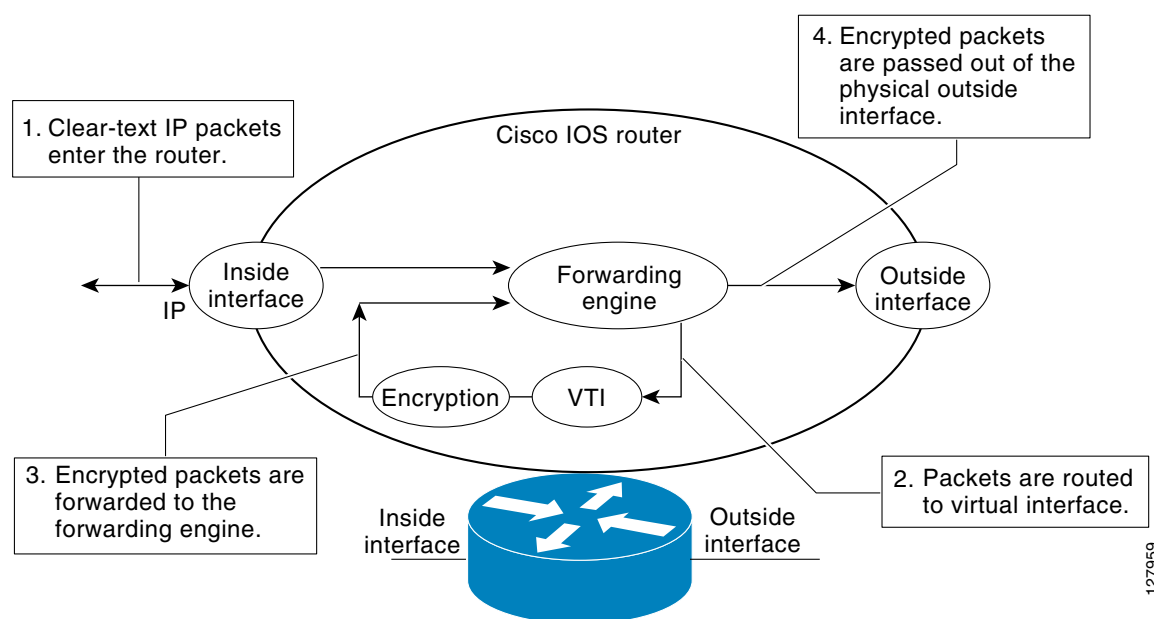
Dynamic routing can be used with SVTIs. Routing with DVTIs is **not** supported or recommended.

## Traffic Encryption with the IPsec Virtual Tunnel Interface

When an IPsec VTI is configured, encryption occurs in the tunnel. Traffic is encrypted when it is forwarded to the tunnel interface. Traffic forwarding is handled by the IP routing table, and dynamic or static routing can be used to route traffic to the SVTI. DVTI uses reverse route injection to further simplify the routing configurations. Using IP routing to forward the traffic to encryption simplifies the IPsec VPN configuration because the use of ACLs with a crypto map in native IPsec configurations is not required. The IPsec virtual tunnel also allows you to encrypt multicast traffic with IPsec.

IPsec packet flow into the IPsec tunnel is illustrated in [Figure 3](#).

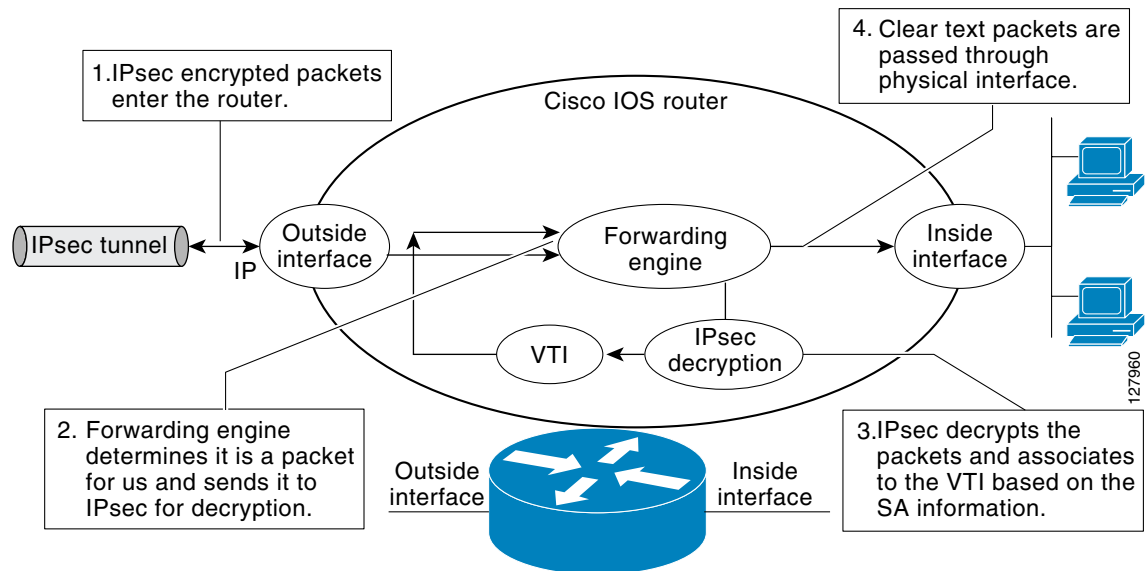
**Figure 3** Packet Flow into the IPsec Tunnel



After packets arrive on the inside interface, the forwarding engine switches the packets to the VTI, where they are encrypted. The encrypted packets are handed back to the forwarding engine, where they are switched through the outside interface.

[Figure 4](#) shows the packet flow out of the IPsec tunnel.

**Figure 4** Packet Flow out of the IPsec Tunnel



## How to Configure IPsec Virtual Tunnel Interface

- [Configuring Static IPsec Virtual Tunnel Interfaces, page 7](#)
- [Configuring Dynamic IPsec Virtual Tunnel Interfaces, page 9](#)

### Configuring Static IPsec Virtual Tunnel Interfaces

This configuration shows how to configure a static IPsec VTI.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto IPsec profile** *profile-name*
4. **set transform-set** *transform-set-name*
5. **interface** *type number*
6. **ip address** *address mask*
7. **tunnel mode ipsec ipv4**
8. **tunnel source** *interface*
9. **tunnel destination** *ip-address*
10. **tunnel protection IPsec profile** *profile-name* [**shared**]

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                    | Purpose                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                       | Enters global configuration mode.                                                                                |
| Step 3 | <b>crypto IPsec profile</b> <i>profile-name</i><br><br><b>Example:</b><br>Router(config)# crypto IPsec profile PROF                                                                  | Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers.                 |
| Step 4 | <b>set transform-set</b> <i>transform-set-name</i><br>[ <i>transform-set-name2</i> ... <i>transform-set-name6</i> ]<br><br><b>Example:</b><br>Router(config)# set transform-set tset | Specifies which transform sets can be used with the crypto map entry.                                            |
| Step 5 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface tunnel0                                                                                      | Specifies the interface on which the tunnel will be configured and enters interface configuration mode.          |
| Step 6 | <b>ip address</b> <i>address mask</i><br><br><b>Example:</b><br>Router(config-if)# ip address 10.1.1.1<br>255.255.255.0                                                              | Specifies the IP address and mask.                                                                               |
| Step 7 | <b>tunnel mode ipsec ipv4</b><br><br><b>Example:</b><br>Router(config-if)# tunnel mode ipsec ipv4                                                                                    | Defines the mode for the tunnel.                                                                                 |
| Step 8 | <b>tunnel source</b> <i>interface</i><br><br><b>Example:</b><br>Router(config-if)# tunnel source loopback0                                                                           | Specifies the tunnel source as a loopback interface.                                                             |



|         | Command or Action                                                                                                                                                    | Purpose                                              |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| Step 9  | <b>tunnel destination</b> <i>ip-address</i><br><br><b>Example:</b><br>Router(config-if)# tunnel destination<br>172.16.1.1                                            | Identifies the IP address of the tunnel destination. |
| Step 10 | <b>tunnel protection IPsec profile</b> <i>profile-name</i><br>[ <b>shared</b> ]<br><br><b>Example:</b><br>Router(config-if)# tunnel protection IPsec<br>profile PROF | Associates a tunnel interface with an IPsec profile. |

## Configuring Dynamic IPsec Virtual Tunnel Interfaces

This task shows how to configure a dynamic IPsec VTI.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto IPsec profile** *profile-name*
4. **set transform-set** *transform-set-name*
5. **interface virtual-template** *number*
6. **tunnel mode** *mode*
7. **tunnel protection IPsec profile** *profile-name* [**shared**]
8. **exit**
9. **crypto isakamp profile** *profile-name*
10. **virtual-template** *template-number*

### DETAILED STEPS

|        | Command or Action                                                              | Purpose                                                                                                            |
|--------|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                  |

|         | Command or Action                                                                                                                                                                    | Purpose                                                                                          |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Step 3  | <b>crypto IPsec profile</b> <i>profile-name</i><br><br><b>Example:</b><br>Router(config)# crypto IPsec profile PROF                                                                  | Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers. |
| Step 4  | <b>set transform-set</b> <i>transform-set-name</i><br>[ <i>transform-set-name2</i> ... <i>transform-set-name6</i> ]<br><br><b>Example:</b><br>Router(config)# set transform-set tset | Specifies which transform sets can be used with the crypto map entry.                            |
| Step 5  | <b>interface virtual-template</b> <i>number</i><br><br><b>Example:</b><br>Router(config)# interface virtual-template 2                                                               | Defines a virtual-template tunnel interface and enters interface configuration mode.             |
| Step 6  | <b>tunnel mode ipsec ipv4</b><br><br><b>Example:</b><br>Router(config-if)# tunnel mode ipsec ipv4                                                                                    | Defines the mode for the tunnel.                                                                 |
| Step 7  | <b>tunnel protection IPsec profile</b> <i>profile-name</i><br>[ <i>shared</i> ]<br><br><b>Example:</b><br>Router(config-if)# tunnel protection IPsec profile PROF                    | Associates a tunnel interface with an IPsec profile.                                             |
| Step 8  | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                                                        | Exits interface configuration mode.                                                              |
| Step 9  | <b>crypto isakamp profile</b> <i>profile-name</i><br><br><b>Example:</b><br>Router(config)# crypto isakamp profile red                                                               | Defines the ISAKAMP profile to be used for the virtual template.                                 |
| Step 10 | <b>virtual-template</b> <i>template-number</i><br><br><b>Example:</b><br>Router(config)# virtual-template 1                                                                          | Specifies the virtual template attached to the ISAKAMP profile.                                  |

## Configuration Examples for IPsec Virtual Tunnel Interface

The following examples are provided to illustrate configuration scenarios for IPsec VTIs:

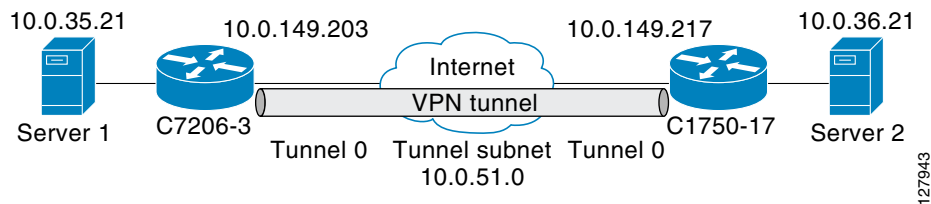
- [Static Virtual Tunnel Interface with IPsec: Example, page 11](#)
- [VRF-Aware Static Virtual Tunnel Interface: Example, page 14](#)
- [Static Virtual Tunnel Interface with QoS: Example, page 14](#)
- [Static Virtual Tunnel Interface with Virtual Firewall: Example, page 15](#)

- [Dynamic Virtual Tunnel Interface Easy VPN Server: Example, page 16](#)
- [Dynamic Virtual Tunnel Interface Easy VPN Client: Example, page 18](#)
- [VRF-Aware IPsec with Dynamic VTI: Example, page 20](#)
- [Dynamic Virtual Tunnel Interface with Virtual Firewall: Example, page 20](#)
- [Dynamic Virtual Tunnel Interface with QoS: Example, page 21](#)

## Static Virtual Tunnel Interface with IPsec: Example

The following example configuration uses a preshared key for authentication between peers. VPN traffic is forwarded to the IPsec VTI for encryption and then sent out the physical interface. The tunnel on subnet 10 checks packets for IPsec policy and passes them to the Crypto Engine (CE) for IPsec encapsulation. [Figure 5](#) illustrates the IPsec VTI configuration.

**Figure 5** VTI with IPsec



### C7206 Router Configuration

```

version 12.3

service timestamps debug datetime
service timestamps log datetime
hostname 7200-3
no aaa new-model
ip subnet-zero
ip cef
controller ISA 6/1
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
group 2
crypto isakmp key Cisco12345 address 0.0.0.0 0.0.0.0
crypto IPsec transform-set T1 esp-3des esp-sha-hmac
crypto IPsec profile P1
set transform-set T1
!

interface Tunnel0
 ip address 10.0.51.203 255.255.255.0
 ip ospf mtu-ignore
 load-interval 30
 tunnel source 10.0.149.203
 tunnel destination 10.0.149.217
 tunnel mode IPsec ipv4
 tunnel protection IPsec profile P1

```

```

!
interface Ethernet3/0
 ip address 10.0.149.203 255.255.255.0
 duplex full
!
interface Ethernet3/3
 ip address 10.0.35.203 255.255.255.0
 duplex full
!
ip classless
ip route 10.0.36.0 255.255.255.0 Tunnel0
line con 0
line aux 0
line vty 0 4
end

```

### C1750 Router Configuration

```

version 12.3

hostname c1750-17
no aaa new-model
ip subnet-zero
ip cef
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2

crypto isakmp key Cisco12345 address 0.0.0.0 0.0.0.0
crypto IPsec transform-set T1 esp-3des esp-sha-hmac
crypto IPsec profile P1
 set transform-set T1
!
interface Tunnel0
 ip address 10.0.51.217 255.255.255.0
 ip ospf mtu-ignore
 tunnel source 10.0.149.217
 tunnel destination 10.0.149.203
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile P1
!
interface FastEthernet0/0
 ip address 10.0.149.217 255.255.255.0
 speed 100
 full-duplex
!
interface Ethernet1/0
 ip address 10.0.36.217 255.255.255.0
 load-interval 30
 full-duplex
!

ip classless
ip route 10.0.35.0 255.255.255.0 Tunnel0
line con 0
line aux 0
line vty 0 4
end

```

## Verifying the Results for the IPsec Static Virtual Tunnel Interface: Example

This section provides information that you can use to confirm that your configuration is working properly. In this display, Tunnel 0 is “up,” and the line protocol is “up.” If the line protocol is “down,” the session is not active.

### Verifying the C7206 Status

```
Router# show interface tunnel 0
```

```
Tunnel0 is up, line protocol is up
Hardware is Tunnel
Internet address is 10.0.51.203/24
MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
reliability 255/255, txload 103/255, rxload 110/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 10.0.149.203, destination 10.0.149.217
Tunnel protocol/transport IPsec/IP, key disabled, sequencing disabled
Tunnel TTL 255

Checksumming of packets disabled, fast tunneling enabled
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Tunnel protection via IPsec (profile "P1")
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 1/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
30 second input rate 13000 bits/sec, 34 packets/sec
30 second output rate 36000 bits/sec, 34 packets/sec
191320 packets input, 30129126 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
59968 packets output, 15369696 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
```

```
Router# show crypto session
```

```
Crypto session current status
Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.149.217 port 500
IKE SA: local 10.0.149.203/500 remote 10.0.149.217/500 Active
IPsec FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 4, origin: crypto map
```

```
Router# show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C 10.0.35.0/24 is directly connected, Ethernet3/3
S 10.0.36.0/24 is directly connected, Tunnel0
```

```
C 10.0.51.0/24 is directly connected, Tunnel0
C 10.0.149.0/24 is directly connected, Ethernet3/0
```

## VRF-Aware Static Virtual Tunnel Interface: Example

To add VRF to the static VTI example, include the **ip vrf** and **ip vrf forwarding** commands to the configuration as shown in the following example.

### C7206 Router Configuration

```
hostname c7206
.
.
ip vrf sample-vti1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
.
.
interface Tunnel0
 ip vrf forwarding sample-vti1
 ip address 10.0.51.217 255.255.255.0
 tunnel source 10.0.149.217
 tunnel destination 10.0.149.203
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile P1
.
.
!
end
```

## Static Virtual Tunnel Interface with QoS: Example

You can apply any QoS policy to the tunnel endpoint by including the **service-policy** statement under the tunnel interface. The following example is policing traffic out the tunnel interface.

### C7206 Router Configuration

```
hostname c7206
.
.
class-map match-all VTI
 match any
!
policy-map VTI
 class VTI
 police cir 2000000
 conform-action transmit
 exceed-action drop
!
.
.
interface Tunnel0
 ip address 10.0.51.217 255.255.255.0
 tunnel source 10.0.149.217
 tunnel destination 10.0.149.203
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile P1
```

```

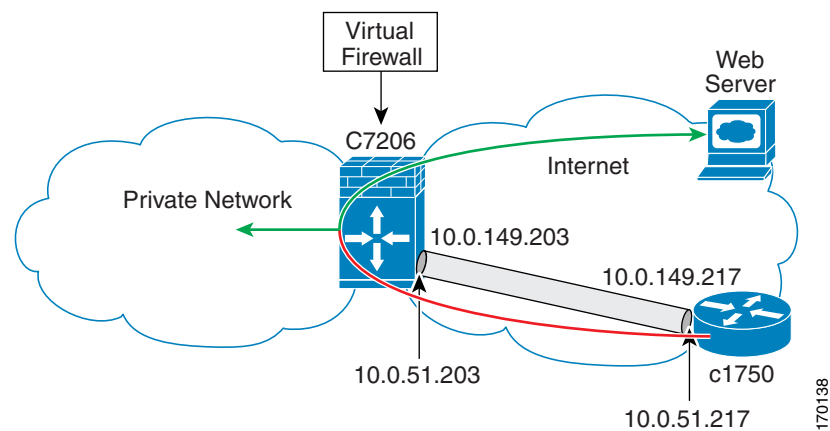
service-policy output VTI
!
.
.
!
end

```

## Static Virtual Tunnel Interface with Virtual Firewall: Example

Applying the virtual firewall to the static VTI tunnel allows traffic from the spoke to pass through the hub to reach the internet. [Figure 6](#) illustrates a static VTI with the spoke protected inherently by the corporate firewall.

**Figure 6**      *Static VTI with Virtual Firewall*



The basic static VTI configuration has been modified to include the virtual firewall definition.

### C7206 Router Configuration

```

hostname c7206
.
.
ip inspect max-incomplete high 1000000
ip inspect max-incomplete low 800000
ip inspect one-minute high 1000000
ip inspect one-minute low 800000
ip inspect tcp synwait-time 60
ip inspect tcp max-incomplete host 100000 block-time 2
ip inspect name IOSFW1 tcp timeout 300
ip inspect name IOSFW1 udp
!
.
.
interface GigabitEthernet0/1
description Internet Connection
ip address 172.18.143.246 255.255.255.0
ip access-group 100 in
ip nat outside
!
interface Tunnel0
ip address 10.0.51.217 255.255.255.0
ip nat inside

```

```

ip inspect IOSFW1 in
tunnel source 10.0.149.217
tunnel destination 10.0.149.203
tunnel mode ipsec ipv4
tunnel protection ipsec profile P1
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.143.1
!
ip nat translation timeout 120
ip nat translation finrst-timeout 2
ip nat translation max-entries 300000
ip nat pool test1 10.2.100.1 10.2.100.50 netmask 255.255.255.0
ip nat inside source list 110 pool test1 vrf test-vti1 overload
!
access-list 100 permit esp any any
access-list 100 permit udp any eq isakmp any
access-list 100 permit udp any eq non500-isakmp any
access-list 100 permit icmp any any
access-list 110 deny esp any any
access-list 110 deny udp any eq isakmp any
access-list 110 permit ip any any
access-list 110 deny udp any eq non500-isakmp any
!
end

```

## Dynamic Virtual Tunnel Interface Easy VPN Server: Example

The following example illustrates the use of the DVTI Easy VPN server, which serves as an IPsec remote access aggregator. The client can be a home user running a Cisco VPN client or it can be a Cisco IOS router configured as an Easy VPN client.

### C7206 Router Configuration

```

hostname c7206
!
aaa new-model
aaa authentication login local_list local
aaa authorization network local_list local
aaa session-id common
!
ip subnet-zero
ip cef
!
username cisco password 0 cisco123
!
controller ISA 1/1
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp client configuration group group1
 key cisco123
 pool group1pool
 save-password
!
crypto isakmp profile vpn1-ra
 match identity group group1
 client authentication list local_list

```



```

isakmp authorization list local_list
client configuration address respond
virtual-template 1
!
crypto ipsec transform-set VTI-TS esp-3des esp-sha-hmac
!
crypto ipsec profile test-vti1
set transform-set VTI-TS
!
interface GigabitEthernet0/1
description Internet Connection
ip address 172.18.143.246 255.255.255.0
!
interface GigabitEthernet0/2
description Internal Network
ip address 10.2.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
ip unnumbered GigabitEthernet0/1
ip virtual-reassembly
tunnel mode ipsec ipv4
tunnel protection ipsec profile test-vti1
!
ip local pool group1pool 192.168.1.1 192.168.1.4
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.143.1
!
end

```

## Verifying the Results for the Dynamic Virtual Tunnel Interface Easy VPN Server: Example

The following examples show that a dynamic VTI has been configured for an Easy VPN server.

Router# **show running-config interface Virtual-Access2**

Building configuration...

```

Current configuration : 250 bytes
!
interface Virtual-Access2
ip unnumbered GigabitEthernet0/1
ip virtual-reassembly
tunnel source 172.18.143.246
tunnel destination 172.18.143.208
tunnel mode ipsec ipv4
tunnel protection ipsec profile test-vti1
no tunnel protection ipsec initiate
end

```

Router# **show ip route**

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

```

Gateway of last resort is 10.2.1.10 to network 0.0.0.0

```

 172.18.0.0/24 is subnetted, 1 subnets
C 172.18.143.0 is directly connected, GigabitEthernet0/1

```

```

 192.168.1.0/32 is subnetted, 1 subnets
S 192.168.1.1 [1/0] via 0.0.0.0, Virtual-Access2
 10.0.0.0/24 is subnetted, 1 subnets
C 10.2.1.0 is directly connected, GigabitEthernet0/2
S* 0.0.0.0/0 [1/0] via 172.18.143.1

```

## Dynamic Virtual Tunnel Interface Easy VPN Client: Example

The following example shows how you can set up a router as the Easy VPN client. This example uses basically the same idea as the Easy VPN client that you can run from a PC to connect. In fact, the configuration of the Easy VPN server will work for the software client or the Cisco IOS client.

```

hostname c1841
!
no aaa new-model
!
ip cef
!
username cisco password 0 cisco123
!
crypto ipsec client ezvpn CLIENT
 connect manual
 group group1 key cisco123
 mode client
 peer 172.18.143.246
 virtual-interface 1
 username cisco password cisco123
 xauth userid mode local
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.255
!
interface FastEthernet0/0
 description Internet Connection
 ip address 172.18.143.208 255.255.255.0
 crypto ipsec client ezvpn CLIENT
!
interface FastEthernet0/1
 ip address 10.1.1.252 255.255.255.0
 crypto ipsec client ezvpn CLIENT inside
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
!
ip route 0.0.0.0 0.0.0.0 172.18.143.1 254
!
end

```

The client definition can be set up in many different ways. The mode specified with the **connect** command can be automatic or manual. If the connect mode is set to manual, the IPsec tunnel has to be initiated manually by a user.

Also note use of the **mode** command. The mode can be client, network-extension, or network-extension-plus. This example indicates client mode, which means that the client is given a private address from the server. Network-extension mode is different from client mode in that the client specifies for the server its attached private subnet. Depending on the mode, the routing table on either end will be slightly different. The basic operation of the IPsec tunnel remains the same, regardless of the specified mode.

## Verifying the Results for the Dynamic Virtual Tunnel Interface Easy VPN Client: Example

The following examples illustrate different ways to display the status of the DVTI.

```
Router# show running-config interface Virtual-Access2
```

```
Building configuration...
```

```
Current configuration : 148 bytes
!
interface Virtual-Access2
 ip unnumbered Loopback1
 tunnel source FastEthernet0/0
 tunnel destination 172.18.143.246
 tunnel mode ipsec ipv4
end
```

```
Router# show running-config interface Loopback1
```

```
Building configuration...
```

```
Current configuration : 65 bytes
!
interface Loopback1
 ip address 192.168.1.1 255.255.255.255
end
```

```
Router# show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is 172.18.143.1 to network 0.0.0.0
```

```
 10.0.0.0/32 is subnetted, 1 subnets
C 10.1.1.1 is directly connected, Loopback0
 172.18.0.0/24 is subnetted, 1 subnets
C 172.18.143.0 is directly connected, FastEthernet0/0
 192.168.1.0/32 is subnetted, 1 subnets
C 192.168.1.1 is directly connected, Loopback1
S* 0.0.0.0/0 [1/0] via 0.0.0.0, Virtual-Access2
```

```
Router# show crypto ipsec client ezvpn
```

```
Easy VPN Remote Phase: 6
```

```
Tunnel name : CLIENT
Inside interface list: FastEthernet0/1
Outside interface: Virtual-Access2 (bound to FastEthernet0/0)
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 192.168.1.1
Mask: 255.255.255.255
Save Password: Allowed
Current EzVPN Peer: 172.18.143.246
```

## VRF-Aware IPsec with Dynamic VTI: Example

This example shows how to configure VRF-Aware IPsec to take advantage of the dynamic VTI:

```
hostname c7206
.
.
ip vrf test-vti1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
.
.
interface Virtual-Template1 type tunnel
 ip vrf forwarding test-vti1
 ip unnumbered Loopback0
 ip virtual-reassembly
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile test-vti1
!
.
.
end
```

## Dynamic Virtual Tunnel Interface with Virtual Firewall: Example

The DVTI Easy VPN server can be configured behind a virtual firewall. Behind-the-firewall configuration allows users to enter the network, while the network firewall is protected from unauthorized access. The virtual firewall uses Context-Based Access Control (CBAC) and NAT applied to the Internet interface as well as to the virtual template.

```
hostname c7206
.
.
ip inspect max-incomplete high 1000000
ip inspect max-incomplete low 800000
ip inspect one-minute high 1000000
ip inspect one-minute low 800000
ip inspect tcp synwait-time 60
ip inspect tcp max-incomplete host 100000 block-time 2
ip inspect name IOSFW1 tcp timeout 300
ip inspect name IOSFW1 udp
!
.
.
interface GigabitEthernet0/1
 description Internet Connection
 ip address 172.18.143.246 255.255.255.0
 ip access-group 100 in
 ip nat outside
!
interface GigabitEthernet0/2
 description Internal Network
 ip address 10.2.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip nat inside
 ip inspect IOSFW1 in
```

```

tunnel mode ipsec ipv4
tunnel protection ipsec profile test-vti1
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.143.1
!
ip nat translation timeout 120
ip nat translation finrst-timeout 2
ip nat translation max-entries 300000
ip nat pool test1 10.2.100.1 10.2.100.50 netmask 255.255.255.0
ip nat inside source list 110 pool test1 vrf test-vti1 overload
!
access-list 100 permit esp any any
access-list 100 permit udp any eq isakmp any
access-list 100 permit udp any eq non500-isakmp any
access-list 100 permit icmp any any
access-list 110 deny esp any any
access-list 110 deny udp any eq isakmp any
access-list 110 permit ip any any
access-list 110 deny udp any eq non500-isakmp any
!
end

```

## Dynamic Virtual Tunnel Interface with QoS: Example

You can add QoS to the DVTI tunnel by applying the service policy to the virtual template. When the template is cloned to make the virtual-access interface, the service policy will be applied there. The following example shows the basic DVTI configuration with QoS added.

```

hostname c7206
.
.
class-map match-all VTI
 match any
!
policy-map VTI
 class VTI
 police cir 2000000
 conform-action transmit
 exceed-action drop
!
.
.
interface Virtual-Templat1 type tunnel
 ip vrf forwarding test-vti1
 ip unnumbered Loopback0
 ip virtual-reassembly
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile test-vti1
 service-policy output VTI
!
.
.
!
end

```

## Additional References

The following sections provide references related to IPsec virtual tunnel interface.

## Related Documents

| Related Topic          | Document Title                                                                                                                                                                                     |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IPsec, security issues | <i>Cisco IOS Security Configuration Guide</i> , Release 12.4                                                                                                                                       |
| QoS, configuring       | <ul style="list-style-type: none"> <li>Quality of Service (QoS) Support for Enhanced Easy VPN</li> <li><i>Cisco IOS Quality of Service Solutions Configuration Guide</i>, Release 12.4T</li> </ul> |
| Security commands      | <i>Cisco IOS Security Command Reference</i> , Release 12.4T                                                                                                                                        |
| VPN configuration      | <ul style="list-style-type: none"> <li><i>Cisco Easy VPN Remote</i></li> <li><i>Easy VPN Server</i></li> </ul>                                                                                     |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

| RFC      | Title                                                            |
|----------|------------------------------------------------------------------|
| RFC 2401 | <i>Security Architecture for the Internet Protocol</i>           |
| RFC 2408 | <i>Internet Security Association and Key Management Protocol</i> |
| RFC 2409 | <i>The Internet Key Exchange (IKE)</i>                           |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features

- **crypto isakmp profile**
- **interface virtual-template**
- **show vtemplate**
- **tunnel mode**
- **virtual-template**

For information about these commands, see the Cisco IOS Security Command Reference at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html). For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

# Feature Information for IPsec Virtual Tunnel Interface

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click Cancel at the login dialog box and follow the instructions that appear.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for IPsec Virtual Tunnel Interface

| Feature Name                   | Releases                                            | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Static IPsec VTIs              | 12.3(7)T<br>12.3(14)T<br>12.2(33)SRA<br>12.2(33)SXH | IPsec VTIs (VTIs) provide a routable interface type for terminating IPsec tunnels and an easy way to define protection between sites to form an overlay network. IPsec VTIs simplify configuration of IPsec for protection of remote links, support multicast, and simplify network management and load balancing.<br><br>Static tunnel interfaces can be configured to encapsulate IPv6 or IPv4 packets in IPv6.                                                                                                                                                                                                                                                                                                                                                                               |
| Dynamic IPsec VTIs             | 12.3(7)T<br>12.3(14)T                               | Dynamic VTIs provide efficiency in the use of IP addresses and provide secure connectivity. Dynamic VTIs allow dynamically downloadable per-group and per-user policies to be configured on a RADIUS server. The per-group or per-user definition can be created using Xauth User or Unity group, or it can be derived from a certificate. Dynamic VTIs are standards based, so interoperability in a multiple-vendor environment is supported. IPsec dynamic VTIs allow you to create highly secure connectivity for remote access VPNs and can be combined with Cisco Architecture for Voice, Video, and Integrated Data (AVVID) to deliver converged voice, video, and data over IP networks. The dynamic VTI simplifies VRF-aware IPsec deployment. The VRF is configured on the interface. |
| IPSec Virtual Tunnel Interface | Cisco IOS XE Release 2.1                            | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork



Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

---

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

---

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.





# IPSec VPN Accounting

The IPSec VPN Accounting feature allows for a session to be accounted for by indicating when the session starts and when it stops.

A VPN session is defined as an Internet Key Exchange (IKE) security association (SA) and the one or more SA pairs that are created by the IKE SA. The session starts when the first IP Security (IPSec) pair is created and stops when all IPSec SAs are deleted.

Session identifying information and session usage information is passed to the Remote Authentication Dial-In User Service (RADIUS) server via standard RADIUS attributes and vendor-specific attributes (VSAs).

## Feature Specifications for IPSec VPN Accounting

| Feature History                                                                                                                                                                              |                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| Release                                                                                                                                                                                      | Modification                                                  |
| 12.2(15)T                                                                                                                                                                                    | This feature was introduced.                                  |
| Cisco IOS XE Release 2.1                                                                                                                                                                     | This feature was introduced on Cisco ASR 1000 Series Routers. |
| Supported Platforms                                                                                                                                                                          |                                                               |
| Cisco 2610–2613, Cisco 2620–Cisco 2621, Cisco 2650–Cisco 2651, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 3725, Cisco 3745, Cisco 7100, Cisco 7200, Cisco 7400, Cisco ubr7100, Cisco ubr7200. |                                                               |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for IPSec VPN Accounting, page 2](#)
- [Information About IPSec VPN Accounting, page 2](#)



- [How to Configure IPsec VPN Accounting](#), page 6
- [Configuration Examples for IPsec VPN Accounting](#), page 12
- [Additional References](#), page 16
- [Command Reference](#), page 17
- [Glossary](#), page 19

## Prerequisites for IPsec VPN Accounting

You need to understand how to configure RADIUS and authentication, authorization, and accounting (AAA) accounting. For information about configuring RADIUS and AAA, refer to the following documents:

- *Configuring Basic AAA RADIUS for Dial-In Clients*
- [How Does RADIUS Work?](#)
- The chapter “[Configuring RADIUS](#)” in the *Cisco IOS Security Configuration Guide*
- The chapter “[RADIUS Commands](#)” in the *Cisco IOS Security Command Reference*, Release 12.2
- The chapter “[Configuring Accounting](#)” in the *Cisco IOS Security Configuration Guide*, Release 12.2

You also need to know how to configure IPsec accounting. For information about configuring IPsec accounting, refer to the chapter “[Configuring IPsec Network Security](#)” in the *Cisco IOS Security Configuration Guide*, Release 12.2.

## Information About IPsec VPN Accounting

To configure IPsec VPN accounting, you must understand the following concepts:

- [RADIUS Accounting](#), page 2
- [IKE and IPsec Subsystem Interaction](#), page 4

## RADIUS Accounting

For many large networks, it is required that user activity be recorded for auditing purposes. The method that is used most is RADIUS accounting.

RADIUS accounting allows for a session to be accounted for by indicating when the session starts and when it stops. Additionally, session identifying information and session usage information will be passed to the RADIUS server via RADIUS attributes and VSAs.

## RADIUS Start Accounting

The RADIUS Start packet contains many attributes that generally identify who is requesting the service and of what the property of that service consists. [Table 1](#) represents the attributes required for the start.

**Table 1** *RADIUS Accounting Start Packet Attributes*

| <b>RADIUS Attributes Value</b> | <b>Attribute</b>    | <b>Description</b>                                                                                                                                              |
|--------------------------------|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1                              | user-name           | Username used in extended authentication (XAUTH). The username may be NULL when XAUTH is not used.                                                              |
| 4                              | nas-ip-address      | Identifying IP address of the network access server (NAS) that serves the user. It should be unique to the NAS within the scope of the RADIUS server.           |
| 5                              | nas-port            | Physical port number of the NAS that serves the user.                                                                                                           |
| 8                              | framed-ip-address   | Private address allocated for the IP Security (IPSec) session.                                                                                                  |
| 40                             | acct-status-type    | Status type. This attribute indicates whether this accounting request marks the beginning (start), the end (stop), or an update of the session.                 |
| 41                             | acct-delay-time     | Number of seconds the client has been trying to send a particular record.                                                                                       |
| 44                             | acct-session-id     | Unique accounting identifier that makes it easy to match start and stop records in a log file.                                                                  |
| 26                             | vrf-id              | String that represents the name of the Virtual Route Forwarder (VRF).                                                                                           |
| 26                             | isakmp-initiator-ip | Endpoint IP address of the remote Internet Key Exchange (IKE) initiator (V4).                                                                                   |
| 26                             | isakmp-group-id     | Name of the VPN group profile used for accounting.                                                                                                              |
| 26                             | isakmp-phase1-id    | Phase 1 identification (ID) used by IKE (for example, domain name [DN], fully qualified domain name [FQDN], IP address) to help identify the session initiator. |

## RADIUS Stop Accounting

The RADIUS Stop packet contains many attributes that identify the usage of the session. Table 2 represents the additional attributes required for the RADIUS stop packet. It is possible that only the stop packet will be sent without the start if configured to do so. If only the stop packet is sent, this allows an easy way to reduce the number of records going to the AAA server.

**Table 2** *RADIUS Accounting Stop Packet Attributes*

| <b>RADIUS Attributes Value</b> | <b>Attribute</b>   | <b>Description</b>                                                                                                    |
|--------------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------|
| 42                             | acct-input-octets  | Number of octets that have been received from the Unity client over the course of the service that is being provided. |
| 43                             | acct-output-octets | Number of octets that have been sent to the Unity client in the course of delivering this service.                    |

**Table 2** *RADIUS Accounting Stop Packet Attributes (continued)*

| <b>RADIUS Attributes Value</b> | <b>Attribute</b>      | <b>Description</b>                                                                                                                  |
|--------------------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| 46                             | acct-session-time     | Length of time (in seconds) that the Unity client has received service.                                                             |
| 47                             | acct-input-packets    | Quantity of packets that have been received from the Unity client in the course of delivering this service.                         |
| 48                             | acct-output-packets   | Quantity of packets that have been sent to the Unity client in the course of delivering this service.                               |
| 49                             | acct-terminate-cause  | For future use.                                                                                                                     |
| 52                             | acct-input-gigawords  | How many times the Acct-Input-Octets counter has wrapped around the $2^{32}$ (2 to the 32nd power) over the course of this service. |
| 52                             | acct-output-gigawords | How many times the Acct-Input-Octets counter has wrapped around the $2^{32}$ (2 to the 32nd power) over the course of this service. |

## RADIUS Update Accounting

RADIUS accounting updates are supported. Packet and octet counts are shown in the updates. To learn more about AAA, refer to the following documents:

- [Configuring Basic AAA RADIUS for Dial-In Clients](#)
- The chapter “[RADIUS Commands](#)” in the *Cisco IOS Security Command Reference*, Release 12.2 T
- [How to Assign Privilege Levels with TACACS+ and RADIUS](#)
- Other AAA documentation at the [Cisco.com](#) website

## IKE and IPSec Subsystem Interaction

### Accounting Start

If IPSec accounting is configured, after IKE phases are complete, an accounting start record is generated for the session. New accounting records are not generated during a rekeying.

The following is an account start record that was generated on a router and that is to be sent to the AAA server that is defined:

```
*Aug 23 04:06:20.131: RADIUS(00000002): sending
*Aug 23 04:06:20.131: RADIUS(00000002): Send Accounting-Request to 10.1.1.4:1646 id 4, len 220
*Aug 23 04:06:20.131: RADIUS: authenticator 38 F5 EB 46 4D BE 4A 6F - 45 EB EF 7D B7 19 FB 3F
*Aug 23 04:06:20.135: RADIUS: Acct-Session-Id [44] 10 "00000001"
*Aug 23 04:06:20.135: RADIUS: Vendor, Cisco [26] 31
*Aug 23 04:06:20.135: RADIUS: Cisco AVpair [1] 25 "isakmp-group-id=cclient"
*Aug 23 04:06:20.135: RADIUS: Framed-IP-Address [8] 6 10.13.13.1
*Aug 23 04:06:20.135: RADIUS: Vendor, Cisco [26] 20
*Aug 23 04:06:20.135: RADIUS: Cisco AVpair [1] 14 "vrf-id=cisco"
*Aug 23 04:06:20.135: RADIUS: Vendor, Cisco [26] 35
```

```
*Aug 23 04:06:20.135: RADIUS: Cisco AVpair [1] 29 "isakmp-initator-ip=11.1.2.2"
*Aug 23 04:06:20.135: RADIUS: Vendor, Cisco [26] 36
*Aug 23 04:06:20.135: RADIUS: Cisco AVpair [1] 30 "connect-progress=No
Progress"
*Aug 23 04:06:20.135: RADIUS: User-Name [1] 13 "joe@cclient"
*Aug 23 04:06:20.135: RADIUS: Acct-Status-Type [40] 6 Start [1]
*Aug 23 04:06:20.135: RADIUS: Vendor, Cisco [26] 25
*Aug 23 04:06:20.135: RADIUS: cisco-nas-port [2] 19 "FastEthernet0/0.1"
*Aug 23 04:06:20.135: RADIUS: NAS-Port [5] 6 0
*Aug 23 04:06:20.135: RADIUS: NAS-IP-Address [4] 6 10.1.1.147
*Aug 23 04:06:20.135: RADIUS: Acct-Delay-Time [41] 6 0
*Aug 23 04:06:20.139: RADIUS: Received from id 21645/4 10.1.1.4:1646, Accounting-response,
len 20
*Aug 23 04:06:20.139: RADIUS: authenticator B7 E3 D0 F5 61 9A 89 D8 - 99 A6 8A 8A 98 79
9D 5D
```

## Accounting Stop

An accounting stop packet is generated when there are no more flows (IPSec SA pairs) with the remote peer.

The accounting stop records contain the following information:

- Packets out
- Packets in
- Octets out
- Gigawords in
- Gigawords out

Below is an account start record that was generated on a router. The account start record is to be sent to the AAA server that is defined.

```
*Aug 23 04:20:16.519: RADIUS(00000003): Using existing nas_port 0
*Aug 23 04:20:16.519: RADIUS(00000003): Config NAS IP: 100.1.1.147
*Aug 23 04:20:16.519: RADIUS(00000003): sending
*Aug 23 04:20:16.519: RADIUS(00000003): Send Accounting-Request to 100.1.1.4:1646 id 19,
len 238
*Aug 23 04:20:16.519: RADIUS: authenticator 82 65 5B 42 F0 3F 17 C3 - 23 F3 4C 35 A2 8A
3E E6
*Aug 23 04:20:16.519: RADIUS: Acct-Session-Id [44] 10 "00000002"
*Aug 23 04:20:16.519: RADIUS: Vendor, Cisco [26] 20
*Aug 23 04:20:16.519: RADIUS: Cisco AVpair [1] 14 "vrf-id=cisco"
*Aug 23 04:20:16.519: RADIUS: Vendor, Cisco [26] 35
*Aug 23 04:20:16.519: RADIUS: Cisco AVpair [1] 29 "isakmp-initator-ip=11.1.1.2"
*Aug 23 04:20:16.519: RADIUS: Vendor, Cisco [26] 36
*Aug 23 04:20:16.519: RADIUS: Cisco AVpair [1] 30 "connect-progress=No
Progress"
*Aug 23 04:20:16.519: RADIUS: Acct-Session-Time [46] 6 709
*Aug 23 04:20:16.519: RADIUS: Acct-Input-Octets [42] 6 152608
*Aug 23 04:20:16.519: RADIUS: Acct-Output-Octets [43] 6 152608
*Aug 23 04:20:16.519: RADIUS: Acct-Input-Packets [47] 6 1004
*Aug 23 04:20:16.519: RADIUS: Acct-Output-Packets [48] 6 1004
*Apr 23 04:20:16.519: RADIUS: Acct-Input-Giga-Word[52] 6 0
*Apr 23 04:20:16.519: RADIUS: Acct-Output-Giga-Wor[53] 6 0
*Aug 23 04:20:16.519: RADIUS: Acct-Terminate-Cause[49] 6 none [0]
*Aug 23 04:20:16.519: RADIUS: Vendor, Cisco [26] 32
*Aug 23 04:20:16.519: RADIUS: Cisco AVpair [1] 26 "disc-cause-ext=No Reason"
*Aug 23 04:20:16.519: RADIUS: Acct-Status-Type [40] 6 Stop [2]
*Aug 23 04:20:16.519: RADIUS: Vendor, Cisco [26] 25
*Aug 23 04:20:16.519: RADIUS: cisco-nas-port [2] 19 "FastEthernet0/0.1"
```

```
*Aug 23 04:20:16.519: RADIUS: NAS-Port [5] 6 0
*Aug 23 04:20:16.519: RADIUS: NAS-IP-Address [4] 6 100.1.1.147
*Aug 23 04:20:16.519: RADIUS: Acct-Delay-Time [41] 6 0
*Aug 23 04:20:16.523: RADIUS: Received from id 21645/19 100.1.1.4:1646,
Accounting-response, len 20
*Aug 23 04:20:16.523: RADIUS: authenticator F1 CA C1 28 CE A0 26 C9 - 3E 22 C9 DA EA B8
22 A0
```

## Accounting Updates

If accounting updates are enabled, accounting updates are sent while a session is “up.” The update interval is configurable. To enable the accounting updates, use the **aaa accounting update** command.

The following is an accounting update record that is being sent from the router:

```
Router#
*Aug 23 21:46:05.263: RADIUS(00000004): Using existing nas_port 0
*Aug 23 21:46:05.263: RADIUS(00000004): Config NAS IP: 100.1.1.147
*Aug 23 21:46:05.263: RADIUS(00000004): sending
*Aug 23 21:46:05.263: RADIUS(00000004): Send Accounting-Request to 100.1.1.4:1646 id 22,
len 200
*Aug 23 21:46:05.263: RADIUS: authenticator 30 FA 48 86 8E 43 8E 4B - F9 09 71 04 4A F1
52 25
*Aug 23 21:46:05.263: RADIUS: Acct-Session-Id [44] 10 "00000003"
*Aug 23 21:46:05.263: RADIUS: Vendor, Cisco [26] 20
*Aug 23 21:46:05.263: RADIUS: Cisco AVpair [1] 14 "vrf-id=cisco"
*Aug 23 21:46:05.263: RADIUS: Vendor, Cisco [26] 35
*Aug 23 21:46:05.263: RADIUS: Cisco AVpair [1] 29 "isakmp-initator-ip=11.1.1.2"
*Aug 23 21:46:05.263: RADIUS: Vendor, Cisco [26] 36
*Aug 23 21:46:05.263: RADIUS: Cisco AVpair [1] 30 "connect-progress=No
Progress"
*Aug 23 21:46:05.263: RADIUS: Acct-Session-Time [46] 6 109
*Aug 23 21:46:05.263: RADIUS: Acct-Input-Octets [42] 6 608
*Aug 23 21:46:05.263: RADIUS: Acct-Output-Octets [43] 6 608
*Aug 23 21:46:05.263: RADIUS: Acct-Input-Packets [47] 6 4
*Aug 23 21:46:05.263: RADIUS: Acct-Output-Packets [48] 6 4
*Aug 23 21:46:05.263: RADIUS: Acct-Status-Type [40] 6 Watchdog [3]
*Aug 23 21:46:05.263: RADIUS: Vendor, Cisco [26] 25
*Aug 23 21:46:05.263: RADIUS: cisco-nas-port [2] 19 "FastEthernet0/0.1"
*Aug 23 21:46:05.263: RADIUS: NAS-Port [5] 6 0
*Aug 23 21:46:05.263: RADIUS: NAS-IP-Address [4] 6 100.1.1.147
*Aug 23 21:46:05.263: RADIUS: Acct-Delay-Time [41] 6 0
*Aug 23 21:46:05.267: RADIUS: Received from id 21645/22 100.1.1.4:1646,
Accounting-response, len 20
*Aug 23 21:46:05.267: RADIUS: authenticator 51 6B BB 27 A4 F5 D7 61 - A7 03 73 D3 0A AC
1C
```

## How to Configure IPSec VPN Accounting

This section contains the following procedures:

- [Configuring IPSec VPN Accounting, page 7](#)
- [Configuring Accounting Updates, page 10](#)
- [Troubleshooting for IPSec VPN Accounting, page 11](#)



# Configuring IPSec VPN Accounting

To enable IPSec VPN Accounting, you need to perform the following required task:

## Prerequisites

Before configuring IPSec VPN accounting, you must first configure IPSec. To learn about configuring IPSec, refer to the following documents:

- The chapter “[Configuring IPSec Network Security](#)” in the *Cisco IOS Security Configuration Guide*, Release 12.2
- Other IPSec documentation at the [Cisco.com](#) website

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** *list-name method*
5. **aaa authorization network** *list-name method*
6. **aaa accounting network** *list-name start-stop [broadcast] group group-name*
7. **aaa session-id** common
8. **crypto isakmp profile** *profile-name*
9. **vrf** *ivrf*
10. **match identity group** *group-name*
11. **client authentication list** *list-name*
12. **isakmp authorization list** *list-name*
13. **client configuration address** [**initiate** | **respond**]
14. **accounting** *list-name*
15. **exit**
16. **crypto dynamic-map** *dynamic-map-name dynamic-seq-num*
17. **set transform-set** *transform-set-name*
18. **set isakmp-profile** *profile-name*
19. **reverse-route** [**remote-peer**]
20. **exit**
21. **crypto map** *map-name ipsec-isakmp dynamic dynamic-template-name*
22. **radius-server host** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
23. **radius-server key** *string*
24. **radius-server vsa send accounting**
25. **interface** *interface-id*
26. **crypto map** *map-name*

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                          | Purpose                                                                                                                                                                                   |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                          |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                             | Enters global configuration mode.                                                                                                                                                         |
| Step 3 | <b>aaa new-model</b><br><br><b>Example:</b><br>Router (config)# aaa new-model                                                                                                              | Enables periodic interim accounting records to be sent to the accounting server.                                                                                                          |
| Step 4 | <b>aaa authentication login list-name method</b><br><br><b>Example:</b><br>Router (config)# aaa authentication login<br>cisco-client group radius                                          | Enforces authentication, authorization, and accounting (AAA) authentication for extended authorization (XAUTH) via RADIUS or local.                                                       |
| Step 5 | <b>aaa authorization network list-name method</b><br><br><b>Example:</b><br>Router (config)# aaa authorization network<br>cisco-client group radius                                        | Sets AAA authorization parameters on the remote client from RADIUS or local.                                                                                                              |
| Step 6 | <b>aaa accounting network list-name start-stop [broadcast] group group-name</b><br><br><b>Example:</b><br>Router (config)# aaa accounting network acc<br>start-stop broadcast group radius | Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.                                                                             |
| Step 7 | <b>aaa session-id common</b><br><br><b>Example:</b><br>Router (config)# aaa session-id common                                                                                              | Specifies whether the same session ID will be used for each AAA accounting service type within a call or whether a different session ID will be assigned to each accounting service type. |
| Step 8 | <b>crypto isakmp profile profile-name</b><br><br><b>Example:</b><br>Route (config)# crypto isakmp profile cisco                                                                            | Audits IP security (IPSec) user sessions and enters isakmp-profile submode.                                                                                                               |
| Step 9 | <b>vrf ivrf</b><br><br><b>Example:</b><br>Router (conf-isa-prof)# vrf cisco                                                                                                                | Associates the on-demand address pool with a Virtual Private Network (VPN) routing and forwarding (VRF) instance name.                                                                    |

|         | Command or Action                                                                                                                                           | Purpose                                                                                                                                                                                                          |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 10 | <b>match identity group</b> <i>group-name</i><br><br><b>Example:</b><br>Router(conf-isa-prof)# match identity group cisco                                   | Matches an identity from a peer in an ISAKMP profile.                                                                                                                                                            |
| Step 11 | <b>client authentication list</b> <i>list-name</i><br><br><b>Example:</b><br>Router(conf-isa-prof)# client authentication list cisco                        | Configures Internet Key Exchange (IKE) extended authentication (XAUTH) in an Internet Security Association and Key Management Protocol (ISAKMP) profile.                                                         |
| Step 12 | <b>isakmp authorization list</b> <i>list-name</i><br><br><b>Example:</b><br>Router(conf-isa-prof)# <b>isakmp authorization list cisco-client</b>            | Configures an IKE shared secret and other parameters using the AAA server in an ISAKMP profile. The shared secret and other parameters are generally pushed to the remote peer via mode configuration (MODECFG). |
| Step 13 | <b>client configuration address</b> [initiate   respond]<br><br><b>Example:</b><br>Router(conf-isa-prof)# client configuration address respond              | Configures IKE mode configuration (MODECFG) in the ISAKMP profile.                                                                                                                                               |
| Step 14 | <b>accounting</b> <i>list-name</i><br><br><b>Example:</b><br>Router(conf-isa-prof)# accounting acc                                                          | Enables AAA accounting services for all peers that connect via this ISAKMP profile.                                                                                                                              |
| Step 15 | <b>exit</b><br><br><b>Example:</b><br>Router(conf-isa-prof)# exit                                                                                           | Exits isakmp-profile submode.                                                                                                                                                                                    |
| Step 16 | <b>crypto dynamic-map</b> <i>dynamic-map-name</i> <i>dynamic-seq-num</i><br><br><b>Example:</b><br>Router(config)# crypto dynamic-map mymap 10 ipsec-isakmp | Creates a dynamic crypto map template and enters the crypto map configuration command mode.                                                                                                                      |
| Step 17 | <b>set transform-set</b> <i>transform-set-name</i><br><br><b>Example:</b><br>Router(config-crypto-map)# set transform-set aswan                             | Specifies which transform sets can be used with the crypto map template.                                                                                                                                         |
| Step 18 | <b>set isakmp-profile</b> <i>profile-name</i><br><br><b>Example:</b><br>Router(config-crypto-map)# set isakmp-profile cisco                                 | Sets the ISAKMP profile name.                                                                                                                                                                                    |

|         | Command or Action                                                                                                                                                                                   | Purpose                                                                                                                                                                                                            |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 19 | <b>reverse-route</b> [ <b>remote-peer</b> ]<br><br><b>Example:</b><br>Router(config-crypto-map)# reverse-route                                                                                      | Allows routes (ip addresses) to be injected for destinations behind the VPN remote tunnel endpoint and may include a route to the tunnel endpoint itself (using the <b>remote-peer</b> keyword for the crypto map. |
| Step 20 | <b>exit</b><br><br><b>Example:</b><br>Router(config-crypto-map)# exit                                                                                                                               | Exits dynamic crypto map configuration mode.                                                                                                                                                                       |
| Step 21 | <b>crypto map</b> <i>map-name</i> ipsec-isakmp dynamic <i>dynamic-template-name</i><br><br><b>Example:</b><br>Router(config)# crypto map mymap ipsec-isakmp dynamic dmap                            | Enters crypto map configuration mode                                                                                                                                                                               |
| Step 22 | <b>radius-server host</b> <i>ip-address</i> [ <b>auth-port</b> <i>port-number</i> ] [ <b>acct-port</b> <i>port-number</i> ]<br><br><b>Example:</b><br>Router(config)# radius-server host 172.16.1.4 | Specifies a RADIUS server host.                                                                                                                                                                                    |
| Step 23 | <b>radius-server key</b> <i>string</i><br><br><b>Example:</b><br>Router(config)# radius-server key nsite                                                                                            | Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.                                                                                                 |
| Step 24 | <b>radius-server vsa send accounting</b><br><br><b>Example:</b><br>Router(config)# radius-server vsa send accounting                                                                                | Configures the network access server to recognize and use vendor-specific attributes.                                                                                                                              |
| Step 25 | <b>interface</b> <i>type slot/port</i><br><br><b>Example:</b><br>Router(config)# interface FastEthernet 1/0                                                                                         | Configures an interface type and enters interface configuration mode.                                                                                                                                              |
| Step 26 | <b>crypto map</b> <i>map-name</i><br><br><b>Example:</b><br>Router(config-if)# crypto map mymap                                                                                                     | Applies a previously defined crypto map set to an interface.                                                                                                                                                       |

## Configuring Accounting Updates

To send accounting updates while a session is “up,” perform the following optional task:

### Prerequisites

Before you configure accounting updates, you must first configure IPSec VPN accounting. See the section “[Configuring IPSec VPN Accounting](#).”

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa accounting update periodic *number***

## DETAILED STEPS

|        | Command or Action                                                               | Purpose                                                                                     |
|--------|---------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                                                   | Enables privileged EXEC mode.                                                               |
|        | <b>Example:</b><br>Router> enable                                               | <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>        |
| Step 2 | <b>configure terminal</b>                                                       | Enters global configuration mode.                                                           |
|        | <b>Example:</b><br>Router# configure terminal                                   |                                                                                             |
| Step 3 | <b>aaa accounting update periodic <i>number</i></b>                             | (Optional) Enables periodic interim accounting records to be sent to the accounting server. |
|        | <b>Example:</b><br>Router (config)# aaa accounting update periodic 1-2147483647 |                                                                                             |

## Troubleshooting for IPSec VPN Accounting

To display messages about IPSec accounting events, perform the following optional task:

## SUMMARY STEPS

1. **enable**
2. **debug crypto isakmp aaa**

## DETAILED STEPS

|        | Command or Action                                  | Purpose                                                                                                 |
|--------|----------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                      | Enables privileged EXEC mode.                                                                           |
|        | <b>Example:</b><br>Router> enable                  | <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                    |
| Step 2 | <b>debug crypto isakmp aaa</b>                     | Displays messages about Internet Key Exchange (IKE) events.                                             |
|        | <b>Example:</b><br>Router# debug crypto isakmp aaa | <ul style="list-style-type: none"> <li>• The <b>aaa</b> keyword specifies accounting events.</li> </ul> |

# Configuration Examples for IPsec VPN Accounting

- [Accounting and ISAKMP-Profile Example, page 12](#)
- [Accounting Without ISAKMP Profiles Example, page 14](#)

## Accounting and ISAKMP-Profile Example

The following example shows a configuration for supporting remote access clients with accounting and ISAKMP profiles:

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sheep
!
aaa new-model
!
!
aaa accounting network ipsecaaa start-stop group radius
aaa accounting update periodic 1
aaa session-id common
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name cisco.com
ip name-server 172.29.2.133
ip name-server 172.29.11.48
!
!
crypto isakmp policy 1
authentication pre-share
group 2
!
crypto isakmp policy 10
hash md5
authentication pre-share
lifetime 200
crypto isakmp key cisco address 172.31.100.2

crypto iakmp client configuration group cclient
key jegjegjhrj
pool addressA

crypto-isakmp profile groupA
vrf cisco
match identity group cclient
client authentication list cisco-client
isakmp authorization list cisco-client
client configuration address respond
accounting acc
!
!
crypto ipsec transform-set esp-des-md5 esp-des esp-md5-hmac
!
crypto dynamic-map remotes 1
set peer 172.31.100.2
```

```
set security-association lifetime seconds 120
set transform-set esp-des-md5
reverse-route

!
crypto map test 10 ipsec-isakmp dynamic remotes
!
voice call carrier capacity active
!
interface Loopback0
ip address 10.20.20.20 255.255.255.0
no ip route-cache
no ip mroute-cache
!
interface FastEthernet0/0
ip address 10.2.80.203 255.255.255.0
no ip mroute-cache
load-interval 30
duplex full
!
interface FastEthernet1/0
ip address 192.168.219.2 255.255.255.0
no ip mroute-cache
duplex auto
speed auto
!
interface FastEthernet1/1
ip address 172.28.100.1 255.255.255.0
no ip mroute-cache
duplex auto
speed auto
crypto map test
!
no fair-queue
ip default-gateway 10.2.80.1
ip classless
ip route 10.0.0.0 0.0.0.0 10.2.80.1
ip route 10.20.0.0 255.0.0.0 10.2.80.56
ip route 10.10.10.0 255.255.255.0 172.31.100.2
ip route 10.0.0.2 255.255.255.255 10.2.80.73

ip local pool addressA 192.168.1.1 192.168.1.253
no ip http server
ip pim bidir-enable
!
!
ip access-list extended encrypt
permit ip host 10.0.0.1 host 10.5.0.1
!
access-list 101 permit ip host 10.20.20.20 host 10.10.10.10
!
!
radius-server host 172.27.162.206 auth-port 1645 acct-port 1646 key cisco123
radius-server retransmit 3
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
```

```

gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
exec prompt timestamp
line aux 0
line vty 5 15
 ntp server 172.31.150.52
end

```

## Accounting Without ISAKMP Profiles Example

The following example shows a full Cisco IOS configuration that supports accounting remote access peers when ISAKMP profiles are not used:

```

version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sheep
!
aaa new-model
!
!
aaa accounting network ipsecaaa start-stop group radius
aaa accounting update periodic 1
aaa session-id common
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name cisco.com
ip name-server 172.29.2.133
ip name-server 172.29.11.48
!
!
crypto isakmp policy 1
 authentication pre-share
 group 2
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
 lifetime 200
crypto isakmp key cisco address 172.31.100.2
!
!
crypto ipsec transform-set esp-des-md5 esp-des esp-md5-hmac
!
crypto map test client accounting list ipsecaaa
crypto map test 10 ipsec-isakmp
 set peer 172.31.100.2
 set security-association lifetime seconds 120
 set transform-set esp-des-md5
 match address 101
!
voice call carrier capacity active
!

```



```
interface Loopback0
 ip address 10.20.20.20 255.255.255.0
 no ip route-cache
 no ip mroute-cache
!
interface FastEthernet0/0
 ip address 10.2.80.203 255.255.255.0
 no ip mroute-cache
 load-interval 30
 duplex full
!
interface FastEthernet1/0
 ip address 192.168.219.2 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
!
interface FastEthernet1/1
 ip address 172.28.100.1 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
 crypto map test
!
no fair-queue
ip default-gateway 10.2.80.1
ip classless
ip route 10.0.0.0 0.0.0.0 10.2.80.1
ip route 10.30.0.0 255.0.0.0 10.2.80.56
ip route 10.10.10.0 255.255.255.0 172.31.100.2
ip route 10.0.0.2 255.255.255.255 10.2.80.73
no ip http server
ip pim bidir-enable
!
!
ip access-list extended encrypt
 permit ip host 10.0.0.1 host 10.5.0.1
!
access-list 101 permit ip host 10.20.20.20 host 10.10.10.10
!
!
radius-server host 172.27.162.206 auth-port 1645 acct-port 1646 key cisco123
radius-server retransmit 3
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 exec prompt timestamp
line aux 0
line vty 5 15
!
exception core-file ioscrypto/core/sheep-core
```

```
exception dump 172.25.1.129
ntp clock-period 17208229
ntp server 172.71.150.52
!
end
```

## Additional References

For additional information related to IPSec VPN accounting, refer to the following references:

## Related Documents

| Related Topic                            | Document Title                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuring AAA accounting               | <ul style="list-style-type: none"> <li>The chapter “<a href="#">Configuring Accounting</a>” in the <i>Cisco IOS Security Configuration Guide</i>, Release 12.2</li> </ul>                                                                                                                                                                                                                             |
| Configuring IPSec VPN accounting         | <ul style="list-style-type: none"> <li>The chapter “<a href="#">Configuring IPSec Network Security</a>” in the <i>Cisco IOS Security Configuration Guide</i>, Release 12.2</li> </ul>                                                                                                                                                                                                                 |
| Configuring basic AAA RADIUS             | <ul style="list-style-type: none"> <li><i>Configuring Basic AAA RADIUS for Dial-In Clients</i></li> <li><a href="#">How Does RADIUS Work?</a></li> <li>The chapter “<a href="#">Configuring RADIUS</a>” in the <i>Cisco IOS Security Configuration Guide</i>, Release 12.2</li> <li>The chapter “<a href="#">RADIUS Commands</a>” in the <i>Security Command Reference</i>, Release 12.2 T</li> </ul> |
| Configuring ISAKMP profiles              | <i>VRF-Aware IPSec</i> , Cisco IOS Release 12.2(15)T feature module                                                                                                                                                                                                                                                                                                                                   |
| Privilege levels with TACACS+ and RADIUS | <a href="#">How to Assign Privilege Levels with TACACS+ and RADIUS</a>                                                                                                                                                                                                                                                                                                                                |
| IP security, RADIUS, and AAA commands    | <i>Cisco IOS Security Command Reference</i> , Release 12.2 T                                                                                                                                                                                                                                                                                                                                          |

## Standards

| Standards | Title |
|-----------|-------|
| None      |       |

## MIBs

| MIBs | MIBs Link                                                                                                                                                                                                                                                                                                                |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | <p>To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:</p> <p><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></p> |

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

## RFCs

| RFCs | Title |
|------|-------|
| None |       |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following commands are introduced or modified in the feature or features

- **client authentication list**
- **client configuration address**
- **crypto isakmp profile**
- **crypto map (global IPSec)**
- **debug crypto isakmp**
- **isakmp authorization list**
- **match identity**
- **set isakmp-profile**
- **vrf**

For information about these commands, see the Cisco IOS Security Command Reference at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at

<http://tools.cisco.com/Support/CLILookup> or the Master Command List.

# Glossary

**IKE**—Internet Key Exchange. IKE establishes a shared security policy and authenticates keys for services (such as IP security [IPSec]) that require keys. Before any IPSec traffic can be passed, each router, firewall, and host must verify the identity of its peer. This can be done by manually entering preshared keys into both hosts or by a certification authority (CA) service.

**IPSec**—IP security. IPSec is A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

**ISAKMP**—Internet Security Association and Key Management Protocol. ISAKMP is an Internet IPSec protocol (RFC 2408) that negotiates, establishes, modifies, and deletes security associations. It also exchanges key generation and authentication data (independent of the details of any specific key generation technique), key establishment protocol, encryption algorithm, or authentication mechanism.

**L2TP session**—Layer 2 Transport Protocol. L2TP are communications transactions between the L2TP access concentrator (LAC) and the L2TP network server (LNS) that support tunneling of a single PPP connection. There is a one-to-one relationship among the PPP connection, L2TP session, and L2TP call.

**NAS**—network access server. A NAS is a Cisco platform (or collection of platforms, such as an AccessPath system) that interfaces between the packet world (for example, the Internet) and the circuit world (for example, the public switched telephone network [PSTN]).

**PFS**—perfect forward secrecy. **PFS is a cryptographic characteristic associated with a derived shared secret value. With PFS, if one key is compromised, previous and subsequent keys are not compromised because subsequent keys are not derived from previous keys.**

**QM**—Queue Manager. The Cisco IP Queue Manager (IP QM) is an intelligent, IP-based, call-treatment and routing solution that provides powerful call-treatment options as part of the Cisco IP Contact Center (IPCC) solution.

**RADIUS**—Remote Authentication Dial-In User Service. RADIUS is a database for authenticating modem and ISDN connections and for tracking connection time.

**RSA**—Rivest, Shamir, and Adelman. Rivest, Shamir, and Adelman are the inventors of the Public-key cryptographic system that can be used for encryption and authentication.

**SA**—security association. A SA is an instance of security policy and keying material that is applied to a data flow.

**TACACS+**—Terminal Access Controller Access Control System Plus. TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or network access server.

**TED**—Tunnel Endpoint Discovery. TED is a Cisco IOS software feature that allows routers to discover IPSec endpoints.

**VPN**—Virtual Private Network. A VPN enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.

**VRF**—A VPN routing/forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

**VSA**—vendor-specific attribute. A VSA is an attribute that has been implemented by a particular vendor. It uses the attribute Vendor-Specific to encapsulate the resulting AV pair: essentially, Vendor-Specific = protocol:attribute = value.

**XAUTH**—Extended authentication. XAUTH is an optional exchange between IKE Phase 1 and IKE Phase 2, in which the router demands additional authentication information in an attempt to authenticate the actual user (as opposed to authenticating the peer).

**Note**

---

Refer to the [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

---

---

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



# IPSec VPN High Availability Enhancements

## Feature History

| Release   | Modification                                                                                                                        |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------|
| 12.1(9)E  | This feature was introduced in Cisco IOS Release 12.1(9)E.                                                                          |
| 12.2(8)T  | This feature was integrated into Cisco IOS Release 12.2(8)T.                                                                        |
| 12.2(11)T | This feature was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300 and Cisco AS5800 platforms. |
| 12.2(9)YE | This feature was integrated into Cisco IOS Release 12.2(9)YE.                                                                       |
| 12.2(14)S | This feature was integrated into Cisco IOS Release 12.2(14)S.                                                                       |

This feature module describes the IPSec VPN High Availability Enhancements. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 4](#)
- [Supported Standards, MIBs, and RFCs, page 5](#)
- [Configuration Tasks, page 6](#)
- [Configuration Examples, page 8](#)
- [Command Reference, page 10](#)

## Feature Overview

The IPSec VPN High Availability Enhancements feature consists of two new features—[Reverse Route Injection](#) (RRI) and [Hot Standby Router Protocol and IPSec](#) (HSRP)—that work together to provide users with a simplified network design for VPNs, and reduced configuration complexity on remote peers with respect to defining gateway lists. When used together, RRI and HSRP provide a more reliable network design for VPNs and reduce configuration complexity on remote peers.



**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

## Reverse Route Injection

Reverse Route Injection (RRI) is a feature designed to simplify network design for Virtual Private Networks (VPNs) in which there is a requirement for redundancy or load balancing. RRI works with both dynamic and static crypto maps.

In the dynamic case, as remote peers establish IPSec security associations (SAs) with an RRI-enabled router, a static route is created for each subnet or host protected by that remote peer. For static crypto maps, a static route is created for each destination of an extended access list rule. When RRI is used on a static crypto map with an access control list (ACL), routes will always exist, even without the negotiation of IPSec SAs.



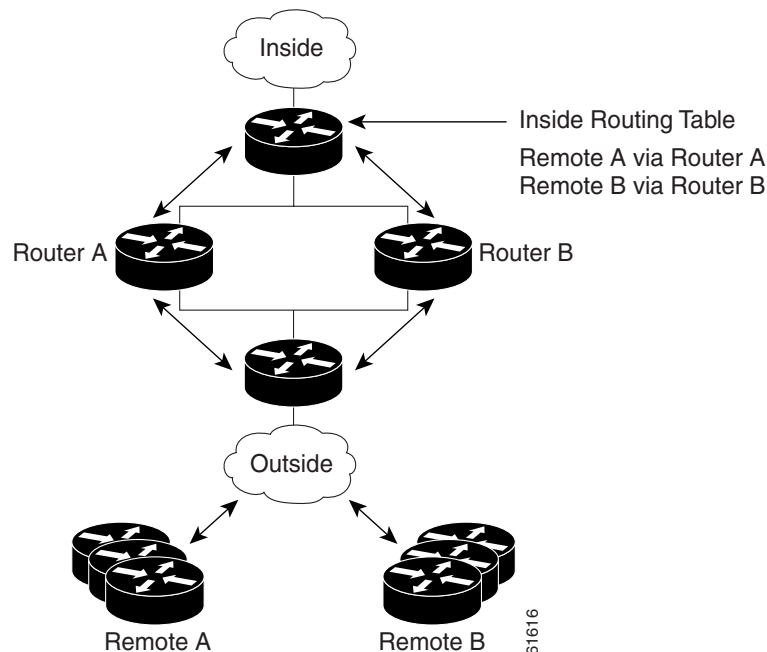
### Note

Use of any keyword in ACLs with RRI is not supported.

When routes are created, they are injected into any dynamic routing protocol and distributed to surrounding devices. This traffic flows, requiring IPSec to be directed to the appropriate RRI router for transport across the correct SAs to avoid IPSec policy mismatches and possible packet loss.

Figure 87 shows a RRI configuration functionality topology. Remote A is being serviced by Router A and Remote B connected to Router B, providing load balancing across VPN gateways at the central site. RRI on the central site devices will ensure that the other router on the inside of the network can automatically make the correct forwarding decision. RRI also eliminates the need to administer static routes on the inside router.

**Figure 87**      **Topology Showing Reverse Route Injection Configuration Functionality**



61616



## Hot Standby Router Protocol and IPSec

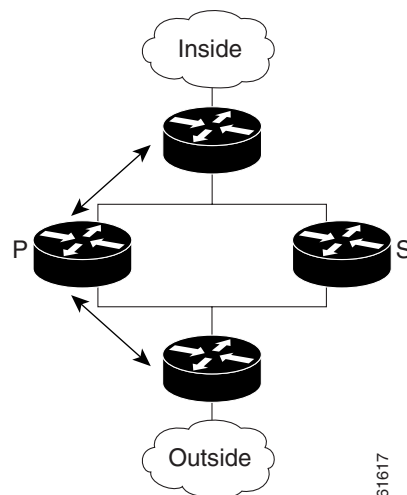
Hot Standby Router Protocol (HSRP) is designed to provide high network availability by routing IP traffic from hosts on Ethernet networks without relying on the availability of any single router. HSRP is particularly useful for hosts that do not support a router discovery protocol, such as ICMP Router Discovery Protocol (IRDP), and do not have the functionality to switch to a new router when their selected router reloads or loses power. Without this functionality, a router that loses its default gateway because of a router failure is unable to communicate with the network.

HSRP is configurable on LAN interfaces using standby command-line interface (CLI) commands. It is now possible to use the standby IP address from an interface as the local IPSec identity, or local tunnel endpoint.

By using the standby IP address as the tunnel endpoint, failover can be applied to VPN routers by using HSRP. Remote VPN gateways connect to the local VPN router via the standby address that belongs to the *active* device in the HSRP group. In the event of failover, the *standby* device takes over ownership of the standby IP address and begins to service remote VPN gateways.

Figure 88 shows the enhanced HSRP functionality topology. Traffic is serviced by the active Router P, the active device in the standby group. In the event of failover, traffic is diverted to Router S, the original standby device. Router S assumes the role of the new active router and takes ownership of the standby IP address.

**Figure 88**      **Topology Showing Hot Standby Router Protocol Functionality**



### Note

In case of a failover, HSRP does not facilitate IPSec state information transference between VPN routers. This means that without this state transference, SAs to remotes will be deleted requiring Internet Key Exchange (IKE) and IPSec SAs to be reestablished. To make IPSec failover more efficient, it is recommended that IKE keepalives be enabled on all routers.

## Benefits

### Reverse Route Injection

- Enables routing of IPSec traffic to a specific VPN headend device in environments that have multiple (redundant) VPN headend devices.

- Ensures predictable failover time of remote sessions between headend devices when using IKE keepalives, especially in environments in which remote device route flapping is common (not taking into consideration the effects of route convergence, which may vary depending on the routing protocol used and the size of the network).
- Eliminates the need for the administration of static routes on upstream devices as routes are dynamically learned by these devices.

#### Hot Standby Router Protocol with IPSec

Failover can be applied to VPN routers through the use of HSRP. Remote VPN gateways connect to the local VPN router through the standby address that belongs to the active device in the HSRP group. This functionality reduces configuration complexity on remote peers with respect to defining gateway lists because only the HSRP standby address needs to be defined.

## Related Documents

- [IPSec Stateful Failover \(VPN High Availability\)](#)
- [Cisco IOS Security Configuration Guide](#), Release 12.2
- [Cisco IOS IP Configuration Guide](#), Release 12.2 (Configuring IP Services chapter)
- [VPN Acceleration Module Installation and Configuration Guide](#)
- [SA-VAM2 Installation and Configuration Guide](#)
- [Release Notes for the SA-VAM2](#)
- [Cisco 7100 Series VPN Router Installation and Configuration Guide](#)
- [Cisco 7200 VXR Installation and Configuration Guide](#)
- [Cisco 7401ASR Installation and Configuration Guide](#)

## Supported Platforms

#### Cisco IOS Release 12.1(9)E and Cisco IOS Release 12.2(8)T

- Cisco 7100 series
- Cisco 7200VXR series

#### Cisco IOS Release 12.2(8)T Only

- Cisco 1710
- Cisco 1720
- Cisco 1750
- Cisco 1751
- Cisco 2600 series
- Cisco 3620
- Cisco 3631
- Cisco 3640
- Cisco 3660

- Cisco 3725
- Cisco 3745
- Cisco uBR7200
- Cisco uBR925

**Cisco IOS Release 12.2(11)T Only**

- Cisco AS5300 series
- Cisco AS5800 series

**Cisco IOS Release 12.2(9)YE**

- Cisco 7401ASR router

**Cisco IOS Release 12.2(14)S**

- Cisco 7200 series
- Cisco 7400 series

**Finding Support Information for Platforms and Cisco IOS Software Images**

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Supported Standards, MIBs, and RFCs

**Standards**

- No new or modified standards are supported by this feature.

**MIBs**

- No new or modified standards are supported by this feature.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

**RFCs**

- No new or modified RFCs are supported by this feature.

## Configuration Tasks

See the following sections for configuration tasks for the IPSec VPN High Availability Enhancements feature. Each task in the list is identified as either required or optional.

- [Configuring Reverse Route Injection on a Dynamic Crypto Map](#) (required)
- [Configuring Reverse Route Injection on a Static Crypto Map](#) (required)
- [Configuring HSRP with IPSec](#) (required)
- [Verifying VPN IPSec Crypto Configuration](#) (optional)

### Configuring Reverse Route Injection on a Dynamic Crypto Map

Dynamic crypto map entries, like regular static crypto map entries, are grouped into sets. A set is a group of dynamic crypto map entries all with the same dynamic map name but each with a different dynamic sequence number. Each member of the set may be configured for RRI.

To create a dynamic crypto map entry and enable RRI, use the following commands beginning in global configuration mode:

|        | Command                                                 | Purpose                                                                                                                                                                                                                                         |
|--------|---------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router (config)# <b>crypto dynamic</b> map-name seq-num | Creates a dynamic crypto map entry and enters crypto map configuration mode.                                                                                                                                                                    |
| Step 2 | Router (config-crypto-m)# <b>set transform-set</b>      | Specifies which transform sets are allowed for the crypto map entry. Lists multiple transform sets in order of priority (highest priority first).<br><br>This entry is the only configuration statement required in dynamic crypto map entries. |
| Step 3 | Router (config-crypto-m)# <b>reverse-route</b>          | Creates source proxy information.                                                                                                                                                                                                               |

### Configuring Reverse Route Injection on a Static Crypto Map

Before configuring RRI on a static crypto map, please note the following items:

- Routes are not created based on access list 102 as reverse-route is not enabled on mymap 2. RRI is not enabled by default and is not displayed in the router configuration.
- Enable a routing protocol to distribute the VPN routes to upstream devices.
- If Cisco Express Forwarding (CEF) is run on a VPN router configured for RRI, adjacencies need to be formed for each RRI injected network through the next hop device. As the next hop is not explicitly defined in the routing table for these routes, proxy-ARP should be enabled on the next hop router which allows the CEF adjacency to be formed using the layer two addresses of that device. In cases where there are many RRI injected routes, adjacency tables may become quite large as an entry is created for each device from each of the subnets represented by the RRI route. This issue is to be resolved in a future release.

To add RRI to a static crypto map set, use the following commands beginning in global configuration mode:

|        | Command                                                                    | Purpose                                                                                                                                           |
|--------|----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router (config)# <b>crypto map</b> map-name seq-num<br><b>ipsec-isakmp</b> | Adds a dynamic crypto map set to a static crypto map set and enters interface configuration mode.                                                 |
| Step 2 | Router (config-if)# <b>set peer ip address</b>                             | Specifies an IPSec peer IP address in a crypto map entry.                                                                                         |
| Step 3 | Router (config-if)# <b>reverse-route</b>                                   | Creates dynamically static routes based on crypto access control lists (ACLs).                                                                    |
| Step 4 | Router (config-if)# <b>match address</b>                                   | Specifies an extended access list for a crypto map entry.                                                                                         |
| Step 5 | Router (config-if)# <b>set transform-set</b>                               | Specifies which transform sets are allowed for the crypto map entry. Lists multiple transform sets in order of priority (highest priority first). |

## Configuring HSRP with IPSec

When configuring HSRP with IPSec, the following conditions may apply:

- When HSRP is applied to a crypto map on an interface, the crypto map must be reapplied if the standby IP address or the standby name is changed on that interface.
- If HSRP is applied to a crypto map on an interface, and the user deletes the standby IP address or the standby name from that interface, the crypto tunnel endpoint is reinitialized to the actual IP address of that interface.
- If a user adds the standby IP address and the standby name to an interface with the requirement IPSec failover, the crypto map must be reapplied with the appropriate redundancy information.
- Standby priorities should be equal on active and standby routers. If they are not, the higher priority router takes over as the active router. When that occurs, the active router goes into a cycle where it continuously goes down and comes back up.
- The IP addresses on the HSRP-tracked interfaces on the standby and active routers should both be either lower or higher on one router than the other. In the case of equal priorities (an HA requirement), HSRP will assign the active state-based IP address. If an addressing scheme exists so that the public IP address of router A is lower than the public IP address of router B, but the opposite is true for their private interfaces, an active/standby-standby/active split condition could exist which will break connectivity.



### Note

To configure HSRP without IPSec refer to the “[Configuring IP Services](#)” chapter of the *Cisco IOS IP Configuration Guide*, Release 12.2.

To apply a crypto map set to an interface, use the following commands beginning in global configuration mode:

|        | Command                                                                  | Purpose                                                                                |
|--------|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Step 1 | Router (config)# <b>interface</b> <i>type slot/port</i>                  | Specifies an interface and enters interface configuration mode.                        |
| Step 2 | Router (config-if)# <b>standby name</b> <i>group-name</i>                | Specifies the standby group name (required).                                           |
| Step 3 | Router (config-if)# <b>standby ip</b> <i>ip-address</i>                  | Specifies the IP address of the standby groups (required for one device in the group). |
| Step 4 | Router (config-if)# <b>crypto map map-name redundancy [standby-name]</b> | Specifies IP redundancy address as the tunnel endpoint for IPSec.                      |

## Verifying VPN IPSec Crypto Configuration

To verify your VPN IPSec crypto configuration, use the following EXEC commands:

| Command                                                                                 | Purpose                                         |
|-----------------------------------------------------------------------------------------|-------------------------------------------------|
| Router# <b>show crypto ipsec transform-set</b>                                          | Displays your transform set configuration.      |
| Router# <b>show crypto map [interface <i>interface</i>   tag <i>map-name</i>]</b>       | Displays your crypto map configuration.         |
| Router# <b>show crypto ipsec sa [map <i>map-name</i>   address   identity] [detail]</b> | Displays information about IPSec SAs.           |
| Router# <b>show crypto dynamic-map [tag <i>map-name</i>]</b>                            | Displays information about dynamic crypto maps. |

## Configuration Examples

This section provides the following configuration examples:

- [Reverse Route Injection on a Dynamic Crypto Map Example](#)
- [Reverse Route Injection on a Static Crypto Map Example](#)
- [HSRP and IPSec Example](#)

### Reverse Route Injection on a Dynamic Crypto Map Example

In the following example, using the reverse route crypto map subcommand in the definition of the dynamic crypto map template ensures that routes are created for any remote proxies (subnets or hosts), protected by the connecting remote IPSec peers.

```
crypto dynamic mydynmap 1
 set transform-set esp-3des-sha
 reverse-route
```

This template is then associated with a “parent” crypto map statement and then applied to an interface.

```
crypto map mymap 3 ipsec-isakmp dynamic mydynmap

interface FastEthernet 0/0
crypto map mymap
```

## Reverse Route Injection on a Static Crypto Map Example

RRI is a good solution for topologies that require encrypted traffic to be diverted to a VPN router and all other traffic to a different router.

In these scenarios, RRI eliminates the need to manually define static routes on devices.

RRI is not required if a single VPN router is used and all traffic passes through the VPN router during its path in and out of the network.

If the user chooses to manually define static routes on the VPN router for remote proxies, and have these routes permanently installed in the routing table, RRI should not be enabled on the crypto map instance that covers the same remote proxies. In this case, there is no possibility of user defined static routes being removed by RRI.

Routing convergence can affect the success of a failover based on the routing protocol used to advertise routes (link state versus periodic update). It is recommended that a link state routing protocol such as OSPF be used to help speed convergence time by ensuring that routing updates are sent as soon as a change in routing state is detected.

In the following example, RRI is enabled for mymap 1, but not for mymap 2. Upon the application of the crypto map to the interface, a route is created based on access-list 101 analogous to the following:

```
IP route 172.17.11.0 255.255.255.0 FastEthernet 0/0

crypto map mymap 1 ipsec-isakmp
 set peer 172.17.11.1
 reverse-route
 set transform-set esp-3des-sha
 match address 101
crypto map mymap 2 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set esp-3des-sha
 match address 102

access-list 101 permit ip 192.168.1.0 0.0.0.255 172.17.11.0 0.0.0.255
access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255

interface FastEthernet 0/0
 crypto map mymap
```

## HSRP and IPSec Example

The following example shows how all remote VPN gateways connect to the router via 192.168.0.3. The crypto map on the interface binds this standby address as the local tunnel endpoint for all instances of *mymap* and at the same time ensures that HSRP failover is facilitated between an active and standby device belonging to the same standby group, group1.

Note that RRI is also enabled to provide the ability for only the *active* device in the HSRP group to be advertising itself to inside devices as the next hop VPN gateway to the remote proxies. If there is a failover, routes are deleted on the formerly active device and created on the newly active device.

```
crypto map mymap 1 ipsec-isakmp
 set peer 10.1.1.1
 reverse-route
 set transform-set esp-3des-sha
 match address 102

Interface FastEthernet 0/0
 ip address 192.168.0.2 255.255.255.0
 standby name group1
 standby ip 192.168.0.3
 crypto map mymap redundancy group1

access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
```

The standby name needs to be configured on all devices in the standby group and the standby address needs to be configured on at least one member of the group. If the standby name is removed from the router, the IPSec SAs will be deleted. If the standby name is added again, regardless of whether the same name or a different name is used, the crypto map (using the redundancy option) will have to be reapplied to the interface.

## Command Reference

The following commands are introduced or modified in the feature or features:  
documented in this module:

- [crypto map \(interface IPSec\)](#)
- [reverse-route](#)

For information about these commands, see the Cisco IOS Security Command Reference at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

---

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





# Low Latency Queueing (LLQ) for IPSec Encryption Engines

---

## Feature History

| Release   | Modification                                                  |
|-----------|---------------------------------------------------------------|
| 12.2(13)T | This feature was introduced.                                  |
| 12.2(14)S | This feature was integrated into Cisco IOS Release 12.2(14)S. |

This feature module describes the Low Latency Queueing (LLQ) for IPSec encryption engines feature in Cisco IOS Release 12.2(13)T and 12.2(14)S. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 3](#)
- [Supported Standards, MIBs, and RFCs, page 4](#)
- [Prerequisites, page 4](#)
- [Configuration Tasks, page 4](#)
- [Monitoring and Maintaining LLQ for IPSec Encryption Engines, page 8](#)
- [Configuration Examples, page 8](#)
- [Command Reference, page 9](#)
- [Glossary, page 9](#)

## Feature Overview

Low Latency Queueing (LLQ) for IPSec encryption engines helps reduce packet latency by introducing the concept of queueing before crypto engines. Prior to this, the crypto processing engine gave data traffic and voice traffic equal status. Administrators now designate voice traffic as priority. Data packets arriving at a router interface are directed into a data packet inbound queue for crypto engine processing. This queue is called the best effort queue. Voice packets arriving on a router interface are directed into



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

a priority packet inbound queue for crypto engine processing. This queue is called the priority queue. The crypto engine undertakes packet processing in a favorable ratio for voice packets. Voice packets are guaranteed a minimum processing bandwidth on the crypto engine.

## Benefits

The Low Latency Queueing (LLQ) for IPSec encryption engines feature guarantees a certain level of crypto engine processing time for priority designated traffic.



### Note

On the Cisco 2600 platform, with the exception of the Cisco 2691 router, the CPU utilization maximizes out before the crypto engine becomes congested, so latency is not improved.

### Better Voice Performance

Voice packets can be identified as priority, allowing the crypto engine to guarantee a certain percentage of processing bandwidth. This feature impacts the end user experience by assuring voice quality if voice traffic is directed onto a congested network.

### Improved Latency and Jitters

Predictability is a critical component of network performance. The Low Latency Queueing (LLQ) for IPSec encryption engines feature delivers network traffic predictability relating to VPN. With this feature disabled, an end user employing an IP phone over VPN might experience jitter or latency, both symptoms of overall network latency and congestion. With this feature enabled, these undesirable characteristics are dissipated.

## Restrictions

- No per-tunnel QoS policy. An interface QoS policy represents all tunnels.
- Assume the same IP precedence/DSCP marking for inbound and outbound voice packets.
- Assume the IP precedence/DSCP marking for voice packets are done at the source.
- Limited match criteria for voice traffic in the interface QoS policy.
- Assume call admission control is enforced within the enterprise.
- No strict error checking when aggregate policy's bandwidth exceeds crypto engine bandwidth. Only a warning is displayed but configuration is allowed.
- Assume voice packets are either all encrypted or unencrypted.

## Related Features and Technologies

- CBWFQ
- Priority Queueing
- Weighted Fair Queueing

## Related Documents

- [Quality of Service Solutions Command Reference](#), Cisco IOS Release 12.2
- [Class-Based Weighted Fair Queueing](#) feature module, Cisco IOS Release 12.1
- [IP RTP Priority](#) feature module, Cisco IOS Release 12.0

## Supported Platforms

### 12.2(14)S and higher

The LLQ for IPSec encryption engines feature is supported on the following platform:

- Cisco 7200 series

### 12.2(13)T

The LLQ for IPSec encryption engines feature is supported on all platforms using Cisco IOS Release 12.2(13)T or later, including:

- Cisco 2600 series
- Cisco 3600 series
- Cisco 7100 series
- Cisco 7200 series

## Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side-by-side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

## Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

## Supported Standards, MIBs, and RFCs

### Standards

- No new or modified standards are supported by this feature.

### MIBs

- No new or modified standards are supported by this feature.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

### RFCs

- No new or modified RFCs are supported by this feature.

## Prerequisites

To use this feature, you should be familiar with the following:

- Access control lists
- Bandwidth management
- CBWFQ

## Configuration Tasks

To configure LLQ for IPSec encryption engines, perform the tasks described in the following section.


**Note**

See the [Quality of Service Solutions Command Reference](#), Cisco IOS Release 12.2, to learn more about configuring server policies on interfaces.

- [Defining Class Maps](#) (required)
- [Configuring Class Policy in the Policy Map](#) (required)
- [Configuring Class Policy for a Priority Queue](#) (required)
- [Configuring Class Policy Using a Specified Bandwidth](#) (optional)
- [Configuring the Class-Default Class Policy](#) (optional)
- [Attaching the Service Policy](#) (required)
- [Verifying Configuration of Policy Maps and Their Classes](#) (optional)

## Defining Class Maps

To create a class map containing match criteria against which a packet is checked to determine if it belongs to a class, use the following commands beginning in global configuration mode:

|               | Command                                                                                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>class-map</b> class-map-name                                                                                                                                                                                               | Specifies the name of the class map to be created.                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Step 2</b> | Router(config-cmap)# <b>match access-group</b> {access-group / name access-group-name}<br><br>or<br><br>Router(config-cmap)# <b>match input-interface</b> interface-name<br><br>or<br><br>Router(config-cmap)# <b>match protocol</b> protocol | Specifies the name of the access control list (ACL) against whose contents packets are checked to determine if they belong to the class.<br><br>Specifies the name of the input interface used as a match criterion against which packets are checked to determine if they belong to the class.<br><br>Specifies the name of the protocol used as a match criterion against which packets are checked to determine if they belong to the class. |

## Configuring Class Policy in the Policy Map

To configure a policy map and create class policies that make up the service policy, begin with the **policy-map** command to specify the policy map name. Then use one or more of the following commands to configure the policy for a standard class or the default class:

- **priority**
- **bandwidth**
- **queue-limit** or **random-detect**
- **fair-queue** (for class-default class only)

For each class that you define, you can use one or more of the commands listed to configure the class policy. For example, you might specify bandwidth for one class and both bandwidth and queue limit for another class.

The default class of the policy map (commonly known as the class-default class) is the class to which traffic is directed if that traffic does not satisfy the match criteria of the other classes defined in the policy map.

You can configure class policies for as many classes as are defined on the router, up to the maximum of 64. However, the total amount of bandwidth allocated for all classes in a policy map must not exceed the minimum committed information rate (CIR) configured for the virtual circuit (VC) minus any bandwidth reserved by the **frame-relay voice bandwidth** and **frame-relay ip rtp priority** commands. If the minimum CIR is not configured, the bandwidth defaults to one half of the CIR. If all of the bandwidth is not allocated, the remaining bandwidth is allocated proportionally among the classes on the basis of their configured bandwidth.

To configure class policies in a policy map, perform the tasks described in the following sections. The task in the first section is required; the tasks in the remaining sections are optional.

## Configuring Class Policy for a Priority Queue

To configure a policy map and give priority to a class within the policy map, use the following commands beginning in global configuration mode:

|               | Command                                                | Purpose                                                                                                      |
|---------------|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config) # <b>policy-map</b> policy-map          | Specifies the name of the policy map to be created or modified.                                              |
| <b>Step 2</b> | Router(config-cmap) # <b>class</b> class-name          | Specifies the name of a class to be created and included in the service policy.                              |
| <b>Step 3</b> | Router(config-pmap-c) # <b>priority</b> bandwidth-kbps | Creates a strict priority class and specifies the amount of bandwidth, in kbps, to be assigned to the class. |

## Configuring Class Policy Using a Specified Bandwidth

To configure a policy map and create class policies that make up the service policy, use the following commands beginning in global configuration mode:

|               | Command                                                 | Purpose                                                                                                                                                                                                                                                                 |
|---------------|---------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config) # <b>policy-map</b> policy-map           | Specifies the name of the policy map to be created or modified.                                                                                                                                                                                                         |
| <b>Step 2</b> | Router(config-cmap) # <b>class</b> class-name           | Specifies the name of a class to be created and included in the service policy.                                                                                                                                                                                         |
| <b>Step 3</b> | Router(config-pmap-c) # <b>bandwidth</b> bandwidth-kbps | Specifies the amount of bandwidth to be assigned to the class, in kbps, or as a percentage of the available bandwidth. Bandwidth must be specified in kbps or as a percentage consistently across classes. (Bandwidth of the priority queue must be specified in kbps.) |

To configure more than one class in the same policy map, repeat [Step 2](#) and [Step 3](#).

## Configuring the Class-Default Class Policy

The class-default class is used to classify traffic that does not fall into one of the defined classes. Even though the class-default class is predefined when you create the policy map, you still have to configure it. If a default class is not configured, then traffic that does not match any of the configured classes is given best-effort treatment, which means that the network will deliver the traffic if it can, without any assurance of reliability, delay prevention, or throughput.

To configure a policy map and the class-default class, use the following commands beginning in global configuration mode:

|        | Command                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                        |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>policy-map</b> policy-map                                                                                                               | Specifies the name of the policy map to be created or modified.                                                                                                                                                                                                                |
| Step 2 | Router(config-cmap)# <b>class class-default</b><br><i>default-class-name</i>                                                                               | Specifies the default class so that you can configure or modify its policy.                                                                                                                                                                                                    |
| Step 3 | Router(config-pmap-c)# <b>bandwidth</b><br>bandwidth-kbps<br><br>or<br><br>Router(config-pmap-c)# <b>fair-queue</b><br>[ <i>number-of-dynamic-queues</i> ] | Specifies the amount of bandwidth, in kbps, to be assigned to the class.<br><br><br>Specifies the number of dynamic queues to be reserved for use by flow-based WFQ running on the default class. The number of dynamic queues is derived from the bandwidth of the interface. |

## Attaching the Service Policy

To attach a service policy to the output interface and enable LLQ for IPSec encryption engines, use the following command in map-class configuration mode:

|        | Command                                                       | Purpose                                                                                                         |
|--------|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>interface</b> type number                  | Specifies the interface using the LLQ for IPSec encryption engines.                                             |
| Step 2 | Router(config-if)# <b>service-policy output</b><br>policy-map | Attaches the specified service policy map to the output interface and enables LLQ for IPSec encryption engines. |

## Verifying Configuration of Policy Maps and Their Classes

To display the contents of a specific policy map or all policy maps configured on an interface, use the following commands in EXEC mode, as needed:

|        | Command                                  | Purpose                                                                                                                                        |
|--------|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router# <b>show frame-relay pvc dlci</b> | Displays statistics about the PVC and the configuration of classes for the policy map on the specified data-link connection identifier (DLCI). |

|        | Command                                                                     | Purpose                                                                                                 |
|--------|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Step 2 | Router# <b>show policy-map interface</b><br><i>interface-name</i>           | When LLQ is configured, displays the configuration of classes for all policy maps.                      |
| Step 3 | Router# <b>show policy-map interface</b><br><i>interface-name dlci dlci</i> | When LLQ is configured, displays the configuration of classes for the policy map on the specified DLCI. |

## Monitoring and Maintaining LLQ for IPsec Encryption Engines

To monitor and maintain LLQ for IPsec encryption engines, use the following command in EXEC mode:

|        | Command                            | Purpose                                                                               |
|--------|------------------------------------|---------------------------------------------------------------------------------------|
| Step 1 | Router# <b>show crypto eng qos</b> | Displays quality of service queueing statistics for LLQ for IPsec encryption engines. |

For a more detailed list of commands that can be used to monitor LLQ for IPsec encryption engines, see the section [“Verifying Configuration of Policy Maps and Their Classes”](#)

## Configuration Examples

This section provides the following configuration example:

- [LLQ for IPsec Encryption Engines Example](#)

### LLQ for IPsec Encryption Engines Example

In the following example, a strict priority queue with a guaranteed allowed bandwidth of 50 kbps is reserved for traffic that is sent from the source address 10.10.10.10 to the destination address 10.10.10.20, in the range of ports 16384 through 20000 and 53000 through 56000.

First, the following commands configure access list 102 to match the desired voice traffic:

```
Router(config)# access-list 102 permit udp host 10.10.10.10 host 10.10.10.20 range 16384 20000
Router(config)# access-list 102 permit udp host 10.10.10.10 host 10.10.10.20 range 53000 56000
```

Next, the class map voice is defined, and the policy map called policy1 is created; a strict priority queue for the class voice is reserved, a bandwidth of 20 kbps is configured for the class bar, and the default class is configured for WFQ. The service-policy command then attaches the policy map to the fas0/0.

```
Router(config)# class-map voice
Router(config-cmap)# match access-group 102
Router(config)# policy-map policy1
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 50
Router(config-pmap)# class bar
Router(config-pmap-c)# bandwidth 20
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue
Router(config)# interface fas0/0
```



```
Router(config-if)# service-policy output policy1
```

## Command Reference

The following new command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **show crypto eng qos**

For information about these commands, see the Cisco IOS Security Command Reference at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

## Glossary

**IKE**—Internet Key Exchange. IKE establishes a shared security policy and authenticates keys for services (such as IPSec). Before any IPSec traffic can be passed, each router/firewall/host must verify the identity of its peer. This can be done by manually entering preshared keys into both hosts or by a CA service.

**IPSec**—IP Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

---

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





# L2TP—IPSec Support for NAT and PAT Windows Clients

The L2TP—IPSec Support for NAT and PAT Windows Clients feature allows more than one Windows client to connect to a Layer 2 Tunneling Protocol (L2TP) Network Server (LNS) at one time with IP Security (IPSec) enabled and a network address translation (NAT) or port address translation (PAT) server between the Windows client and LNS.

Currently, if one Windows client is connected to a Cisco IOS LNS router through a NAT or PAT server with IPSec enabled, and then another Windows client connects to the same Cisco IOS LNS router, the first client's connection is effectively terminated. Enabling L2TP—IPSec Support for NAT and PAT Windows Clients ensures that Windows client connections in this environment are established and maintained until the connection is closed.

## History for the L2TP—IPSec Support for NAT and PAT Windows Clients Feature

| Release    | Modification                                      |
|------------|---------------------------------------------------|
| 12.3(11)T4 | This feature was introduced.                      |
| 12.4(1)    | This feature was integrated into Release 12.4(1). |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for L2TP—IPSec Support for NAT and PAT Windows Clients, page 2](#)
- [Restrictions for L2TP—IPSec Support for NAT and PAT Windows Clients, page 2](#)
- [Information About L2TP—IPSec Support for NAT and PAT Windows Clients, page 2](#)
- [How to Enable L2TP—IPSec Support for NAT and PAT Windows Clients, page 4](#)
- [Configuration Examples for L2TP—IPSec Support for NAT and PAT Windows Clients, page 6](#)



**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

- [Additional References, page 8](#)
- [Command Reference, page 10](#)

## Prerequisites for L2TP—IPSec Support for NAT and PAT Windows Clients

- You have an environment consisting of Windows clients and Cisco IOS LNS routers with IPSec enabled and a NAT or PAT server between the Windows client and LNS router.
- You must have a version of IPSec that contains the L2TP—IPSec Support for NAT and PAT Windows Clients feature.
- You must understand Windows 2000 concepts and configuration requirements.
- You must understand Cisco IOS LNS routers concepts and configuration requirements.
- You must understand NAT and PAT concepts and configuration requirements.
- You must understand IPSec concepts and configuration requirements.
- You must understand L2TP concepts and configuration requirements.

## Restrictions for L2TP—IPSec Support for NAT and PAT Windows Clients

- Tested only with Windows 2000 L2TP/IPsec clients running hotfix 818043.
- Port translation is not a standard default behavior. Port translation is incompatible with standard IPSec because it changes the LNS header port information.
- L2TP requires the client to have Microsoft DUN configured. L2TP is supported solely by Windows 2000 MS-DUN (L2TP is not supported by Windows 95, Windows 98, or Windows NT).

## Information About L2TP—IPSec Support for NAT and PAT Windows Clients

To use the L2TP—IPSec Support for NAT and PAT Windows Clients feature, the following concept should be understood:

- [How L2TP—IPSec Support for NAT and PAT Windows Clients Works, page 2](#)

## How L2TP—IPSec Support for NAT and PAT Windows Clients Works

With the L2TP—IPSec Support for NAT and PAT Windows Clients feature not enabled, Windows clients lose connection with the Cisco IOS LNS router when another Windows client establishes an IPSec-protected L2TP tunnel to the Cisco IOS LNS router when IPSec is enabled and there is a NAT or PAT server between the Windows clients and the LNS.

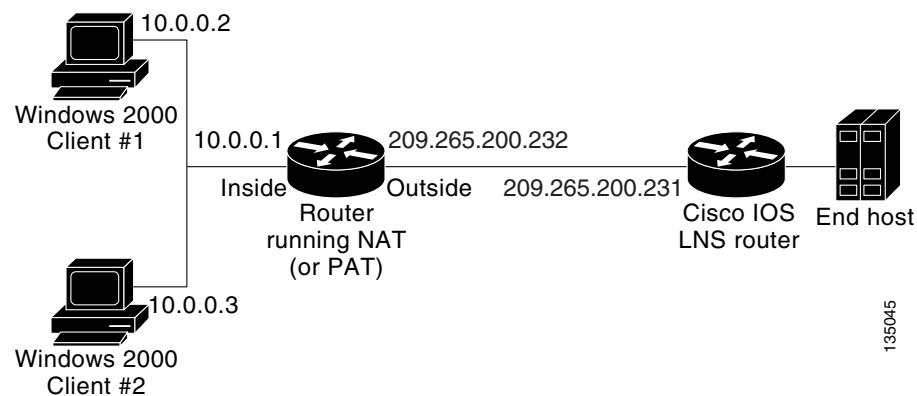
**Note**

If you do not have IPSec enabled, or you do not have a NAT or PAT server, you can have multiple Windows clients connect to a LNS without this command enabled.

### Without L2TP—IPSec Support for NAT and PAT Windows Clients Feature Enabled

For example, [Figure 91](#) shows two Windows 2000 clients that are trying to connect to the end host through the router running NAT or PAT and the same Cisco IOS LNS router. IPSec is enabled.

**Figure 91** Multiple Windows 2000 Clients, NAT Router, and Cisco IOS LNS Router with IP Addresses



The Windows 2000 Client #1 establishes an IPSec-protected L2TP tunnel to the Cisco IOS LNS router. The Windows 2000 client and the Cisco IOS LNS router recognize that there is a router running NAT between them and IPSec and NAT-Traversal (NAT-T) are enabled. The Windows 2000 client attempts to establish an IPSec security association (SA) and requests transport mode (which it does by default) with proxies from 10.0.0.2, its local address, to 209.265.200.231, the Cisco IOS LNS router's address.

In transport mode NAT, running on the router, translates all outgoing connections (including 10.0.0.2) to its outside IP address (209.265.200.232), the address the traffic will come in on. However, NAT cannot modify the L2TP port designation (1701), which is protected by the IPSec encrypted area. So now, we have a local address of 209.265.200.231, a remote address of 209.265.200.232 and a remote port of 1701. All traffic is sent to the Windows 2000 Client #1 that matches the tunnel 209.265.200.231, port 1701.

Then Windows 2000 Client #2 establishes an IPSec-protected L2TP tunnel to the Cisco IOS LNS router, again in transport mode. And NAT, again, translates all outgoing connections to its outside IP address (209.265.200.232), but it cannot modify the L2TP port designation (1701). All traffic is now sent to Windows 2000 Client #2 that matches tunnel 209.265.200.231, port 1701. This second Windows client connection has effectively ended Windows Client #1's connection to the Cisco IOS LNS router since it is no longer receiving traffic.

### With L2TP—IPSec Support for NAT and PAT Windows Clients Feature Enabled

With the L2TP—IPSec Support for NAT and PAT Windows Clients feature enabled, IPSec can translate the L2TP ports after decryption. This feature allows IPSec to map traffic from different hosts to different source ports. L2TP can now distinguish between traffic destined for multiple Windows 2000 clients.

So now, when an SA is created, a translated port will be assigned to it. This port is client-specific. The same port will be used for any new SA created by that client. When an encrypted request is received and decrypted, the source port is translated from the standard value, 1701, to a client specific value. The request with the translated port is then forwarded to L2TP.

As shown in [Figure 91](#) with port translation enabled, the Windows 2000 Client #1 would have a translated port number of 1024 assigned and Windows 2000 Client #2 would have a translated port number of 1025 assigned.

When L2TP sends the reply packet, it uses the translated port number and creates a packet to that destination port. IPSec uses the destination port number to select the SA with which to encrypt the packet. Before encrypting the packet, IPSec translates the destination port back to the standard port number, 1701, which the Windows 2000 client expects. IPSec encrypts the packet, either with the SA to Windows 2000 Client #1 if the destination port was 1024 or with the SA to Windows 2000 Client #2 if the destination port was 1025. And now, all traffic is sent to the appropriate client and multiple Windows clients can be connected to a Cisco IOS LNS router through a NAT server at the same time.

The connection is maintained until one of the following actions occurs:

- The IPSec connection is closed.
- The NAT or PAT device ends the session.
- The LNS closes the session.
- The Windows client closes the session.

## How to Enable L2TP—IPSec Support for NAT and PAT Windows Clients

This section contains the following procedure that allows you to enable NAT/PAT port translation:

- [Enabling L2TP—IPSec Support, page 4](#)

### Enabling L2TP—IPSec Support

Use the following task to enable L2TP—IPSec Support for NAT and PAT Windows Clients for environments that have IPSec enabled and include multiple windows clients, a NAT or PAT server, L2TP, and a Cisco IOS LNS router.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* [**ipsec-isakmp**]  
or  
**crypto dynamic-map** *dynamic-map-name dynamic-seq-num*
4. **set nat demux**
5. **exit**
6. **exit**
7. **show crypto map** [**interface** *interface* | **tag** *map-name*]  
or  
**show crypto dynamic-map** [**tag** *map-name*]
8. **show crypto ipsec sa**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                            | Purpose                                                                                                                                                                                                           |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                       | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                  |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                                                               | Enters global configuration mode.                                                                                                                                                                                 |
| Step 3 | <b>crypto map</b> <i>map-name</i> <i>seq-num</i> [ <b>ipsec-isakmp</b> ]<br><br><b>Example:</b><br>Router(config)# crypto map STATIC_MAP 5<br><br>or<br><b>crypto dynamic-map</b> <i>dynamic-map-name</i> <i>dynamic-seq-num</i><br><br><b>Example:</b><br>Router(config)# crypto dynamic-map DYNAMIC_MAP 10 | Names the static crypto map entry to create (or modify) and enters crypto map configuration mode.<br><br>or<br>Names the dynamic crypto map entry to create (or modify) and enters crypto map configuration mode. |
| Step 4 | <b>set nat demux</b><br><br><b>Example:</b><br>Router(config-crypto-map)# set nat demux                                                                                                                                                                                                                      | Enables L2TP—IPSec support.                                                                                                                                                                                       |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-crypto-map)# exit                                                                                                                                                                                                                                        | Exits crypto map configuration mode and returns to global configuration mode.                                                                                                                                     |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                                                                                                                                                                                                   | Exits global configuration mode and returns to privileged EXEC mode.                                                                                                                                              |

|        | Command or Action                                                                         | Purpose                                                                 |
|--------|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Step 7 | <b>show crypto map</b> [ <b>interface</b> <i>interface</i>   <b>tag</b> <i>map-name</i> ] | (Optional) Displays information about crypto map configuration.         |
|        | <b>Example:</b><br>Router# show crypto map                                                | or                                                                      |
|        | or                                                                                        |                                                                         |
|        | <b>show crypto dynamic-map</b> [ <b>tag</b> <i>map-name</i> ]                             | (Optional) Displays information about dynamic crypto map configuration. |
|        | <b>Example:</b><br>Router# show crypto dynamic-map                                        |                                                                         |
| Step 8 | <b>show crypto ipsec sa</b>                                                               | (Optional) Displays the settings used by current SAs.                   |
|        | <b>Example:</b><br>Router# show crypto ipsec sa                                           |                                                                         |

## Configuration Examples for L2TP—IPSec Support for NAT and PAT Windows Clients

This section provides the following configuration example:

- [Dynamic Map Configuration: Example, page 6](#)

### Dynamic Map Configuration: Example

The following example shows how to enable the L2TP—IPSec Support for NAT and PAT Windows Clients feature for a dynamic crypto map:

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 72_LNS
!
boot-start-marker
boot-end-marker
!
aaa new-model
!
!
aaa authentication ppp default local
aaa session-id common
ip subnet-zero
!
!
no ip cef
no ip domain lookup
ip domain name cisco.com
```



```
ip dhcp excluded-address 20.0.0.8
ip dhcp excluded-address 20.0.0.10
!
!
ip vrf VPN
 rd 1:1
!
!Enable virtual private networking.
vpdn enable
vpdn ip udp ignore checksum
!
! Default L2TP VPDN group
vpdn-group L2TP
!
!Enables the LNS to accept dial in requests; specifies L2TP as the tunneling
!protocol; specifies the number of the virtual templates used to clone
!virtual-access interfaces
 accept-dialin
 protocol l2tp
 virtual-template 1

!Disables L2TP tunnel authentication.
no l2tp tunnel authentication
!
!
crypto keyring L2TP
 pre-shared-key address 0.0.0.0 0.0.0.0 key *****
!
!Defines an Internet Key Exchange (IKE) policy and assigns priority 1.
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
 lifetime 3600
!
crypto isakmp key cisco hostname w2k01
crypto isakmp keepalive 3600
!
crypto ipsec security-association lifetime seconds 600
!
!Defines a transform set.
crypto ipsec transform-set TS1 esp-3des esp-sha-hmac
 mode transport
!
!Names the dynamic crypto map entry and enters crypto map configuration mode; Enables
!L2TP-IPSec support; Specifies which transform sets can be used with the crypto map
!entry
crypto dynamic-map DYN_MAP 10
 set nat demux
 set transform-set TS1!
!
crypto map CRYP_MAP 6000 ipsec-isakmp dynamic DYN_MAP
!
interface Loopback0
 ip address 12.0.0.8 255.255.255.255
!
interface FastEthernet0/0
 ip address 11.0.0.8 255.255.255.0
 no ip route-cache
 duplex full
 speed 100
 crypto map CRYP_MAP
!
interface FastEthernet0/1
```

```

ip address 20.0.0.8 255.255.255.0
duplex full
speed 100
!
interface FastEthernet2/0
ip address 172.19.192.138 255.255.255.0
duplex full
!
interface Virtual-Template1
ip unnumbered Loopback0
peer default ip address pool POOL
ppp mtu adaptive
ppp authentication chap ms-chap
!
router ospf 1
log-adjacency-changes
redistribute static subnets
network 11.0.0.0 0.0.0.255 area 0
!
ip local pool POOL 20.0.0.100 20.0.0.110
ip classless
ip route 171.0.0.0 255.0.0.0 172.19.192.1
!
no ip http server
no ip http secure-server
!
!
control-plane
!
gatekeeper
shutdown!
!
line con 0
exec-timeout 0 0
logging synchronous
stopbits 1
line aux 0
stopbits 1
line vty 0 4
!
end

```

## Additional References

The following sections provide references related to L2TP—IPSec Support for NAT and PAT Windows Clients.

## Related Documents

| Related Topic                       | Document Title                                                        |
|-------------------------------------|-----------------------------------------------------------------------|
| IP Security and Encryption Overview | <a href="#">Cisco IOS Security Configuration Guide</a> , Release 12.3 |
| Configuring IPSec Network Security  | <a href="#">Cisco IOS Security Configuration Guide</a> , Release 12.3 |

## Standards

| Standard | Title |
|----------|-------|
| None     | —     |

## MIBs

| MIB  | MIBs Link                                                                                                                                                                                                                  |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC  | Title |
|------|-------|
| None | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                         | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Command Reference

The following new command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **set nat demux**

For information about these commands, see the Cisco IOS Security Command Reference at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

---

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



# Pre-Fragmentation for IPSec VPNs

---

## Feature History

| Release                  | Modification                                                  |
|--------------------------|---------------------------------------------------------------|
| 12.1(11b)E               | This feature was introduced.                                  |
| 12.2(13)T                | This feature was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(14)S                | This feature was integrated into Cisco IOS Release 12.2(14)S. |
| Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers. |

This feature module describes the Pre-fragmentation for IPSec VPNs feature in Cisco IOS Release 12.2(13)T and 12.2(14)S. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 4](#)
- [Configuration Tasks, page 6](#)
- [Configuration Tasks, page 6](#)
- [Configuration Examples, page 8](#)
- [Command Reference, page 9](#)

## Feature Overview

When a packet is nearly the size of the maximum transmission unit (MTU) of the outbound link of the encrypting router, and it is encapsulated with IPSec headers, it is likely to exceed the MTU of the outbound link. This causes packet fragmentation after encryption, which makes the decrypting router reassemble in the process path. Pre-fragmentation for IPSec VPNs increases the decrypting router's performance by enabling it to operate in the high performance CEF path instead of the process path.

This feature allows an encrypting router to predetermine the encapsulated packet size from information available in transform sets, which are configured as part of the IPSec security association (SA). If it is predetermined that the packet will exceed the MTU of the output interface, the packet is fragmented before encryption. This function avoids process level reassembly before decryption and helps improve decryption performance and overall IPSec traffic throughput.



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

**Note**

---

The pre-fragmentation feature is turned off by default for tunnel interfaces. To receive pre-fragmentation performance benefits, turn pre-fragmentation on after insuring that the tunnel interfaces have the same MTU on both ends.

---

## Benefits

### Increased Performance

Delivers encryption throughput at maximum encryption hardware accelerator speeds. This performance increase is for near MTU-sized packets.

### Uniform Fragmentation

Packets are fragmented into equally sized units to prevent further downstream fragmentation.

### Interoperability

This feature is interoperable with all Cisco IOS platforms and a number of Cisco VPN clients.

## Restrictions

Take the following information into consideration before this feature is configured:

- Pre-fragmentation for IPsec VPNs operates in IPsec tunnel mode and IPsec tunnel mode with GRE, but not with IPsec transport mode.
- Pre-fragmentation for IPsec VPNs configured on the decrypting router in a unidirectional traffic scenario does not improve the performance or change the behavior of either of the peers.
- Pre-fragmentation for IPsec VPNs occurs before the transform is applied if compression is turned on for outgoing packets.
- Pre-fragmentation for IPsec VPNs functionality depends on the egress interface **crypto ipsec df-bit** configuration and the incoming packet “do not fragment” (DF) bit state. See [Table 1](#).

**Table 1** Pre-Fragmentation for IPsec VPNs Dependencies

| Pre-Fragmentation for IPsec VPNs Feature State (Enabled/Disabled) | Egress Interface “crypto ipsec df-bit” Configuration | Incoming Packet DF Bit State | Result                                                                               |
|-------------------------------------------------------------------|------------------------------------------------------|------------------------------|--------------------------------------------------------------------------------------|
| Enabled                                                           | crypto ipsec df-bit clear                            | 0                            | Fragmentation occurs before encryption.                                              |
| Enabled                                                           | crypto ipsec df-bit clear                            | 1                            | Fragmentation occurs before encryption.                                              |
| Disabled                                                          | crypto ipsec df-bit clear                            | 0                            | Fragmentation occurs after encryption and packets are reassembled before decryption. |
| Disabled                                                          | crypto ipsec df-bit clear                            | 1                            | Fragmentation occurs after encryption and packets are reassembled before decryption. |
| Enabled                                                           | crypto ipsec df-bit set                              | 0                            | Fragmentation occurs before encryption.                                              |

**Table 1** *Pre-Fragmentation for IPSec VPNs Dependencies (continued)*

| <b>Pre-Fragmentation for IPSec VPNs Feature State (Enabled/Disabled)</b> | <b>Egress Interface "crypto ipsec df-bit" Configuration</b> | <b>Incoming Packet DF Bit State</b> | <b>Result</b>                                                                        |
|--------------------------------------------------------------------------|-------------------------------------------------------------|-------------------------------------|--------------------------------------------------------------------------------------|
| Enabled                                                                  | crypto ipsec df-bit set                                     | 1                                   | Packets are dropped.                                                                 |
| Disabled                                                                 | crypto ipsec df-bit set                                     | 0                                   | Fragmentation occurs after encryption and packets are reassembled before decryption. |
| Disabled                                                                 | crypto ipsec df-bit set                                     | 1                                   | Packets are dropped.                                                                 |
| Enabled                                                                  | crypto ipsec df-bit copy                                    | 0                                   | Fragmentation occurs before encryption.                                              |
| Enabled                                                                  | crypto ipsec df-bit copy                                    | 1                                   | Packets are dropped.                                                                 |
| Disabled                                                                 | crypto ipsec df-bit copy                                    | 0                                   | Fragmentation occurs after encryption and packets are reassembled before decryption. |
| Disabled                                                                 | crypto ipsec df-bit copy                                    | 1                                   | Packets are dropped.                                                                 |

## Supported Platforms

### 12.2(14)S and higher

The Pre-fragmentation for IPSec VPN feature is supported on the following platforms:

- Cisco 7200 series
- Cisco 7400 series

### 12.2(13)T

The Pre-fragmentation for IPSec VPN feature is supported on all platforms using Cisco IOS Release 12.2(13)T or higher, including:

- Cisco 1710
- Cisco 1720
- Cisco 1721
- Cisco 1751
- Cisco 1760
- Cisco 2600
- Cisco 2691
- Cisco 3620
- Cisco 3640
- Cisco 3660



- Cisco 3725
- Cisco 3745
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7400 series

#### 12.1(11b)E

The Pre-fragmentation for IPSec VPN feature is supported on all platforms using Cisco IOS Release 12.1(11b)E or higher, including:

- Cisco 7100 series

#### Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

#### Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

# Supported Standards, MIBs, and RFCs

## Standards

- No new or modified standards are supported by this feature.

## MIBs

- No new or modified standards are supported by this feature.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

## RFCs

- No new or modified RFCs are supported by this feature.

## Configuration Tasks

See the following sections for configuration tasks for the Pre-fragmentation for IPSec VPNs feature. Each task in the list is identified as either required or optional.

- [Configuring Pre-Fragmentation For IPSec VPNs](#) (required)
- [Verifying Pre-Fragmentation For IPSec VPNs](#) (optional)

## Configuring Pre-Fragmentation For IPSec VPNs

Pre-fragmentation for IPSec VPNs is globally enabled by default. To enable or disable pre-fragmentation for IPSec VPNs while in interface configuration mode, enter the commands in the following table. Use the **no** form of the commands to revert back to the default configuration, or use the commands themselves to enable configuration of the pre-fragmentation IPSec VPNs.



### Note

---

Manually enabling or disabling this feature will override the global configuration.

---

| Command                                                                | Purpose                                                     |
|------------------------------------------------------------------------|-------------------------------------------------------------|
| Router(config-if)# <b>crypto ipsec fragmentation before-encryption</b> | Enables pre-fragmentation for IPsec VPNs on the interface.  |
| Router(config-if)# <b>crypto ipsec fragmentation after-encryption</b>  | Disables pre-fragmentation for IPsec VPNs on the interface. |
| Router(config)# <b>crypto ipsec fragmentation before-encryption</b>    | Enables pre-fragmentation for IPsec VPNs globally.          |
| Router(config)# <b>crypto ipsec fragmentation after-encryption</b>     | Disables pre-fragmentation for IPsec VPNs globally.         |

## Verifying Pre-Fragmentation For IPsec VPNs

To verify that this feature is enabled, consult the interface statistics on the encrypting router and the decrypting router. If fragmentation occurs on the encrypting router, and no reassembly occurs on the decrypting router, fragmentation is happening before encryption, and thus the packets are not being reassembled before decryption. This means that the feature is enabled.



### Note

This method of verification does not apply to packets destined for the decrypting router.

- Step 1** Enter the **show running-configuration** command on the encrypting router. If the feature is enabled, you will observe output similar to the following:

```
Router# show running-configuration
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key abcd123 address 25.0.0.7
!
!
crypto ipsec transform-set fooprime esp-3des esp-sha-hmac
!
crypto map bar 10 ipsec-isakmp
 set peer 25.0.0.7
 set transform-set fooprime
 match address 102
```

If the feature has been disabled, you will observe output similar to the following:

```
Router# show running-configuration
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key abcd123 address 25.0.0.7
!
!
crypto ipsec transform-set fooprime esp-3des esp-sha-hmac
crypto ipsec fragmentation after-encryption
!
crypto map bar 10 ipsec-isakmp
 set peer 25.0.0.7
 set transform-set fooprime
 match address 102
```

- Step 2** Enter the **show running-configuration interface *type number*** command to display statistics for the encrypting router egress interface. If the feature is enabled, you will observe output similar to the following:

```
Router# show running-configuration interface fastethernet 0/0
interface FastEthernet0/0
 ip address 25.0.0.6 255.0.0.0
 no ip mroute-cache
 load-interval 30
 duplex full
 speed 100
 crypto map bar
```

If the feature has been disabled, you will observe output similar to the following:

```
Router# show running-configuration interface fastethernet 0/0

interface FastEthernet0/0
 ip address 25.0.0.6 255.0.0.0
 no ip mroute-cache
 load-interval 30
 duplex full
 speed 100
 crypto map bar
 crypto ipsec fragmentation after-encryption
```

## Configuration Examples

This section provides the following configuration example:

- [Enabling Pre-Fragmentation For IPSec VPNs Example](#)

### Enabling Pre-Fragmentation For IPSec VPNs Example

The following configuration example shows how to configure the Pre-Fragmentation for IPSec VPNs feature:



#### Note

This feature does not show up in the running configuration in this example because the default global pre-fragmentation for IPSec VPNs feature is enabled. Pre-fragmentation for IPSec VPNs shows in the running configuration only when you explicitly enable the feature on the interface.

```
crypto isakmp policy 10
 authentication pre-share
 crypto isakmp key abcd123 address 25.0.0.7
 !
 !
 crypto ipsec transform-set fooprime esp-3des esp-sha-hmac
 !
 crypto map bar 10 ipsec-isakmp
 set peer 25.0.0.7
 set transform-set fooprime
 match address 102
```

# Command Reference

The following commands are introduced or modified in the feature or features

- **crypto ipsec fragmentation**
- **crypto ipsec fragmentation (interface configuration)**

For information about these commands, see the Cisco IOS Security Command Reference at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





# Real-Time Resolution for IPSec Tunnel Peer

---

After a user specifies a host name (instead of an IP address) for remote IP Security (IPSec) peer, the Real-Time Resolution for IPSec Tunnel Peer feature allows the host name to be domain name server (DNS) resolved before the router establishes the IPSec tunnel. Thus, the router can immediately discover whether the IP address of the peer has changed.

## Feature History for Real-Time Resolution for IPSec Tunnel Peer

| Release                  | Modification                                                  |
|--------------------------|---------------------------------------------------------------|
| 12.3(4)T                 | This feature was introduced.                                  |
| Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Restrictions for Real-Time Resolution for IPSec Tunnel Peer, page 2](#)
- [Information About Real-Time Resolution for IPSec Tunnel Peer, page 2](#)
- [How to Configure Real-Time Resolution, page 2](#)
- [Configuration Examples for Real-Time Resolution, page 4](#)
- [Additional References, page 5](#)
- [Command Reference, page 6](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

# Restrictions for Real-Time Resolution for IPsec Tunnel Peer

## Secure DNS Requirement

It is recommended that you use this feature only with secure DNS and when the DNS responses can be authenticated. Otherwise, an attacker can spoof or forge DNS responses and have access to Internet Key Exchange (IKE) authentication data, such as a certificate. If an attacker has a certificate that is trusted by the initiating host, the attacker can successfully establish Phase 1 IKE security association (SA), or the attacker can try to guess the preshared key that is shared between the initiator and the actual responder.

## DNS Initiator

DNS names resolution for remote IPsec peers will work only if they are used as an initiator. The first packet that is to be encrypted will trigger a DNS lookup; after the DNS lookup is complete, subsequent packets will trigger IKE.

# Information About Real-Time Resolution for IPsec Tunnel Peer

To configure real-time resolution for your IPsec peer, you should understand the following concept:

- [Benefits of Real-Time Resolution Via Secure DNS, page 2](#)

## Benefits of Real-Time Resolution Via Secure DNS

When specifying the host name of a remote IPsec peer via the **set peer** command, you can also issue the **dynamic** keyword, which defers DNS resolution of the host name until right before the IPsec tunnel has been established. Deferring resolution enables the Cisco IOS software to detect whether the IP address of the remote IPsec peer has changed. Thus, the software can contact the peer at the new IP address.

If the **dynamic** keyword is not issued, the host name is resolved immediately after it is specified. So, the Cisco IOS software cannot detect an IP address change and, therefore, attempts to connect to the IP address that it previously resolved.

DNS resolution assures users that their established IPsec tunnel is secure and authenticated.

# How to Configure Real-Time Resolution

This section contains the following procedure:

- [Configuring Real-Time Resolution for IPsec Peers, page 2](#)

## Configuring Real-Time Resolution for IPsec Peers

Use this task to configure a router to perform real-time DNS resolution with a remote IPsec peer; that is, the host name of peer is resolved via a DNS lookup right before the router establishes a connection (an IPsec tunnel) with the peer.



## Prerequisites

Before creating a crypto map, you should perform the following tasks:

- Define Internet Security Association Key Management Protocol (ISAKMP) policies.
- Define IPSec transform sets.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num ipsec-isakmp*
4. **match address** *access-list-id*
5. **set peer** {*host-name* [**dynamic**] | *ip-address*}
6. **set transform-set** *transform-set-name1* [*transform-set-name2...transform-set-name6*]

## DETAILED STEPS

|        | Command or Action                                                                                                                       | Purpose                                                                                                                                                                                                  |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                  | Enables privileged EXEC mode.<br><br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                          | Enters global configuration mode.                                                                                                                                                                        |
| Step 3 | <b>crypto map</b> <i>map-name seq-num ipsec-isakmp</i><br><br><b>Example:</b><br>Router(config)# crypto map secure_b 10<br>ipsec-isakmp | Specifies the crypto map entry to create (or modify) and enters crypto map configuration mode.                                                                                                           |
| Step 4 | <b>match address</b> <i>access-list-id</i><br><br><b>Example:</b><br>Router(config-crypto-m)# match address 140                         | Names an extended access list.<br><br>This access list determines which traffic should be protected by IPSec and which traffic should not be protected by IPSec in the context of this crypto map entry. |

|        | Command or Action                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <b>set peer</b> {host-name [ <b>dynamic</b> ]   ip-address}<br><br><b>Example:</b><br>Router(config-crypto-m)# set peer b.cisco.com dynamic                         | Specifies a remote IPSec peer.<br><br>This is the peer to which IPSec-protected traffic can be forwarded. <ul style="list-style-type: none"> <li><b>dynamic</b>—Allows the host name to be resolved via a DNS lookup just before the router establishes the IPSec tunnel with the remote peer. If this keyword is not specified, the host name will be resolved immediately after the host name is specified.</li> </ul> Repeat for multiple remote peers. |
| Step 6 | <b>set transform-set</b> transform-set-name1 [transform-set-name2...transform-set-name6]<br><br><b>Example:</b><br>Router(config-crypto-m)# set transform-set myset | Specifies which transform sets are allowed for this crypto map entry. List multiple transform sets in order of priority (highest priority first).                                                                                                                                                                                                                                                                                                          |

## Troubleshooting Tips

To display crypto map configuration information, use the **show crypto map** command.

## What to Do Next

You need to apply a crypto map set to each interface through which IPSec traffic will flow. Applying the crypto map set to an interface instructs the router to evaluate all the interface's traffic against the crypto map set and to use the specified policy during connection or security association (SA) negotiation on behalf of traffic to be protected by crypto.

# Configuration Examples for Real-Time Resolution

This section provides the following configuration example:

- [Configuring Real-Time Resolution for an IPSec Peer: Example, page 4](#)

## Configuring Real-Time Resolution for an IPSec Peer: Example

[Figure 1](#) and the following example illustrate how to create a crypto map that configures the host name of a remote IPSec peer to DNS resolved via a DNS lookup right before the Cisco IOS software attempts to establish a connection with that peer.

**Figure 1      Real-Time Resolution Sample Topology**

```
! Configure the initiating router.
hostname a.cisco.com
ip domain name cisco.com
ip name server 10.0.0.1
!
crypto map secure_b 10 ipsec-isakmp
 match address 140
 set peer b.cisco.com dynamic
 set transform-set xset
interface serial1
 ip address 30.0.0.1
 crypto map secure_b
access-list 140 permit ...
!
! Configure the responding router (the remote IPSec peer).
hostname b.cisco.com
!
crypto map secure_a 10 ipsec-isakmp
 match address 150
 set peer 30.0.0.1
 set transform-set
interface serial0/1
 ip address 40.0.0.1
 crypto map secure_a
access-list 150 ...

! DNS server configuration

b.cisco.com 40.0.0.1 # the address of serial0/1 of b.cisco.com
```

## Additional References

The following sections provide references related to Real-Time Resolution for IPSec Tunnel Peer.

## Related Documents

| Related Topic                        | Document Title                                                                                                         |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Crypto maps                          | <i>The chapter “Configuring IPSec Network Security” in the Cisco IOS Security Configuration Guide</i>                  |
| ISAKMP policies                      | The chapter “Configuring Internet Key Exchange Security Protocol” in the <i>Cisco IOS Security Configuration Guide</i> |
| IPSec and IKE configuration commands | <i>Cisco IOS Security Command Reference, Release 12.3 T</i>                                                            |

## Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

## MIBs

| MIBs | MIBs Link                                                                                                                                                                                                                  |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs | Title |
|------|-------|
| None | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following commands are introduced or modified in the feature or features

- **set peer (IPSec)**

For information about these commands, see the Cisco IOS Security Command Reference at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





# Reverse Route Injection

---

**First Published: August 16, 2001**

**Last Updated: November 5, 2007**

Reverse route injection (RRI) is the ability for static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint. These protected hosts and networks are known as remote proxy identities.

Each route is created on the basis of the remote proxy network and mask, with the next hop to this network being the remote tunnel endpoint. By using the remote Virtual Private Network (VPN) router as the next hop, the traffic is forced through the crypto process to be encrypted.

Enhancements to the default behavior of RRI, the addition of a route tag value, and enhancements to how RRI is configured were added to the Reverse Route Injection feature in Cisco IOS Release 12.3(14)T.

An enhancement was added in Cisco IOS Release 12.4(15)T that allows a distance metric to be set for routes that are created by a VPN process so that the dynamically learned route on a router can take precedence over a locally configured static route.

## **Finding Feature Information in This Module**

*Your Cisco IOS software release may not support all of the features documented in this module.* To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Reverse Route Injection”](#) section on page 18.

## **Finding Support Information for Platforms and Cisco IOS Catalyst OS Software Images**

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for Reverse Route Injection, page 2](#)
- [Restrictions for Reverse Route Injection, page 2](#)
- [Information About Reverse Route Injection, page 2](#)
- [How to Configure Reverse Route Injection, page 4](#)



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

- [Configuration Examples for Reverse Route Injection, page 10](#)
- [Additional References, page 16](#)
- [Command Reference, page 17](#)
- [Feature Information for Reverse Route Injection, page 26](#)

## Prerequisites for Reverse Route Injection

- IP routing should be enabled and static routes should be redistributed if dynamic routing protocols are to be used to propagate RRI-generated static routes.

## Restrictions for Reverse Route Injection

- If RRI is applied to a crypto map, that map must be unique to one interface on the router. In other words, the same crypto map cannot be applied to multiple interfaces. If more than one crypto map is applied to multiple interfaces, routes may not be cleaned up correctly. If multiple interfaces require a crypto map, each must use a uniquely defined map. This restriction applies only to RRI before Cisco IOS Release 12.3(14)T.
- For static crypto maps, routes are always present if RRI is configured on an applied crypto map. In Cisco IOS Release 12.3(14)T, the default behavior—of routes always being present for a static map—will not apply unless the **static keyword** is added to the **reverse-route** command.

## Information About Reverse Route Injection

To configure the Reverse Route Injection enhancements, you should understand the following concepts:

- [Reverse Route Injection, page 2](#)
- [Enhancements to Reverse Route Injection in Cisco IOS Release 12.4\(15\)T, page 3](#)

## Reverse Route Injection

RRI is the ability for static routes to be automatically inserted into the routing process for those networks and hosts that are protected by a remote tunnel endpoint. These protected hosts and networks are known as remote proxy identities.

Each route is created on the basis of the remote proxy network and mask, with the next hop to this network being the remote tunnel endpoint. By using the remote VPN router as the next hop, the traffic is forced through the crypto process to be encrypted.

After the static route is created on the VPN router, this information is propagated to upstream devices, allowing them to determine the appropriate VPN router to which to send returning traffic in order to maintain IPsec state flows. Being able to determine the appropriate VPN router is particularly useful if multiple VPN routers are used at a site to provide load balancing or failover or if the remote VPN devices are not accessible via a default route. Routes are created in either the global routing table or the appropriate virtual route forwarding (VRF) table.

RRI is applied on a per-crypto map basis, whether this is via a static crypto map or a dynamic crypto map template. The default behavior for the two map types is as follows:



- In the case of a dynamic crypto map, routes are created upon the successful establishment of IPsec security associations (SAs) for those remote proxies. The next hop back to those remote proxies is via the remote VPN router whose address is learned and applied during the creation of the dynamic crypto map template. The routes are deleted after the SAs are deleted. In Cisco IOS Release 12.3(14)T, the creation of routes on the basis of IPsec source proxies on static crypto maps was added. This behavior became the default behavior on static maps and overrode the creation of routes on the basis of crypto ACLs (see the next bullet).
- For static crypto maps, routes are created on the basis of the destination information defined in the crypto access list. The next hop is taken from the first set peer statement that is attached to the crypto map. If at any time, RRI, the peer, or the access list is removed from the crypto map, routes will be deleted. This behavior changes with the addition of the RRI enhancements, as explained in the sections below.

## Enhancements to Reverse Route Injection in Cisco IOS Release 12.4(15)T

The following enhancements have been added to the Reverse Route Injection feature in Cisco IOS Release 12.4(15)T:

- [RRI Distance Metric, page 3](#)
- [Gateway Option, page 3](#)
- [Support for RRI on IPsec Profiles, page 4](#)
- [Tag Option Configuration Changes, page 4](#)
- [show crypto route Command, page 4](#)

### RRI Distance Metric

In general, a static route is created having an administrative distance of 1, which means that static routes always have precedence in the routing table. In some scenarios, however, it is required that dynamically learned routes take precedence over static routes, with the static route being used in the absence of a dynamically learned route. The addition of the **set reverse-route distance** command under either a crypto map or IPsec profile allows you to specify a different distance metric for VPN-created routes so that those routes will be in effect only if a dynamic or more favored route becomes unavailable.

### Gateway Option

This RRI gateway option is relevant to the crypto map only.

This option allows you to configure unique next hops or gateways for remote tunnel endpoints. The option is identical to the way the **reverse-route remote-peer** {*ip-address*} command worked prior to Cisco IOS Release 12.3(14)T in that two routes are created for each VPN tunnel. The first route is to the destination-protected subnet via the remote tunnel endpoint. The second route specifies the next hop to be taken to reach this tunnel endpoint. This RRI gateway option allows specific default paths to be specified for specific groups of VPN connections on platforms that support recursive route lookups.



#### Note

In 12.4(15)T and later releases, the **gateway** keyword option replaces the **reverse-route remote-peer** command (with no *ip-address*). Due to changes to Cisco Express Forwarding (CEF), an interface as a next-hop cannot be used without also adding a next-hop IP address.

## Support for RRI on IPsec Profiles

Previously RRI was available for crypto map configurations only. Cisco IOS Release 12.4(15)T introduces support for relevant RRI options on IPsec profiles that are predominantly used for virtual tunnel interfaces. On tunnel interfaces, only the distance metric and tag options are useful with the generic RRI capability.

**Note**

It is not necessary to specifically enable RRI on dynamic virtual interfaces for Easy VPN clients. Route support is enabled by default. It is necessary to specify tag or distance metric values if these are required.

## Tag Option Configuration Changes

The tag option was introduced in 12.3(14)T for crypto maps. This option is now supported with IPsec profiles under the **set reverse-route tag** command syntax. The **set reverse-route tag** command is also available under the crypto map for uniformity although the legacy **reverse-route tag** command is no longer supported.

## show crypto route Command

The **show crypto route** command displays routes that are created through IPsec via RRI or Easy VPN virtual tunnel interfaces (VTIs). The routes are displayed in one table. To see sample output for the **show crypto route** command, see the section “[show crypto route Command Output: Example](#).”

# How to Configure Reverse Route Injection

The following sections show how to configure reverse route injection for Cisco IOS software before Release 12.4(15)T and for Release 12.4(15)T.

- [Configuring RRI on Crypto Maps for Cisco IOS Releases Prior to 12.4\(15\)T, page 4](#)
- [Configuring RRI with Enhancements Added in Cisco IOS Release 12.4\(15\)T, page 6](#)

## Configuring RRI on Crypto Maps for Cisco IOS Releases Prior to 12.4(15)T

This section includes the following tasks:

- [Configuring RRI Under a Static Crypto Map, page 4](#)
- [Configuring RRI Under a Dynamic Map Template, page 5](#)

## Configuring RRI Under a Static Crypto Map

To configure RRI under a static crypto map for Cisco IOS software prior to Release 12.4(15)T, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **crypto map** {*map-name*} {*seq-name*} **ipsec-isakmp**
4. **reverse-route** [**static** | **tag** *tag-id* [**static**] | **remote-peer** [**static**] | **remote-peer** *ip-address* [**static**]]

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                              | Purpose                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                                 | Enters global configuration mode.                                                                                |
| Step 3 | <b>crypto map</b> { <i>map-name</i> } { <i>seq-name</i> } <b>ipsec-isakmp</b><br><br><b>Example:</b><br>Router (config)# crypto map mymap 1<br>ipsec-isakmp                                                                                                                    | Creates or modifies a crypto map entry and enters crypto map configuration mode.                                 |
| Step 4 | <b>reverse-route</b> [ <b>static</b>   <b>tag</b> <i>tag-id</i> [ <b>static</b> ]   <b>remote-peer</b> [ <b>static</b> ]   <b>remote-peer</b> <i>ip-address</i> [ <b>static</b> ]]<br><br><b>Example:</b><br>Router (config-crypto-map)# reverse-route<br>remote peer 10.1.1.1 | Creates source proxy information for a crypto map entry.                                                         |

## Configuring RRI Under a Dynamic Map Template

To configure RRI under a dynamic map template for Cisco IOS software prior to Release 12.4(15)T, perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto dynamic-map** *dynamic-map-name* *dynamic-seq-name*
4. **reverse-route** [**static** | **tag** *tag-id* [**static**] | **remote-peer** [**static**] | **remote-peer** *ip-address* [**static**]]

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                        | Purpose                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                           | Enters global configuration mode.                                                                                |
| Step 3 | <b>crypto dynamic-map</b> <i>dynamic-map-name</i> <i>dynamic-seq-name</i><br><br><b>Example:</b><br>Router (config)# crypto dynamic-map mymap 1                                                                                                                          | Creates a dynamic crypto map entry and enters the crypto map configuration command mode.                         |
| Step 4 | <b>reverse-route</b> [ <b>static</b>   <b>tag</b> <i>tag-id</i> [ <b>static</b>   <b>remote-peer</b> [ <b>static</b>   <b>remote-peer</b> <i>ip-address</i> [ <b>static</b> ]]]<br><br><b>Example:</b><br>Router (config-crypto-map)# reverse-route remote peer 10.1.1.1 | Creates source proxy information for a crypto map entry.                                                         |

## Configuring RRI with Enhancements Added in Cisco IOS Release 12.4(15)T

The following sections show how to configure RRI with the enhancements that were added in Cisco IOS Release 12.4(15)T:

- [Configuring RRI with Enhancements Under a Static Crypto Map, page 6](#)
- [Configuring RRI with Enhancements Under a Dynamic Map Template, page 7](#)
- [Configuring a RRI Distance Metric Under an IPsec Profile, page 8](#)
- [Verifying Routes That Are Created Through IPsec via RRI or Easy VPN VTIs, page 9](#)

## Configuring RRI with Enhancements Under a Static Crypto Map

To configure RRI with enhancements under a static crypto map (for Cisco IOS Release 12.4(15)T and later releases), perform the following steps.

## SUMMARY STEPS

- enable**
- configure terminal**
- crypto map** *map-name* *seq-name* **ipsec-isakmp**
- reverse-route** [**static** | **remote-peer** *ip-address* [**gateway** ] [**static**]]
- set reverse-route** [**distance** *number* | **tag** *tag-id*]

## DETAILED STEPS

|        | Command or Action                                                                                                                             | Purpose                                                                                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                        | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                | Enters global configuration mode.                                                                                                                                                       |
| Step 3 | <b>crypto map map-name seq-name ipsec-isakmp</b><br><br><b>Example:</b><br>Router (config)# crypto map mymap 1 ipsec-isakmp                   | Creates or modifies a crypto map entry and enters crypto map configuration mode.                                                                                                        |
| Step 4 | <b>reverse-route [static   remote-peer ip-address [gateway] [static]]</b><br><br><b>Example:</b><br>Router (config-crypto-map)# reverse-route | Creates source proxy information for a crypto map entry.<br><br><b>Note</b> The <b>gateway</b> keyword can be added to enable the dual route functionality for default gateway support. |
| Step 5 | <b>set reverse-route [distance number   tag tag-id]</b><br><br><b>Example:</b><br>Router (config-crypto-map)# set reverse-route distance 20   | Specifies a distance metric to be used or a tag value to be associated with these routes.                                                                                               |

## Configuring RRI with Enhancements Under a Dynamic Map Template

To configure RRI with enhancements under a dynamic map template (for Cisco IOS Release 12.4(15)T and later releases), perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto dynamic-map dynamic-map-name dynamic-seq-name**
4. **reverse-route [static | remote-peer ip-address [gateway] [static]]**
5. **set reverse-route [distance number | tag tag-id]**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                        | Purpose                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                           | Enters global configuration mode.                                                                                |
| Step 3 | <b>crypto dynamic-map</b> <i>dynamic-map-name</i><br><i>dynamic-seq-name</i><br><br><b>Example:</b><br>Router (config)# crypto dynamic-map mymap 1                                                                       | Creates a dynamic crypto map entry and enters the crypto map configuration command mode.                         |
| Step 4 | <b>reverse-route</b> [ <b>static</b>   <b>remote-peer</b> <i>ip-address</i><br>[ <i>gateway</i> ] [ <b>static</b> ]]<br><br><b>Example:</b><br>Router (config-crypto-map)# reverse-route<br>remote peer 10.1.1.1 gateway | Creates source proxy information for a crypto map entry.                                                         |
| Step 5 | <b>set reverse-route</b> [ <b>distance</b> <i>number</i>   <b>tag</b><br><i>tag-id</i> ]<br><br><b>Example:</b><br>Router (config-crypto-map)# set reverse-route<br>distance 20                                          | Specifies a distance metric to be used or a tag value to be associated with these routes.                        |

## Configuring a RRI Distance Metric Under an IPsec Profile

To configure a RRI distance metric under an IPsec profile for Cisco IOS Release 12.4(15)T and later releases, perform the following steps:

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec profile** *name*
4. **set reverse-route** [**distance** *number* | **tag** *tag-id*]

## DETAILED STEPS

|        | Command or Action                                                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                             |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                          | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                    |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                  | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                   |
| Step 3 | <b>crypto ipsec profile name</b><br><br><b>Example:</b><br>Router (config)# crypto ipsec profile myprofile                                      | Creates or modifies an IPsec profile and enters IPsec profile configuration mode.                                                                                                                                                                                                                                                                   |
| Step 4 | <b>set reverse-route [distance number   tag tag-id]</b><br><br><b>Example:</b><br>Router (config-crypto-profile)# set reverse-route distance 20 | Defines a distance metric for each static route or tags a reverse route injection- (RRI-) created route. <ul style="list-style-type: none"> <li><b>distance</b>—Defines a distance metric for each static route.</li> <li><b>tag</b>—Sets a tag value that can be used as a “match” value for controlling distribution using route maps.</li> </ul> |

## Verifying Routes That Are Created Through IPsec via RRI or Easy VPN VTIs

To display routes that are created through IPsec via RRI or Easy VPN VTIs, perform the following steps.

## SUMMARY STEPS

1. enable
2. show crypto route

## DETAILED STEPS

|        | Command or Action                                                            | Purpose                                                                                                          |
|--------|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                       | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>show crypto route</b><br><br><b>Example:</b><br>Router# show crypto route | Displays routes that are created through IPsec via RRI or Easy VPN VTIs.                                         |

## Troubleshooting Tips

To observe the behavior of RRI and its relationship to the creation and deletion of an IPsec SA, you can use the **debug crypto ipsec** command (see the [Cisco IOS Debug Command Reference](#), Release 12.4T).

# Configuration Examples for Reverse Route Injection

This section contains the following sections:

- [Configuring RRI Prior to Cisco IOS Release 12.3\(14\)T: Examples, page 10](#)
- [Configuring RRI with Enhancements Added in Cisco IOS Release 12.3\(14\)T: Examples, page 11](#)
- [Configuring RRI with Enhancements Added in Cisco IOS Release 12.4\(15\)T: Examples, page 12](#)

## Configuring RRI Prior to Cisco IOS Release 12.3(14)T: Examples

The following are examples of RRI configurations and output before Cisco IOS Release 12.3(14)T:

- [Configuring RRI When Crypto ACLs Exist: Example, page 10](#)
- [Configuring RRI When Two Routes Are Created, One for the Remote Endpoint and One for Route Recursion: Example, page 11](#)

### Configuring RRI When Crypto ACLs Exist: Example

The following example shows that all remote VPN gateways connect to the router via 192.168.0.3. RRI is added on the static crypto map, which creates routes on the basis of the source network and source netmask that are defined in the crypto access control list (ACL):

```
crypto map mymap 1 ipsec-isakmp
 set peer 10.1.1.1
 reverse-route
 set transform-set esp-3des-sha
 match address 102

Interface FastEthernet 0/0
 ip address 192.168.0.2 255.255.255.0
 standby name group1
 standby ip 192.168.0.3
 crypto map mymap redundancy group1

access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
```

In Cisco IOS Release 12.3(14)T and later releases, for the static map to retain this same behavior of creating routes on the basis of crypto ACL content, the **static** keyword is required, that is, **reverse-route static**.



#### Note

The **reverse-route** command in this situation creates routes that are analogous to the following static route command-line interface (CLI) commands (**ip route**):

#### Remote Tunnel Endpoint

```
ip route 10.1.1.1 255.255.255.255 192.168.1.1
```



**VPNSM**

```
ip route 10.1.1.1 255.255.255.255 vlan0.1
```

---

## Configuring RRI When Two Routes Are Created, One for the Remote Endpoint and One for Route Recursion: Example

In the following example, two routes are created, one for the remote endpoint and one for route recursion to the remote endpoint via the interface on which the crypto map is configured:

```
reverse-route remote-peer
```

## Configuring RRI with Enhancements Added in Cisco IOS Release 12.3(14)T: Examples

The following are examples of configurations and output for RRI enhancements that were added in Cisco IOS Release 12.3(14)T.

- [Configuring RRI When Crypto ACLs Exist: Example, page 11](#)
- [Configuring RRI with Route Tags: Example, page 11](#)
- [Configuring RRI for One Route to the Remote Proxy via a User-Defined Next Hop: Example, page 12](#)

### Configuring RRI When Crypto ACLs Exist: Example

The following example shows that RRI has been configured for a situation in which there are existing ACLs:

```
crypto map mymap 1 ipsec-isakmp
 set peer 172.17.11.1
 reverse-route static
 set transform-set esp-3des-sha
 match address 101

access-list 101 permit ip 192.168.1.0 0.0.0.255 172.17.11.0 0.0.0.255
```

### Configuring RRI with Route Tags: Example

The following example shows how RRI-created routes can be tagged with a tag number and then used by a routing process to redistribute those tagged routes via a route map:

```
crypto dynamic-map ospf-clients 1
 reverse-route tag 5

router ospf 109
 redistribute rip route-map rip-to-ospf

route-map rip-to-ospf permit
 match tag 5
 set metric 5
 set metric-type type1

Router# show ip ospf topology
```

```
P 10.81.7.48/29, 1 successors, FD is 2588160, tag is 5
 via 192.168.82.25 (2588160/2585600), FastEthernet0/1
```

## Configuring RRI for One Route to the Remote Proxy via a User-Defined Next Hop: Example

**Note** This option is applicable only to crypto maps.

The preceding example shows that one route has been created to the remote proxy via a user-defined next hop. This next hop should not require a recursive route lookup unless it will recurse to a default route.

```
reverse-route remote-peer 10.4.4.4
```

The preceding example yields the following prior to Cisco IOS Release 12.3(14)T:

```
10.0.0.0/24 via 10.1.1.1 (in the VRF table if VRFs are configured)
10.1.1.1/32 via 10.4.4.4 (in the global route table)
```

And this result occurs with RRI enhancements:

```
10.0.0.0/24 via 10.4.4.4 (in the VRF table if VRFs are configured, otherwise in the global
table)
```

## Configuring RRI with Enhancements Added in Cisco IOS Release 12.4(15)T: Examples

The following are examples of configurations and output for RRI enhancements that were added in Cisco IOS Release 12.4(15)T.

- [Configuring a RRI Distance Metric Under a Crypto Map: Example, page 12](#)
- [Configuring RRI with Route Tags: Example, page 11](#)
- [debug and show Command Output for a RRI Distance Metric Configuration Under a Crypto Map: Example, page 13](#)
- [Configuring a RRI Distance Metric for a VTI: Example, page 14](#)
- [debug and show Command Output for a RRI Metric Configuration Having a VTI: Example, page 14](#)
- [show crypto route Command Output: Example, page 15](#)

## Configuring a RRI Distance Metric Under a Crypto Map: Example

The following configuration shows a server and client configuration for which a RRI distance metric has been set under a crypto map:

### Server

```
crypto dynamic-map mymap
 set security-association lifetime seconds 300
 set transform-set 3dessa
 set isakmp-profile profile1
 set reverse-route distance 20
 reverse-route
```

### Client

```
crypto ipsec client ezvpn ez
 connect auto
 group cisco key cisco
```

```

mode client
peer 10.0.0.119
username XXX password XXX
xauth userid mode local

```

## Configuring RRI with Route Tags: Example

The following example shows how RRI-created routes can be tagged with a tag number and then used by a routing process to redistribute those tagged routes via a route map:

```

crypto dynamic-map ospf-clients 1
 set reverse-route tag 5

router ospf 109
 redistribute rip route-map rip-to-ospf

route-map rip-to-ospf permit
 match tag 5
 set metric 5
 set metric-type type1

Router# show ip ospf topology

P 10.81.7.48/29, 1 successors, FD is 2588160, tag is 5
 via 192.168.82.25 (2588160/2585600), FastEthernet0/1

```

## debug and show Command Output for a RRI Distance Metric Configuration Under a Crypto Map: Example

The following are **debug** and **show** command output for a RRI distance metric configuration under a crypto map on a server:

```

Router# debug crypto ipsec

00:23:37: IPSEC(validate_proposal_request): proposal part #1,
 (key eng. msg.) INBOUND local= 10.0.0.119, remote= 10.0.0.14,
 local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
 remote_proxy= 192.168.6.1/255.255.255.255/0/0 (type=1),
 protocol= ESP, transform= esp-3des esp-sha-hmac (Tunnel),
 lifedur= 0s and 0kb,
 spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
00:23:37: IPSEC(key_engine): got a queue event with 1 KMI message(s)
00:23:37: IPSEC(rte_mgr): VPN Route Event create routes for peer or rekeying for
 10.0.0.128
00:23:37: IPSEC(rte_mgr): VPN Route Refcount 1 FastEthernet0/0
00:23:37: IPSEC(rte_mgr): VPN Route Added 192.168.6.1 255.255.255.255 via 10.0.0.14 in IP
 DEFAULT TABLE with tag 0 distance 20
00:23:37: IPSEC(policy_db_add_ident): src 0.0.0.0, dest 192.168.6.1, dest_port 0

Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.0.0.14 to network 0.0.0.0

```

```

C 192.200.200.0/24 is directly connected, Loopback0
 10.20.20.20/24 is subnetted, 1 subnets
C 10.30.30.30 is directly connected, Loopback4
C 192.168.5.0/24 is directly connected, Loopback3
 10.20.20.20/24 is subnetted, 2 subnets
S 10.3.1.0 [1/0] via 10.0.0.113
C 10.20.20.20 is directly connected, FastEthernet0/0
 192.168.6.0/32 is subnetted, 1 subnets
S 192.168.6.1 [20/0] via 10.0.0.14
C 192.168.3.0/24 is directly connected, Loopback2
 10.15.0.0/24 is subnetted, 1 subnets
C 10.15.0.0 is directly connected, Loopback6
S* 0.0.0.0/0 [1/0] via 10.0.0.14

```

## Configuring a RRI Distance Metric for a VTI: Example

The following configuration shows a server and client configuration in which a RRI distance metric has been set for a VTI:

### Server Configuration

```

crypto isakmp profile profile1
 keyring mykeyring
 match identity group cisco
 client authentication list authenlist
 isakmp authorization list autholist
 client configuration address respond
 virtual-template 1
crypto ipsec profile vi
 set transform-set 3dessa
 set reverse-route distance 20
 set isakmp-profile profile1
!
interface Virtual-Template1 type tunnel
 ip unnumbered
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi

```

### Client Configuration

```

crypto ipsec client ezvpn ez
 connect auto
 group cisco key cisco
 mode client
 peer 10.0.0.119
 username XXX password XXX
 virtual-interface 1

```

## debug and show Command Output for a RRI Metric Configuration Having a VTI: Example

The following are **debug** and **show** command output for a RRI metric configuration for a VTI on a server:

```

Router# debug crypto ipsec

00:47:56: IPSEC(key_engine): got a queue event with 1 KMI message(s)
00:47:56: Crypto mapdb : proxy_match
 src addr : 0.0.0.0
 dst addr : 192.168.6.1
 protocol : 0
 src port : 0

```

```

dst port : 0
00:47:56: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with the same proxies and peer 10.0.0.14
00:47:56: IPSEC(rte_mgr): VPN Route Event create routes for peer or rekeying for 10.0.0.14
00:47:56: IPSEC(rte_mgr): VPN Route Refcount 1 Virtual-Access2
00:47:56: IPSEC(rte_mgr): VPN Route Added 192.168.6.1 255.255.255.255 via Virtual-Access2 in IP DEFAULT TABLE with tag 0 distance 20
00:47:56: IPSEC(policy_db_add_ident): src 0.0.0.0, dest 192.168.6.1, dest_port 0

00:47:56: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.0.0.110, sa_proto= 50,
sa_spi= 0x19E1175C(434181980),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 87
00:47:56: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.0.0.14, sa_proto= 50,
sa_spi= 0xADC90C5(182227141),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 88
00:47:56: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, changed state to up
00:47:56: IPSEC(key_engine): got a queue event with 1 KMI message(s)
00:47:56: IPSEC(key_engine_enable_outbound): rec'd enable notify from ISAKMP
00:47:56: IPSEC(key_engine_enable_outbound): enable SA with spi 182227141/50
00:47:56: IPSEC(update_current_outbound_sa): updated peer 10.0.0.14 current outbound sa to SPI ADC90C5

```

Router# **show ip route**

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

```

Gateway of last resort is 10.0.0.14 to network 0.0.0.0

```

C 192.200.200.0/24 is directly connected, Loopback0
 10.20.20.20/24 is subnetted, 1 subnets
C 10.30.30.30 is directly connected, Loopback4
C 192.168.5.0/24 is directly connected, Loopback3
 10.20.20.20/24 is subnetted, 2 subnets
S 10.3.1.0 [1/0] via 10.0.0.113
C 10.20.20.20 is directly connected, FastEthernet0/0
 192.168.6.0/32 is subnetted, 1 subnets
S 192.168.6.1 [20/0] via 0.0.0.0, Virtual-Access2
C 192.168.3.0/24 is directly connected, Loopback2
 10.15.0.0/24 is subnetted, 1 subnets
C 10.15.0.0 is directly connected, Loopback6
S* 0.0.0.0/0 [1/0] via 10.0.0.14

```

## show crypto route Command Output: Example

The following output example displays routes, in one table, that are created through IPsec via RRI or Easy VPN VTIs:

Router# **show crypto route**

```

VPN Routing Table: Shows RRI and VTI created routes
Codes: RRI - Reverse-Route, VTI- Virtual Tunnel Interface
S - Static Map ACLs

```

```

Routes created in table GLOBAL DEFAULT
192.168.6.2/255.255.255.255 [0/0] via 10.0.0.133
 on Virtual-Access3 RRI
10.1.1.0/255.255.255.0 [10/0] via Virtual-Access2 VTI
192.168.6.1/255.255.255.255 [0/0] via Virtual-Access2 VTI

```

## Additional References

The following sections provide references related to Reverse Route Injection enhancements.

### Related Documents

| Related Topic               | Document Title                                                       |
|-----------------------------|----------------------------------------------------------------------|
| Cisco IOS Security commands | <a href="#">Cisco IOS Security Command Reference</a> , Release 12.4T |
| Other Cisco IOS commands    | <a href="#">Cisco IOS Command Reference</a> , Release 12.4T          |

### Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

### MIBs

| MIBs | MIBs Link                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

### RFCs

| RFCs | Title |
|------|-------|
| None | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

## Command Reference

The following commands are introduced or modified in the feature or features

- **reverse-route**
- **set reverse-route**
- **show crypto route**

For information about these commands, see the Cisco IOS Security Command Reference at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

# Feature Information for Reverse Route Injection

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for Reverse Route Injection

| Feature Name                      | Releases                          | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reverse Route Injection           | 12.1(9)E<br>12.2(8)T<br>12.2(8)YE | <p>Reverse route injection (RRI) is the ability for static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint. These protected hosts and networks are known as remote proxy identities.</p> <p>Each route is created on the basis of the remote proxy network and mask, with the next hop to this network being the remote tunnel endpoint. By using the remote Virtual Private Network (VPN) router as the next hop, the traffic is forced through the crypto process to be encrypted.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>“Reverse Route Injection” section on page 2</li> </ul> <p>The following commands were introduced or modified by this feature: <b>reverse-route</b>.</p> |
| Reverse Route Remote Peer Options | 12.2(13)T<br>12.2(14)S            | <p>An enhancement was added to RRI to allow you to specify an interface or address as the explicit next hop to the remote VPN device. This functionality allows the overriding of a default route to properly direct outgoing encrypted packets.</p> <p>The following sections provide information about the remote peer options:</p> <ul style="list-style-type: none"> <li>“Enhancements to Reverse Route Injection in Cisco IOS Release 12.4(15)T” section on page 3.</li> </ul>                                                                                                                                                                                                                                                                                                                                                           |



**Table 1**      **Feature Information for Reverse Route Injection (continued)**

| Feature Name                         | Releases                                | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reverse Route Injection Enhancements | 12.3(14)T<br>12.2(33)SRA<br>12.2(33)SXH | <p>The following enhancements were added to the Reverse Route Injection feature:</p> <ul style="list-style-type: none"> <li>• The default behavior of static crypto maps will be the same as that of dynamic crypto maps unless the <b>reverse-route</b> command and <b>static</b> keyword are used.</li> <li>• A route tag value was added for any routes that are created using RRI.</li> <li>• RRI can be configured on the same crypto map that is applied to multiple router interfaces.</li> <li>• RRI configured with the <b>reverse-route remote-peer {ip-address}</b> command, keyword, and argument will create one route instead of two.</li> </ul> <p>The following sections provide information about the Reverse Route Injection enhancements:</p> <ul style="list-style-type: none"> <li>• <a href="#">“Reverse Route Injection” section on page 2</a></li> <li>• <a href="#">“Configuring RRI on Crypto Maps for Cisco IOS Releases Prior to 12.4(15)T” section on page 4</a></li> <li>• <a href="#">“Configuring RRI with Enhancements Added in Cisco IOS Release 12.4(15)T” section on page 6</a></li> <li>• <a href="#">“Configuring RRI When Crypto ACLs Exist: Example” section on page 10</a></li> <li>• <a href="#">“Configuring RRI with Route Tags: Example” section on page 11</a></li> <li>• <a href="#">“Configuring RRI for One Route to the Remote Proxy via a User-Defined Next Hop: Example” section on page 12</a></li> </ul> <p>The following command was modified by these feature enhancements: <b>reverse-route</b>.</p> |
| Gateway Option                       | 12.4(15)T                               | <p>This option allows you to configure unique next hops or gateways for remote tunnel endpoints.</p> <p>The following section provides information about the Gateway Option:</p> <ul style="list-style-type: none"> <li>• <a href="#">“Gateway Option” section on page 3</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

**Table 1**      **Feature Information for Reverse Route Injection (continued)**

| Feature Name                      | Releases                 | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RRI Distance Metric               | 12.4(15)T                | <p>This enhancement allows you to define a metric distance for each static route.</p> <p>The following sections provide information about the RRI distance metric enhancement.</p> <ul style="list-style-type: none"> <li>• “RRI Distance Metric” section on page 3</li> <li>• “Configuring a RRI Distance Metric Under an IPsec Profile” section on page 8</li> <li>• “Configuring a RRI Distance Metric Under a Crypto Map: Example” section on page 12</li> <li>• “debug and show Command Output for a RRI Metric Configuration Having a VTI: Example” section on page 14</li> </ul> <p>The following commands were introduced or modified by this feature: <b>reverse-route</b>, <b>set reverse-route</b>.</p> |
| <b>show crypto route</b> Command  | 12.4(15)T                | This command displays routes that are created through IPsec via RRI or Easy VPN VTIs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Support for RRI on IPsec Profiles | 12.4(15)T                | <p>This feature provides support for relevant RRI options on IPsec profiles that are predominantly used by VTIs.</p> <p>The following section provides information about the Support for RRI on IPsec Profiles feature:</p> <ul style="list-style-type: none"> <li>• “Support for RRI on IPsec Profiles” section on page 4</li> </ul>                                                                                                                                                                                                                                                                                                                                                                              |
| Tag Option Configuration Changes  | 12.4(15)T                | <p>The tag option is now supported with IPsec profiles under the <b>set reverse-route tag</b> command.</p> <p>The following section provides information about this feature enhancement:</p> <ul style="list-style-type: none"> <li>• “Tag Option Configuration Changes” section on page 4</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                              |
| Reverse Route Injection (RRI)     | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





# SafeNet IPSec VPN Client Support

---

The SafeNet IPSec VPN Client Support feature allows you to limit the scope of an Internet Security Association and Key Management Protocol (ISAKMP) profile or ISAKMP keyring configuration to a local termination address or interface. The benefit of this feature is that different customers can use the same peer identities and ISAKMP keys by using different local termination addresses.

## History for the SafeNet IPSec VPN Client Support Feature

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.3(14)T   | This feature was introduced.                                    |
| 12.2(18)SXE | This feature was integrated into Cisco IOS Release 12.2(18)SXE. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for SafeNet IPSec VPN Client Support, page 2](#)  
[Restrictions for SafeNet IPSec VPN Client Support, page 2](#)  
[Information About SafeNet IPSec VPN Client Support, page 2](#)  
[How to Configure SafeNet IPSec VPN Client Support, page 3](#)  
[Configuration Examples for SafeNet IPSec VPN Client Support, page 7](#)  
[Additional References, page 8](#)  
[Command Reference, page 9](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

# Prerequisites for SafeNet IPSec VPN Client Support

- 

# Restrictions for SafeNet IPSec VPN Client Support

- 
- 
- 

# Information About SafeNet IPSec VPN Client Support

Before configuring SafeNet IPSec VPN Client Support, you should understand the following concepts:

- [ISAKMP Profile and ISAKMP Keyring Configurations: Background, page 2](#)
- [Local Termination Address or Interface, page 2](#)

## ISAKMP Profile and ISAKMP Keyring Configurations: Background

Prior to Cisco IOS Release 12.3(14)T, ISAKMP-profile and ISAKMP-keyring configurations could be only global, meaning that the scope of these configurations could not be limited by any locally defined parameters (VRF instances were an exception). For example, if an ISAKMP keyring contained a preshared key for address 10.11.12.13, the same key would be used if the peer had the address 10.11.12.13, irrespective of the interface or local address to which the peer was connected. There are situations, however, in which users prefer that associate keyrings be bound not only with virtual route forwarding (VRF) instances but also to a particular interface. For example, if instead of VRF instances, there are virtual LANS, and the Internet Key Exchange (IKE) is negotiated with a group of peers using one fixed virtual LAN (VLAN) interface. Such a group of peers uses a single preshared key, so if keyrings could be bound to an interface, it would be easy to define a wildcard key without risking that the keys would also be used for other customers.

Sometimes the identities of the peer are not in the control of the administrator, and even if the same peer negotiates for different customers, the local termination address is the only way to distinguish the peer. After such a distinction is made, if the traffic is sent to different VRF instances, configuring an ISAKMP profile is the only way to distinguish the peer. Unfortunately, when the peer uses an identical identity for all such situations, the ISAKMP profile cannot distinguish among the negotiations. For such scenarios, it would be beneficial to bind ISAKMP profiles to a local termination address. If a local termination address could be assigned, identical identities from the peer would not be a problem.

## Local Termination Address or Interface

## Benefit of SafeNet IPSec VPN Client Support

## How to Configure SafeNet IPSec VPN Client Support

- 
- 
- 
- [Examples, page 6](#) (optional)

To configure an ISAKMP profile and limit it to a local termination address or interface, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp profile** *profile-name*
4. *keyring-name*
5. **match identity address** *address*
6. **local-address** { *interface-name* | *ip-address* [*vrf-tag*] }

### DETAILED STEPS

|        | Command or Action                 | Purpose |
|--------|-----------------------------------|---------|
| Step 1 | <b>enable</b>                     |         |
|        | <b>Example:</b><br>Router> enable |         |
|        | <b>configure terminal</b>         |         |
|        | Router# configure terminal        |         |

|                                                                                         |                                                                         |
|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| <b>crypto isakmp profile</b> <i>profile-name</i>                                        | Defines an ISAKMP profile and enters ISAKMP profile configuration mode. |
| Router (config)# crypto isakmp profile profile1<br><i>keyring-name</i>                  |                                                                         |
| Router (conf-isa-profile)# keyring keyring1                                             |                                                                         |
| <b>match identity address</b> <i>address</i>                                            |                                                                         |
| Router (conf-isa-profile)# match identity<br>address 10.0.0.0 255.0.0.0                 |                                                                         |
| <b>local-address</b> { <i>interface-name</i>   <i>ip-address</i><br>[ <i>vrf-tag</i> ]} |                                                                         |
| Router (conf-isa-profile)# local-address<br>serial2/0                                   |                                                                         |



|  |  |
|--|--|
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**show**

- enable**
- debug crypto isakmp**
- show crypto isakmp profile**

## DETAILED STEPS

|                                    |  |
|------------------------------------|--|
|                                    |  |
| Router> enable                     |  |
| Router# debug crypto isakmp        |  |
| <b>show crypto isakmp profile</b>  |  |
| Router# show crypto isakmp profile |  |

## Examples

### debug crypto isakmp Command Output for an ISAKMP Keyring That Is Bound to Local Termination Addresses: Example

```
! Scope of the keyring is limited to interface serial2/0.
local-address serial2/0
! The following is the key string used by the peer.
pre-shared-key address 10.0.0.3 key somerandomkeystring
crypto keyring keyring2
local-address serial2/1
! The following is the keystring used by the peer coming into serial2/1.
pre-shared-key address 10.0.0.3 key someotherkeystring
```

Router#

```
*Feb 11 15:01:29.595: ISAKMP:(0:0:N/A:0):Keyring keyring2 is bound to
10.0.0.0, skipping
*Feb 11 15:01:29.595: ISAKMP:(0:0:N/A:0):Looking for a matching key for
10.0.0.3 in keyring1
*Feb 11 15:01:29.595: ISAKMP:(0:0:N/A:0): : success
*Feb 11 15:01:29.595: ISAKMP:(0:0:N/A:0):found peer pre-shared key
matching 10.0.0.3
*Feb 11 15:01:29.595: ISAKMP:(0:0:N/A:0): local preshared key found
```

```
crypto isakmp profile profile1
```

```
self-identity fqdn
match identity address 10.0.0.1 255.255.255.255
local-address serial2/1
```

```
Router# debug crypto isakmp
```

```
*Feb 11 15:01:29.935: ISAKMP:(0:1:SW:1):: peer matches profile1 profile
```

### show crypto isakmp profile Command Output: Example

```
ISAKMP PROFILE profile1
Identities matched are:
 ip-address 10.0.0.0 255.0.0.0
Certificate maps matched are:
keyring(s): keyring1
trustpoint(s): <all>
Interface binding: serial2/0 (10.20.0.1:global)
```

## Troubleshooting SafeNet IPSec VPN Client Support

## Configuration Examples for SafeNet IPSec VPN Client Support

- 
- 
- 
-

## ISAKMP Profile Bound to a Local Interface: Example

## ISAKMP Keyring Bound to a Local Interface: Example

## ISAKMP Keyring Bound to a Local IP Address: Example

## ISAKMP Keyring Bound to an IP Address and Limited to a VRF: Example

```
ip vrf examplevrf1
 rd 12:3456
crypto keyring ring1
 local-address 10.34.35.36 examplevrf1
interface ethernet2/0
 ip vrf forwarding examplevrf1
 ip address 10.34.35.36 255.255.0.0
```

## Additional References

## Related Documents

| Related Topic | Document Title                                                      |
|---------------|---------------------------------------------------------------------|
|               | <a href="#">VRF-Aware IPSec</a>                                     |
|               | <a href="#">Cisco IOS Security Command Reference, Release 12.3T</a> |

## Standards

| Standard | Title |
|----------|-------|
|          | —     |

## MIBs

| MIB | MIBs Link |
|-----|-----------|
|     |           |

## RFCs

| RFC | Title |
|-----|-------|
|     | —     |

## Technical Assistance

| Description | Link |
|-------------|------|
|             |      |

## Command Reference

- `local-address`

[http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at

<http://tools.cisco.com/Support/CLILookup> or the Master Command List.

---

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



# Stateful Failover for IPSec

---

Stateful failover for IP Security (IPSec) enables a router to continue processing and forwarding IPSec packets after a planned or unplanned outage occurs. Customers employ a backup (secondary) router that automatically takes over the tasks of the active (primary) router if the active router loses connectivity for any reason. This process is transparent to the user and does not require adjustment or reconfiguration of any remote peer.

Stateful failover for IPSec is designed to work in conjunction with stateful switchover (SSO) and Hot Standby Routing Protocol (HSRP). HSRP provides network redundancy for IP networks, ensuring that user traffic immediately and transparently recovers from failures in network edge devices or access circuits. That is, HSRP monitors both the inside and outside interfaces so that if either interface goes down, the whole router is deemed to be down and ownership of Internet Key Exchange (IKE) and IPSec security associations (SAs) is passed to the standby router (which transitions to the HSRP active state). SSO allows the active and standby routers to share IKE and IPSec state information so that each router has enough information to become the active router at any time. To configure stateful failover for IPSec, a network administrator should enable HSRP, assign a virtual IP address, and enable the SSO protocol.

## Feature History for Stateful Failover for IPSec

| Release   | Modification                 |
|-----------|------------------------------|
| 12.3(11)T | This feature was introduced. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for Stateful Failover for IPSec, page 2](#)
- [Restrictions for Stateful Failover for IPSec, page 2](#)
- [Information About Stateful Failover for IPSec, page 3](#)
- [How to Use Stateful Failover for IPSec, page 6](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

- [Configuration Examples for Stateful Failover, page 27](#)
- [Additional References, page 36](#)
- [Command Reference, page 37](#)

## Prerequisites for Stateful Failover for IPSec

### Complete, Duplicate IPSec and IKE Configuration on the Active and Standby Devices

This document assumes that you have a complete IKE and IPSec configuration. (This document describes only how to add stateful failover to a working IPSec configuration.)

The IKE and IPSec configuration that is set up on the active device must be duplicated on the standby device. That is, the crypto configuration must be identical with respect to Internet Security Association and Key Management Protocol (ISAKMP) policy, ISAKMP keys (preshared), IPSec profiles, IPSec transform sets, all crypto map sets that are used for stateful failover, all access control lists (ACLs) that are used in match address statements on the crypto map sets, all AAA configurations used for crypto, client configuration groups, ip local pools used for crypto, and ISAKMP profiles.



#### Note

None of the configuration information between the active and standby device is automatically transferred; the user is responsible for ensuring that the crypto configurations match on both devices. If the crypto configurations on both devices do not match, failover from the active device to the standby device will not be successful.

### Device Requirements

- Stateful failover for IPSec requires that your network contains two identical routers that are available to be either the primary or secondary device. Both routers should be the same type of device, have the same CPU and memory, and have either no encryption accelerator or identical encryption accelerators.
- This feature is currently supported only on a limited number of platforms. To check the latest platform support, go to Cisco Feature Navigator at <http://www.cisco.com/go/fn>.

## Restrictions for Stateful Failover for IPSec

When configuring redundancy for a virtual private network (VPN), the following restrictions exist:

- Both the active and standby devices must run the identical version of the Cisco IOS software, and both the active and standby devices must be connected via hub or switch.
- Only the VPN Acceleration Module (VAM), VAM2, and AIM-VPN/HPII+ hardware encryption accelerators are supported in a Cisco 3845 router, and the AIM-VPN/EPII+ hardware encryption accelerators are supported in a Cisco 3825 router.
- Only “box-to-box” failover is supported; that is, intrachassis failover is currently not supported.
- WAN interfaces between the active (primary) router and the standby (secondary) router are not supported. (HSRP requires inside interfaces and outside interfaces to be connected via LANs.)
- Load balancing is not supported; that is, no more than one device in a redundancy group can be active at any given time.
- Stateful failover of IPSec with Layer 2 Tunneling Protocol (L2TP) is not supported.



- Public key infrastructure (PKI) is not supported when used with stateful failover. (Only preshared keys for IKE are supported.)
- IKE keepalives are not supported. (Enabling this functionality will cause the connection to be torn down after the standby router assumes ownership control.) However, dead peer detection (DPD) and periodic DPD are supported.
- IPSec idle timers are not supported when used with stateful failover.
- A stateful failover crypto map applied to an interface in a virtual route forwarding (VRF) instance is not supported. However, VRF-aware IPSec features are supported when a stateful failover crypto map is applied to an interface in the global VRF.
- Stateful failover is not compatible or interoperable with the State Synchronization Protocol (SSP) version of stateful failover (which is available in Cisco IOS Release 12.2YX1 and Cisco IOS Release 12.2SU).

## Information About Stateful Failover for IPSec

To configure stateful failover for VPNs, you should understand the following concepts:

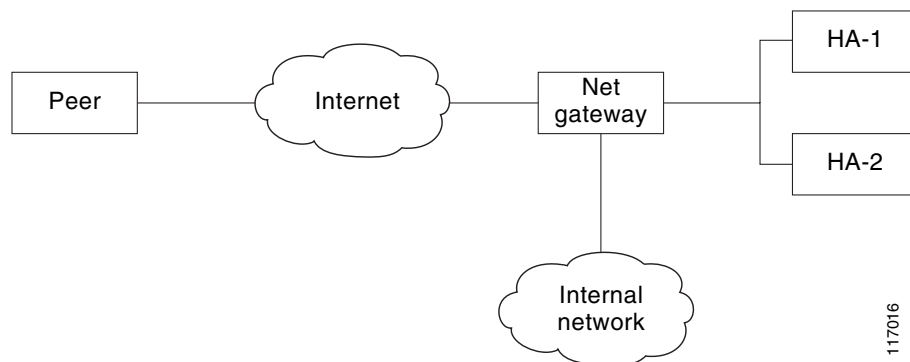
- [Supported Deployment Scenarios: Stateful Failover for IPSec, page 3](#)
- [IPSec Stateful Failover for Remote Access Connections, page 5](#)
- [Dead Peer Detection with IPSec High Availability, page 6](#)

## Supported Deployment Scenarios: Stateful Failover for IPSec

It is recommended that you implement IPSec stateful failover in one of the following recommended deployment scenarios—a single interface scenario or a dual interface scenario.

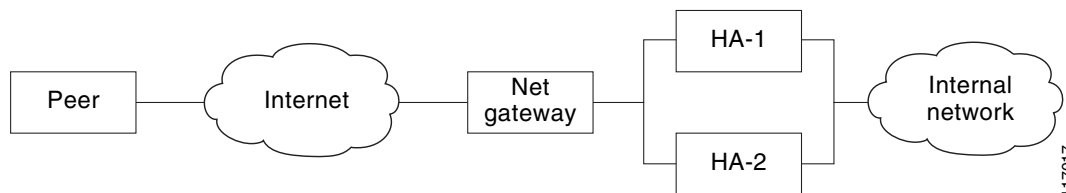
In a single interface scenario, the VPN gateways use one LAN connection for both encrypted traffic arriving from remote peers and decrypted traffic flowing to inside hosts (see [Figure 1](#)). The single interface design allows customers to save money on router ports and subnets. This design is typically used if all traffic flowing in and out of the organization does not traverse the VPN routers.

**Figure 93**      **Single Interface Network Topology**



In a dual interface scenario, a VPN gateway has more than one interface, enabling traffic to flow in and out of the router via separate interfaces (see [Figure 2](#)). This scenario is typically used if traffic flowing in and out of a site must traverse the routers, so the VPN routers will provide the default route out of the network.

**Figure 94 Dual Interface Network Topology**



[Table 1](#) lists the functionality available in both a single interface scenario and a dual interfaces scenario.

**Table 55 IPSec StateFul Failover: Single and Dual Interface Functionality Overview**

| Single Interface                                                                                                                                                                                                                                           | Dual Interface                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Route Injection</b>                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Routes must be injected to provide the devices that are behind the VPN gateways with a next hop for traffic that requires encryption. Stateful failover for IPSec typically requires routes to be injected for this network topology.                      | <p>If the VPN gateways are not the logical next hop for devices inside the network, the routes must be created and injected into the routing process. Thus, traffic that is returning from inside the network can be sent back to the VPN routers for IPSec services before it is sent out. A virtual IP (VIP) address cannot be used as the advertiser of routing updates, so flows must be synchronized via the injected routes.</p> <p>If the VPN gateways are the next hop (default route) for all devices inside the network, the VIP address that is used on the inside interfaces can be used as the next hop. Thus, injection of the VPN routes is not required. However, static routes on inside hosts must be used to direct the routes to the next hop VIP address.</p> |
| <b>HSRP Configuration</b>                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| The role of HSRP is simplified in a single interface design because if the only interface is disabled, the entire device is deemed unavailable. This functionality helps to avoid some of the routing considerations to be discussed in the next scenario. | <p>Because each interface pair functions independently, you should configure HSRP so that multiple pairs of interfaces can be tracked. (That is, HSRP should not be configured on only one pair of interfaces or on both pairs of interfaces without each pair mutually tracking each other.) Mutual tracking means that if the outside interface does fail, the inside interface on the same router will also be deemed down, allowing for complete router failover to the secondary router.</p>                                                                                                                                                                                                                                                                                  |
| <b>Secure State Information</b>                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

**Table 55** *IPSec Stateful Failover: Single and Dual Interface Functionality Overview (continued)*

| Single Interface                                                                                                                | Dual Interface                                                                                                                                                 |
|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| If secured-state information is passed between routers, the information is passed over the same interface as all other traffic. | The router has a separate inside and outside interface; thus, the inside interface can be used as a more secure channel for the exchange of state information. |
| Firewall Configuration                                                                                                          |                                                                                                                                                                |
| The VPN gateways can sit in front of the firewall or behind the firewall.                                                       | VPN gateways may sit behind or in front of a firewall, a firewall can be installed in parallel to the VPN gateways.                                            |

## IPSec Stateful Failover for Remote Access Connections

The main difference between a remote access and a LAN-to-LAN connection is the use of Xauth and mode-config. IKE Xauth is often used to authenticate the user. IKE mode-config is often used to push security policy from the hub (concentrator) router to the user's IPSec implementation. Mode-config is also typically used to assign an internal company network IP address to a user.

In addition to the differences between a remote access configuration and a LAN-to-LAN configuration, you should note the following remote-access-server-specific functions:

- Assigned IP address—The IP address can be assigned to the client via one of the following options:
  - Local IP pools. For local IP pools, the administrator must first configure identical local IP address pools on each router in the high availability (HA) pair (via the **ip local pool client-address-pool** command). This pool name can be applied in one of two places—in a group policy via the **crypto isakmp client configuration group group-name** (and the submode command **pool pool-name**) or in a client configuration via the **crypto isakmp client configuration address-pool local local-pool** command.
  - RADIUS-assigned address. If you are using RADIUS authentication and the RADIUS server returns the Framed-IP-Address attribute, the concentrator will always assign that address to the client. It is recommended that you refer to your RADIUS server vendor's documentation, especially for vendors that allow you to configure address pools on the RADIUS server. Typically those servers require crypto accounting to work properly.

To enable accounting on the HA pair, you should issue the following commands on both Active and Standby devices: **aaa accounting network radius-accounting start-stop group radius** then apply radius-accounting either to the crypto isakmp profile or the crypto map set.

- RADIUS NAS-IP address—The HA pair should appear as a single device to the RADIUS server. Thus, both HA routers must communicate with the RADIUS server using the same IP address. However, when communicating with the RADIUS server, the router must use a physical IP address, not a virtual IP (VIP) address as the NAS-IP address of the router. To configure the RADIUS NAS-IP address for the HA pair, you must configure the same loopback address in the HA pair via **interface loopback ip address** command; thereafter, you must issue the **ip radius source-interface loopback** command in the HA pair. Finally, add the new loopback IP address to the RADIUS servers configuration so the RADIUS server can process requests from the HA pair.

For additional information on how to configure IPSec stateful failover for a remote access connection, see the section [“Configuring IPSec Stateful Failover for an Easy VPN Server: Example”](#) in this document.

## Dead Peer Detection with IPsec High Availability

To configure Dead Peer Detection (DPD) with IPsec High Availability (HA), it is recommended that you use a value other than the default (2 seconds). A keepalive time of 10 seconds with 5 retries seems to work well with HA because of the time it takes for the router to get into active mode.

To configure DPD with IPsec HA, use the **crypto isakmp keepalive** command.

## How to Use Stateful Failover for IPsec

This section contains the following the procedures:

- [Enabling HSRP: IP Redundancy and a Virtual IP Address, page 6](#) (required)
- [Enabling SSO, page 9](#) (required)
- [Configuring Reverse Route Injection on a Crypto Map, page 13](#) (required)
- [Enabling Stateful Failover for IKE and IPsec, page 15](#) (required)
- [Protecting SSO Traffic, page 18](#) (optional)
- [Managing and Verifying High Availability Information, page 20](#) (optional)

## Enabling HSRP: IP Redundancy and a Virtual IP Address

HSRP provides two services—IP redundancy and a VIP address. Each HSRP group may provide either or both of these services. IPsec stateful failover uses the IP redundancy services from only one HSRP standby group. It can use the VIP address from one or more HSRP groups. Use the following task to configure HSRP on the outside and inside interfaces of the router.

**Note**

---

Perform this task on both routers (active and standby) and of both interfaces on each router.

---

## Prerequisites for Spanning Tree Protocol and HSRP Stability

If a switch connects the active and standby routers, you must perform one of the following steps to ensure that the correct settings are configured on that switch:

- Enable the **spanning-tree portfast** command on every switch port that connects to a HSRP-enabled router interface.
- Disable the Spanning Tree Protocol (STP) on the switch only if your switch does not connect to other switches. Disabling spanning tree in a multi-switch environment may cause network instability.
- Enable the **standby delay minimum** *[min-delay]* **reload** *[reload-delay]* command if you do not have access to the switch. The *reload-delay* argument should be set to a value of at least 120 seconds. This command must be applied to all HSRP interfaces on both routers.

For more information on HSRP instability, see the document [Avoiding HSRP Instability in a Switching Environment with Various Router Platforms](#).

**Note**

---

You must perform at least one of these steps for correct HSRP operation.

---

## Restrictions

- Both the inside (private) interface and the outside (public) interface must belong to separate HSRP groups, but the HSRP group number can be the same.
- The state of the inside interface and the outside interface must be the same—both interfaces must be in the active state or standby state; otherwise, the packets will not have a route out of the private network.
- Standby priorities should be equal on both active and standby routers. If the priorities are not equal, the higher priority router will unnecessarily take over as the active router, negatively affecting uptime.
- The IP addresses on the HSRP-tracked interfaces of the standby and active routers should both be either lower or higher on one router than the other. In the case of equal priorities (an HA requirement), HSRP will assign the active state on the basis of the IP address. If an addressing scheme exists so that the public IP address of Router A is lower than the public IP address of Router B, but the opposite is true for their private interfaces, an active/standby-standby/active split condition could exist which will break connectivity.

**Note**

Each time an active device relinquishes control to become the standby device, the active device will reload. This functionality ensures that the state of the new standby device synchronizes correctly with the new active device.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **standby** *standby-group-number* **name** *standby-group-name*
5. **standby** *standby-group-number* **ip** *ip-address*
6. **standby** *standby-group-number* **track** *interface-name*
7. **standby** [*group-number*] **preempt**
8. **standby** [*group-number*] **timers** [*msec*] *hellotime* [*msec*] *holdtime*
9. **standby delay minimum** [*min-delay*] **reload** [*reload-delay*]
10. Repeat.

## DETAILED STEPS

|        | Command or Action                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                                                                                                                                                                                         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                         | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 3 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface Ethernet 0/0                                                   | Configures an interface type for the router and enters interface configuration mode.                                                                                                                                                                                                                                                                                                                                                     |
| Step 4 | <b>standby</b> <i>standby-group-number</i> <b>name</b> <i>standby-group-name</i><br><br><b>Example:</b><br>Router(config-if)# standby 1 name HA-out    | Assigns a user-defined group name to the HSRP redundancy group.<br><br><b>Note</b> The <i>standby-group-number</i> argument should be the same for both routers that are on directly connected interfaces. However, the <i>standby-group-name</i> argument should be different between two (or more) groups on the same router.<br><br>The <i>standby-group-number</i> argument can be the same on the other pair of interfaces as well. |
| Step 5 | <b>standby</b> <i>standby-group-number</i> <b>ip</b> <i>ip-address</i><br><br><b>Example:</b><br>Router(config-if)# standby 1 ip 209.165.201.1         | Assigns an IP address that is to be “shared” among the members of the HSRP group and owned by the primary IP address.<br><br><b>Note</b> The virtual IP address must be configured identically on both routers (active and standby) that are on directly connected interfaces.                                                                                                                                                           |
| Step 6 | <b>standby</b> <i>standby-group-number</i> <b>track</b> <i>interface-name</i><br><br><b>Example:</b><br>Router(config-if)# standby 1 track Ethernet1/0 | Configures HSRP to monitor the second interface so that if either of the two interfaces goes down, HSRP causes failover to the standby device.<br><br><b>Note</b> Although this command is not required, it is recommended for dual interface configurations.                                                                                                                                                                            |
| Step 7 | <b>standby</b> [ <i>group-number</i> ] <b>preempt</b><br><br><b>Example:</b><br>Router(config-if)# standby 1 preempt                                   | Enables the active device to relinquish control because of an interface tracking event.                                                                                                                                                                                                                                                                                                                                                  |

|         | Command or Action                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 8  | <b>standby</b> [ <i>group-number</i> ] <b>timers</b> [ <i>msec</i> ] <i>hellotime</i> [ <i>msec</i> ] <i>holdtime</i><br><br><b>Example:</b><br>Router(config-if)# standby 1 timers 1 5 | (Optional) Configures the time between hello packets and the time before other routers declare the active Hot Standby or standby router to be down. <ul style="list-style-type: none"> <li><i>holdtime</i>—Amount of time the routers take to detect types of failure. A larger hold time means that failure detection will take longer.</li> </ul> For the best stability, it is recommended that you set the hold time between 5 and 10 times the hello interval time; otherwise, a failover could falsely occur when no actual failure has happened. |
| Step 9  | <b>standby delay minimum</b> [ <i>min-delay</i> ] <b>reload</b> [ <i>reload-delay</i> ]<br><br><b>Example:</b><br>Router(config-if)# standby delay minimum reload 120                   | Configures the delay period before the initialization of HSRP groups. <p><b>Note</b> It is suggested that you enter 120 as the value for the <i>reload-delay</i> argument and leave the <i>min-delay</i> argument at the preconfigured default value.</p>                                                                                                                                                                                                                                                                                               |
| Step 10 | Repeat.                                                                                                                                                                                 | Repeat this task on both routers (active and standby) and on both interfaces of each router.                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## Troubleshooting Tips

To help troubleshoot possible HSRP-related configuration problems, issue any of the following HSRP-related debug commands—**debug standby errors**, **debug standby events**, and **debug standby packets [terse]**.

## Examples

The following example shows how to configure HSRP on a router:

```
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 preempt
 standby 1 name HA-out
 standby 1 track Ethernet1/0
 standby delay reload 120
```

## What to Do Next

After you have successfully configured HSRP on both the inside and outside interfaces, you should enable SSO as described in the section “[Enabling SSO](#).”

## Enabling SSO

Use this task to enable SSO, which is used to transfer IKE and IPSec state information between two routers.

## SSO: Interacting with IPSec and IKE

SSO is a method of providing redundancy and synchronization for many Cisco IOS applications and features. SSO is necessary for IPSec and IKE to learn about the redundancy state of the network and to synchronize their internal application state with their redundant peers.

### Prerequisites

- You should configure HSRP before enabling SSO.
- To avoid losing SCTP communication between peers, be sure to include the following commands to the local address section of the SCTP section of the IPC configuration:
  - **retransmit-timeout** *retran-min [msec] retra-max [msec]*
  - **path-retransmit** *max-path-retries*
  - **assoc-retransmit** *retries*

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **redundancy inter-device**
4. **scheme standby** *standby-group-name*
5. **exit**
6. **ipc zone default**
7. **association 1**
8. **protocol sctp**
9. **local-port** *local-port-number*
10. **local-ip** *device-real-ip-address [device-real-ip-address2]*
11. **retransmit-timeout** *retran-min [msec] retra-max [msec]*
12. **path-retransmit** *max-path-retries*
13. **assoc-retransmit** *retries*
14. **exit**
15. **remote-port** *remote-port-number*
16. **remote-ip** *peer-real-ip-address [peer-real-ip-address2]*



## DETAILED STEPS

|        | Command or Action                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|--------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                           | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 3 | <b>redundancy inter-device</b><br><br><b>Example:</b><br>Router(config)# redundancy inter-device                         | Configures redundancy and enters inter-device configuration mode.<br><br>To exit inter-device configuration mode, use the <b>exit</b> command. To remove all inter-device configuration, use the <b>no</b> form of the command.                                                                                                                                                                                                                                                                                                                                                         |
| Step 4 | <b>scheme standby standby-group-name</b><br><br><b>Example:</b><br>Router(config-red-interdevice)# scheme standby HA-out | Defines the redundancy scheme that is to be used. Currently, “standby” is the only supported scheme. <ul style="list-style-type: none"> <li><i>standby-group-name</i>—Must match the standby name specified in the <b>standby name</b> interface configuration command. Also, the standby name should be the same on both routers.</li> </ul> <b>Note</b> Only the active or standby state of the standby group is used for SSO. The VIP address of the standby group is not required or used by SSO. Also, the standby group does not have to be part of any crypto map configuration. |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-red-interdevice)# exit                                               | Exits inter-device configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 6 | <b>ipc zone default</b><br><br><b>Example:</b><br>Router(config)# ipc zone default                                       | Configures the inter-device communication protocol, Inter-Process Communication (IPC), and enters IPC zone configuration mode.<br><br>Use this command to initiate the communication link between the active router and standby router.                                                                                                                                                                                                                                                                                                                                                 |
| Step 7 | <b>association 1</b><br><br><b>Example:</b><br>Router(config-ipczzone)# association 1                                    | Configures an association between the two devices and enters IPC association configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 8 | <b>protocol sctp</b><br><br><b>Example:</b><br>Router(config-ipczzone-assoc)# protocol sctp                              | Configures Stream Control Transmission Protocol (SCTP) as the transport protocol and enters SCTP protocol configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

|         | Command or Action                                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 9  | <b>local-port</b> <i>local-port-number</i><br><br><b>Example:</b><br>Router(config-ipc-protocol-sctp)# local-port 5000                                                             | Defines the local SCTP port number that is used to communicate with the redundant peer and puts you in IPC transport - SCTP local configuration mode. <ul style="list-style-type: none"> <li><i>local-port-number</i>—There is not a default value. This argument must be configured for the local port to enable inter-device redundancy. Valid port values: 1 to 65535.</li> </ul> <p>The local port number should be the same as the remote port number on the peer router.</p> |
| Step 10 | <b>local-ip</b> <i>device-real-ip-address</i> [ <i>device-real-ip-address2</i> ]<br><br><b>Example:</b><br>Router(config-ipc-local-sctp)# local-ip 10.0.0.1                        | Defines at least one local IP address that is used to communicate with the redundant peer. <p>The local IP addresses must match the remote IP addresses on the peer router. There can be either one or two IP addresses, which must be in the global VRF. A virtual IP address cannot be used.</p>                                                                                                                                                                                 |
| Step 11 | <b>retransmit-timeout</b> <i>retran-min</i> [ <i>msec</i> ] <i>retra-max</i> [ <i>msec</i> ]<br><br><b>Example:</b><br>Router(config-ipc-local-sctp)# retransmit-timeout 300 10000 | Configures the maximum amount of time, in milliseconds, that SCTP will wait before retransmitting data. <ul style="list-style-type: none"> <li><i>retran-min</i>: 300 to 60000; default: 300</li> <li><i>retra-max</i>: 300 to 60000; default: 600</li> </ul>                                                                                                                                                                                                                      |
| Step 12 | <b>path-retransmit</b> <i>max-path-retries</i><br><br><b>Example:</b><br>Router(config-ipc-local-sctp)# path-retransmit 10                                                         | Configures the number of consecutive retransmissions SCTP will perform before failing a path within an association. <ul style="list-style-type: none"> <li><i>max-path-retries</i>: 2 to 10; default: 4 retries</li> </ul>                                                                                                                                                                                                                                                         |
| Step 13 | <b>assoc-retransmit</b> <i>retries</i><br><br><b>Example:</b><br>Router(config-ipc-local-sctp)# assoc-retransmit 10                                                                | Configures the number of consecutive retransmissions SCTP will perform before failing an association. <ul style="list-style-type: none"> <li><i>max-association-retries</i>: 2 to 10; default: 4 retries</li> </ul>                                                                                                                                                                                                                                                                |
| Step 14 | <b>exit</b><br><br><b>Example:</b><br>Router(config-ipc-local-sctp)# exit                                                                                                          | Exits IPC transport - SCTP local configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                               |

|         | Command or Action                                                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 15 | <b>remote-port</b> <i>remote-port-number</i><br><br><b>Example:</b><br>Router(config-ipc-protocol-sctp)# remote-port 5000                                     | Defines the remote SCTP port number that is used to communicate with the redundant peer and puts you in IPC transport - SCTP remote configuration mode.<br><br><b>Note</b> <i>remote-port-number</i> —There is not a default value. This argument must be configured for the remote port to enable inter-device redundancy. Valid port values: 1 to 65535.<br><br>The remote port number should be the same as the local port number on the peer router. |
| Step 16 | <b>remote-ip</b> <i>peer-real-ip-address</i><br>[ <i>peer-real-ip-address2</i> ]<br><br><b>Example:</b><br>Router(config-ipc-remote-sctp)# remote-ip 10.0.0.2 | Defines at least one remote IP address of the redundant peer that is used to communicate with the local device. All remote IP addresses must refer to the same device. A virtual IP address cannot be used.                                                                                                                                                                                                                                              |

## Troubleshooting Tips

To help troubleshoot possible SSO-related configuration problems, issue the **debug redundancy** command.

## Examples

The following example shows how to enable SSO:

```

!
redundancy inter-device
 scheme standby HA-out
!
!
ipc zone default
 association 1
 no shutdown
 protocol sctp
 local-port 5000
 local-ip 10.0.0.1
 retransmit-timeout 300 10000
 path-retransmit 10
 assoc-retransmit 10
 remote-port 5000
 remote-ip 10.0.0.2
!

```

## What to Do Next

After you have enabled SSO, you should configure reverse route injection (RRI) on a crypto map as shown in the following section.

## Configuring Reverse Route Injection on a Crypto Map

You should configure RRI on all existing crypto maps that you want to use with stateful failover. RRI is used with stateful failover so routers on the inside network can learn about the correct path to the current active device. When failover occurs, the new active device injects the RRI routes into its IP routing table and sends out routing updates to its routing peers.

Use one of the following tasks to configure RRI on a dynamic or static crypto map.

- [Configuring RRI on Dynamic Crypto Map, page 13](#)
- [Configuring RRI on a Static Crypto Map, page 14](#)

### Configuring RRI on Dynamic Crypto Map

Dynamic crypto map entries, like regular static crypto map entries, are grouped into sets. A set is a group of dynamic crypto map entries all with the same dynamic map name but each with a different dynamic sequence number. Each member of the set may be configured for RRI.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto dynamic-map** *map-name seq-num*
4. **reverse-route**

#### DETAILED STEPS

|        | Command or Action                                                                                                       | Purpose                                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                  | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                          | Enters global configuration mode.                                                                                     |
| Step 3 | <b>crypto dynamic-map</b> <i>map-name seq-num</i><br><br><b>Example:</b><br>Router(config)# crypto dynamic-map mymap 10 | Creates a dynamic crypto map entry and enters crypto map configuration mode.                                          |
| Step 4 | <b>reverse-route</b><br><br><b>Example:</b><br>Router(config-crypto-map)# reverse-route                                 | Enables RRI for a dynamic crypto map.                                                                                 |

## Configuring RRI on a Static Crypto Map

Static crypto map entries are grouped into sets. A set is a group of static crypto map entries all with the same static map name but each with a different sequence number. Each static crypto map in the map set can be configured for RRI. Use this task to configure RRI on a static crypto map.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map *map-name seq-num* ipsec-isakmp**
4. **reverse-route**

### DETAILED STEPS

|        | Command or Action                                                                                                                           | Purpose                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                      | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                              | Enters global configuration mode.                                                                                     |
| Step 3 | <b>crypto map <i>map-name seq-num</i> ipsec-isakmp</b><br><br><b>Example:</b><br>Router(config)# crypto map to-peer-outside 10 ipsec-isakmp | Enters crypto map configuration mode and creates or modifies a crypto map entry.                                      |
| Step 4 | <b>reverse-route</b><br><br><b>Example:</b><br>Router(config-crypto-map)# reverse-route                                                     | Dynamically creates static routes based on crypto ACLs.                                                               |

## Examples

The following example shows how to configure RRI on the static crypto map “to-peer-outside”:

```
crypto map to-peer-outside redundancy replay-interval inbound 1000 outbound 10000
crypto map to-peer-outside 10 ipsec-isakmp
 set peer 209.165.200.225
 set transform-set trans1
 match address peer-outside
 reverse-route
```

## What to Do Next

After you have configured RRI, you can enable stateful failover for IPSec and IKE.

## Enabling Stateful Failover for IKE and IPSec

Use the following tasks to configure stateful failover for IPSec, IKE, and tunnel protection:

- [Enabling Stateful Failover for IKE, page 15](#)
- [Enabling Stateful Failover for IPSec, page 15](#)
- [Enabling Stateful Failover for Tunnel Protection, page 17](#)

### Enabling Stateful Failover for IKE

There is no specific command-line interface (CLI) necessary to enable stateful failover for IKE. It is enabled for a particular VIP address when a stateful failover crypto map is applied to an interface.

### Enabling Stateful Failover for IPSec

Use this task to enable stateful failover for IPSec. All IPSec state information is transferred from the active router to the standby router via the SSO redundancy channel that was specified in the task “[Enabling SSO](#).”

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **crypto map** *map-name* [**redundancy** *standby-group-name* [**stateful**]]

#### DETAILED STEPS

|        | Command or Action                             | Purpose                                                                                                            |
|--------|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
|        | <b>Example:</b><br>Router> enable             |                                                                                                                    |
| Step 2 | <b>configure terminal</b>                     | Enters global configuration mode.                                                                                  |
|        | <b>Example:</b><br>Router# configure terminal |                                                                                                                    |

|        | Command or Action                                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface Ethernet 0/0                                                                                                    | Defines an interface that has already been configured for redundancy and enters interface configuration mode.                                                                                                                                                                                                                                                                                                  |
| Step 4 | <b>crypto map</b> <i>map-name</i> [ <b>redundancy</b> <i>standby-group-name</i> [ <b>stateful</b> ]]<br><br><b>Example:</b><br>Router(config-if)# crypto map to-peer-outside redundancy HA-out stateful | <p>Binds the crypto map on the specified interface to the redundancy group.</p> <p><b>Note</b> Although the standby group does not have to be the same group that was used when enabling SSO, it does have to be the same group that was used with the <b>standby ip</b> command on this interface.</p> <p>This crypto map will use the same VIP address for both IKE and IPSec to communicate with peers.</p> |

## Troubleshooting Tips

To help troubleshoot possible IPSec HA-related problems, issue the **debug crypto ipsec ha** [detail] [update] command.

## Examples

The following example shows how to configure IPSec stateful failover on the crypto map “to-peer-outside”:

```
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 preempt
 standby 1 name HA-out
 standby 1 track Ethernet1/0
 crypto map to-peer-outside redundancy HA-out stateful
```

## Enabling Stateful Failover for Tunnel Protection

Use an existing IPSec profile to configure stateful failover for tunnels using IPSec. (You do not configure the tunnel interface as you would with a crypto map configuration.)

## Restrictions

The tunnel source address must be a VIP address, and it must not be an interface name.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec profile** *name*
4. **redundancy** *standby-group-name* **stateful**
5. **exit**
6. **interface tunnel** *number*

7. **tunnel protection ipsec profile** *name*
8. **tunnel source** *virtual-ip-address*

## DETAILED STEPS

|        | Command or Action                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                 |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                                                       |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                 | Enters global configuration mode.                                                                                                                                                                                                                                                       |
| Step 3 | <b>crypto ipsec profile</b> <i>name</i><br><br><b>Example:</b><br>Router(config)# crypto ipsec profile<br>peer-profile                         | Defines the IPSec parameters that are to be used for IPSec encryption between two routers and enters crypto map configuration mode.                                                                                                                                                     |
| Step 4 | <b>redundancy</b> <i>standby-group-name</i> <b>stateful</b><br><br><b>Example:</b><br>Router(config-crypto-map)# redundancy HA-out<br>stateful | Configures stateful failover for tunnels using IPSec.                                                                                                                                                                                                                                   |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-crypto-map)# exit                                                                          | Exits crypto map configuration mode.                                                                                                                                                                                                                                                    |
| Step 6 | <b>interface tunnel</b> <i>number</i><br><br><b>Example:</b><br>Router(config)# interface tunnel 5                                             | Configures a tunnel interface and enters interface configuration mode<br><ul style="list-style-type: none"><li><i>number</i>—Specifies the number of the interface that you want to create or configure. There is no limit on the number of tunnel interfaces you can create.</li></ul> |
| Step 7 | <b>tunnel protection ipsec profile</b> <i>name</i><br><br><b>Example:</b><br>Router(config-if)# tunnel protection ipsec<br>profile catprofile  | Associates a tunnel interface with an IPSec profile.<br><i>name</i> —Specifies the name of the IPSec profile; this value must match the name specified in the <b>crypto ipsec profile name</b> command.                                                                                 |
| Step 8 | <b>tunnel source</b> <i>virtual-ip-address</i><br><br><b>Example:</b><br>Router(config-if)# tunnel source 10.1.1.1                             | Sets source address for a tunnel interface.<br><ul style="list-style-type: none"><li><i>virtual-ip-address</i>—Must be a VIP address.</li></ul> <b>Note</b> Do not use the interface name as the tunnel source.                                                                         |

## Examples

The following example shows how to configure stateful failover for tunnel protection:

```
crypto ipsec profile peer-profile
```



```
redundancy HA-out stateful

interface Tunnel1
 ip unnumbered Loopback0
 tunnel source 209.165.201.3
 tunnel destination 10.0.0.5
 tunnel protection ipsec profile peer-profile
!
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 name HA-out
```

## What to Do Next

After you have configured stateful failover, you can use the CLI to protect, verify, and manage your configurations. For more information on completing these tasks, see the sections “[Protecting SSO Traffic](#)” and “[Managing and Verifying High Availability Information](#).”

## Protecting SSO Traffic

Use this task to secure a redundancy group via an IPSec profile. To configure SSO traffic protection, the active and standby devices must be directly connected to each other via Ethernet networks.

The crypto maps that are automatically generated when protecting SSO traffic are applied to each interface, which corresponds to an IP address that was specified via the **local-ip** command. Traffic that is destined for an IP address that was specified via the **remote-ip** command is forced out of the crypto-map-configured interface via an automatically created static host route.



### Note

If you are certain that the SSO traffic between the redundancy group runs on a physically secure interface, you do not have to configure SSO traffic protection.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp key** *keystring* **address** *peer-address*
4. **crypto ipsec transform-set** *transform-set-name* *transform-set-list*
5. **crypto ipsec profile** *profile-name*
6. **set transform-set** *transform-set-name*
7. **exit**
8. **redundancy inter-device**
9. **security ipsec** *profile-name*

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                     | Purpose                                                                                                                                            |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                        | Enters global configuration mode.                                                                                                                  |
| Step 3 | <b>crypto isakmp key</b> <i>keystring</i> <b>address</b> <i>peer-address</i><br><br><b>Example:</b><br>Router(config)# crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0             | Configures a preshared authentication key. <ul style="list-style-type: none"> <li><i>peer-address</i>—The SCTP remote IP address.</li> </ul>       |
| Step 4 | <b>crypto ipsec transform-set</b> <i>transform-set-name</i> <i>transform-set-list</i><br><br><b>Example:</b><br>Router(config)# crypto ipsec transform-set trans2 ah-md5-hmac esp-aes | Configures a transform set that defines the packet format and cryptographic algorithms used for IPSec.                                             |
| Step 5 | <b>crypto ipsec profile</b> <i>profile-name</i><br><br><b>Example:</b><br>Router(config)# crypto ipsec profile sso-secure                                                             | Defines an IPSec profile that describes how the traffic will be protected.                                                                         |
| Step 6 | <b>set transform-set</b> <i>transform-set-name</i><br><br><b>Example:</b><br>Router(config-crypto-map)# set transform-set trans2                                                      | Specifies which transform sets can be used with the IPSec profile.                                                                                 |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(config-crypto-map)# exit                                                                                                                 | Exits crypto map configuration mode.                                                                                                               |
| Step 8 | <b>redundancy inter-device</b><br><br><b>Example:</b><br>Router(config)# redundancy inter-device                                                                                      | Configures redundancy and enters inter-device configuration mode.                                                                                  |
| Step 9 | <b>security ipsec</b> <i>profile-name</i><br><br><b>Example:</b><br>Router(config-red-interdevice)# security ipsec sso-secure                                                         | Applies the IPSec profile to the redundancy group communications, protecting all SSO traffic that is passed between the active and standby device. |

## Examples

The following example shows how to configure SSO traffic protection:

```
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0 no-xauth
!
crypto ipsec transform-set trans2 ah-md5-hmac esp-aes
!
crypto ipsec profile sso-secure
 set transform-set trans2
!
redundancy inter-device
 scheme standby HA-out
 security ipsec sso-secure
```

## Managing and Verifying High Availability Information

Use any of the following optional tasks to secure and manage your high availability configurations:

- [Managing Anti-Replay Intervals, page 21](#)
- [Managing and Verifying HA Configurations, page 22](#)

### Managing Anti-Replay Intervals

Use this optional task to modify the interval in which an IP redundancy-enabled crypto map forwards anti-replay updates from the active router to the standby router.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map *map-name* redundancy replay-interval inbound *in-value* outbound *out-value***

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                           | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 3 | <b>crypto map</b> <i>map-name</i> <b>redundancy replay-interval</b><br><b>inbound</b> <i>in-value</i> <b>outbound</b> <i>out-value</i><br><br><b>Example:</b><br>Router(config)# crypto map to-peer-outside<br>redundancy replay-interval inbound 1000<br>outbound 10000 | Modifies the interval at which inbound and outbound replay counters are passed from an active device to a standby device. <ul style="list-style-type: none"> <li><b>inbound</b> <i>in-value</i>—Number of inbound packets that are processed before an anti-replay update is sent from the active router to the standby router. Default value: one update every 1,000 packets.</li> <li><b>outbound</b> <i>out-value</i>—Number of outbound packets that are processed before an anti-replay update is sent from the active router to the standby router. Default value: one update every 100,000 packets.</li> </ul> |

## Examples

The following example shows how to modify replay counter intervals between the active and standby devices on the crypto map “to-peer-outside”:

```
crypto map to-peer-outside redundancy replay-interval inbound 1000 outbound 10000
crypto map to-peer-outside 10 ipsec-isakmp
 set peer 209.165.200.225
 set transform-set trans1
 match address peer-outside
```

## Managing and Verifying HA Configurations

Use any of the steps within this optional task to display and verify the high availability configurations.

### SUMMARY STEPS

1. **enable**
2. **show redundancy** [states | inter-device]
3. **show crypto isakmp sa** [active | standby]
4. **show crypto ipsec sa** [active | standby]
5. **show crypto session** [active | standby]
6. **show crypto ha**
7. **clear crypto isakmp** [active | standby]

8. **clear crypto sa** [active | standby]
9. **clear crypto session** [active | standby]

## DETAILED STEPS

|        | Command or Action                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                  |
|--------|----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                         |
| Step 2 | <b>show redundancy</b> [states   inter-device]<br><br><b>Example:</b><br>Router# show redundancy states        | Displays the current state of SSO on the configured device.<br><br>After the two devices have negotiated with each other, one device should show an “ACTIVE” state and the other device should show a “STANDBY HOT” state.                                                                                                                               |
| Step 3 | <b>show crypto isakmp sa</b> [active   standby]<br><br><b>Example:</b><br>Router# show crypto isakmp sa active | Displays IKE SAs present on the device.<br><br>An “ACTIVE” or “STDBY” state is shown for each SA. <ul style="list-style-type: none"> <li>The <b>active</b> keyword displays only ACTIVE, HA-enabled SAs; The <b>standby</b> keyword displays only STDBY, HA-enabled SAs.</li> </ul>                                                                      |
| Step 4 | <b>show crypto ipsec sa</b> [active   standby]<br><br><b>Example:</b><br>Router# show crypto ipsec sa active   | Displays IPsec SAs present on the device.<br><br>An “ACTIVE” or “STDBY” state is shown for each SA. <ul style="list-style-type: none"> <li>The <b>active</b> keyword displays only ACTIVE, HA-enabled SAs; The <b>standby</b> keyword displays only STDBY, HA-enabled SAs.</li> </ul>                                                                    |
| Step 5 | <b>show crypto session</b> [active   standby]<br><br><b>Example:</b><br>Router# show crypto session active     | Displays crypto sessions that are currently present on the device.<br><br>An “ACTIVE” or “STANDBY” state is shown as part of the state of each session, such as “UP-STANDBY.”<br><br>Only HA-enabled SAs are shown.                                                                                                                                      |
| Step 6 | <b>show crypto ha</b><br><br><b>Example:</b><br>Router# show crypto ha                                         | Displays all virtual IP addresses that are currently in use by IPsec and IKE.                                                                                                                                                                                                                                                                            |
| Step 7 | <b>clear crypto isakmp</b> [active   standby]<br><br><b>Example:</b><br>Router# clear crypto isakmp active     | Clears IKE SAs.<br><br>When this command is issued on the standby device, all standby IKE SAs are resynchronized from the active device. <ul style="list-style-type: none"> <li>The <b>active</b> keyword clears only IKE HA-enabled SAs in the active state; the <b>standby</b> keyword clears only IKE HA-enabled SAs in the standby state.</li> </ul> |

|        | Command or Action                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 8 | <b>clear crypto sa</b> [active   standby]<br><br><b>Example:</b><br>Router# clear crypto sa active           | Clears IPSec SAs.<br><br>When this command is issued on the standby device, all standby IPSec SAs are resynchronized from the active device. <ul style="list-style-type: none"> <li>The <b>active</b> keyword clears only IPSec HA-enabled SAs in the active state; the <b>standby</b> keyword clears only IPSec HA-enabled SAs in the standby state.</li> </ul> |
| Step 9 | <b>clear crypto session</b> [active   standby]<br><br><b>Example:</b><br>Router# clear crypto session active | Clears both IKE and IPSec SAs.<br><br>Any standby SAs will resynchronize from the active device after they are cleared on the standby. Only HA-enabled SAs are cleared from the device.                                                                                                                                                                          |

## Examples

### Verifying the Active Device:Examples

Router# **show redundancy states**

```

my state = 13 -ACTIVE
peer state = 8 -STANDBY HOT
 Mode = Duplex
 Unit ID = 0

Split Mode = Disabled
Manual Swact = Enabled
Communications = Up

client count = 7
client_notification_TMR = 30000 milliseconds
 keep_alive TMR = 4000 milliseconds
 keep_alive count = 0
 keep_alive threshold = 7
 RF debug mask = 0x0

```

Router# **show crypto isakmp sa active**

```

dst src state conn-id slot status
209.165.201.3 209.165.200.225 QM_IDLE 5 0 ACTIVE

```

Router# **show crypto ipsec sa active**

```

interface:Ethernet0/0
 Crypto map tag:to-peer-outside, local addr 209.165.201.3

protected vrf:(none)
local ident (addr/mask/prot/port):(192.168.0.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port):(172.16.0.1/255.255.255.255/0/0)
current_peer 209.165.200.225 port 500
 PERMIT, flags={origin_is_acl,}
#pkts encaps:3, #pkts encrypt:3, #pkts digest:3
#pkts decaps:4, #pkts decrypt:4, #pkts verify:4
#pkts compressed:0, #pkts decompressed:0
#pkts not compressed:0, #pkts compr. failed:0
#pkts not decompressed:0, #pkts decompress failed:0
#send errors 0, #recv errors 0

```

```

local crypto endpt.:209.165.201.3, remote crypto endpt.:209.165.200.225
path mtu 1500, media mtu 1500
current outbound spi:0xD42904F0(3559458032)

inbound esp sas:
spi:0xD3E9ABD0(3555306448)
transform:esp-3des ,
in use settings ={Tunnel, }
conn id:2006, flow_id:6, crypto map:to-peer-outside
sa timing:remaining key lifetime (k/sec):(4586265/3542)
 HA last key lifetime sent(k):(4586267)
ike_cookies:9263635C CA4B4E99 C14E908E 8EE2D79C
IV size:8 bytes
replay detection support:Y
Status:ACTIVE
inbound ah sas:
spi: 0xF3EE3620(4092474912)
transform: ah-md5-hmac ,
in use settings ={Tunnel, }
conn id: 2006, flow_id: 6, crypto map: to-peer-outside
sa timing: remaining key lifetime (k/sec): (4586265/3542)
 HA last key lifetime sent(k): (4586267)
ike_cookies: 9263635C CA4B4E99 C14E908E 8EE2D79C
replay detection support: Y
Status: ACTIVE

inbound pcsp sas:

outbound esp sas:
spi: 0xD42904F0(3559458032)
transform: esp-3des ,
in use settings ={Tunnel, }
conn id: 2009, flow_id: 9, crypto map: to-peer-outside
sa timing: remaining key lifetime (k/sec): (4586266/3542)
 HA last key lifetime sent(k): (4586267)
ike_cookies: 9263635C CA4B4E99 C14E908E 8EE2D79C
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:
spi: 0x75251086(1965363334)
transform: ah-md5-hmac ,
in use settings ={Tunnel, }
conn id: 2009, flow_id: 9, crypto map: to-peer-outside
sa timing: remaining key lifetime (k/sec): (4586266/3542)
 HA last key lifetime sent(k): (4586267)
ike_cookies: 9263635C CA4B4E99 C14E908E 8EE2D79C
replay detection support: Y
Status: ACTIVE

outbound pcsp sas:

Router# show crypto session active
Crypto session current status

Interface: Ethernet0/0
Session status: UP-ACTIVE
Peer: 209.165.200.225 port 500
IKE SA: local 209.165.201.3/500 remote 209.165.200.225/500 Active
IKE SA: local 209.165.201.3/500 remote 209.165.200.225/500 Active
IPSEC FLOW: permit ip host 192.168.0.1 host 172.16.0.1
Active SAs: 4, origin: crypto map

```

```

Router# show crypto ha
IKE VIP: 209.165.201.3
 stamp: 74 BA 70 27 9C 4F 7F 81 3A 70 13 C9 65 22 E7 76
IPSec VIP: 209.165.201.3
IPSec VIP: 255.255.255.253
IPSec VIP: 255.255.255.254

```

### Verifying the Standby Device: Examples

```

Router# show redundancy states
 my state = 8 -STANDBY HOT
 peer state = 13 -ACTIVE
 Mode = Duplex
 Unit ID = 0
 Split Mode = Disabled
 Manual Swact = Enabled
 Communications = Up
 client count = 7
 client_notification_TMR = 30000 milliseconds
 keep_alive TMR = 4000 milliseconds
 keep_alive count = 1
 keep_alive threshold = 7
 RF debug mask = 0x0

Router# show crypto isakmp sa standby
dst src state conn-id slot status
209.165.201.3 209.165.200.225 QM_IDLE 5 0 STDBY

```

```

Router# show crypto ipsec sa standby
interface:Ethernet0/0
 Crypto map tag:to-peer-outside, local addr 209.165.201.3
 protected vrf:(none)
 local ident (addr/mask/prot/port):(192.168.0.1/255.255.255.255/0/0)
 remote ident (addr/mask/prot/port):(172.16.0.1/255.255.255.255/0/0)
 current_peer 209.165.200.225 port 500
 PERMIT, flags={origin_is_acl,}
 #pkts encaps:0, #pkts encrypt:0, #pkts digest:0
 #pkts decaps:0, #pkts decrypt:0, #pkts verify:0
 #pkts compressed:0, #pkts decompressed:0
 #pkts not compressed:0, #pkts compr. failed:0
 #pkts not decompressed:0, #pkts decompress failed:0
 #send errors 0, #recv errors 0
 local crypto endpt.:209.165.201.3, remote crypto endpt.:209.165.200.225
 path mtu 1500, media mtu 1500
 current outbound spi:0xD42904F0(3559458032)
 inbound esp sas:
 spi:0xD3E9ABD0(3555306448)
 transform:esp-3des ,
 in use settings ={Tunnel, }
 conn id:2012, flow_id:12, crypto map:to-peer-outside
 sa timing:remaining key lifetime (k/sec):(4441561/3486)
 HA last key lifetime sent(k):(4441561)
 ike_cookies:00000000 00000000 00000000 00000000
 IV size:8 bytes
 replay detection support:Y
 Status:STANDBY
 inbound ah sas:
 spi:0xF3EE3620(4092474912)
 transform:ah-md5-hmac ,
 in use settings ={Tunnel, }
 conn id:2012, flow_id:12, crypto map:to-peer-outside

```



```

sa timing:remaining key lifetime (k/sec):(4441561/3486)
 HA last key lifetime sent(k):(4441561)
ike_cookies:00000000 00000000 00000000 00000000
replay detection support:Y
Status:STANDBY
inbound pcp sas:
outbound esp sas:
 spi:0xD42904F0(3559458032)
 transform:esp-3des ,
 in use settings ={Tunnel, }
 conn id:2011, flow_id:11, crypto map:to-peer-outside
 sa timing:remaining key lifetime (k/sec):(4441561/3485)
 HA last key lifetime sent(k):(4441561)
 ike_cookies:00000000 00000000 00000000 00000000
 IV size:8 bytes
 replay detection support:Y
 Status:STANDBY
outbound ah sas:
 spi:0x75251086(1965363334)
 transform:ah-md5-hmac ,
 in use settings ={Tunnel, }
 conn id:2011, flow_id:11, crypto map:to-peer-outside
 sa timing:remaining key lifetime (k/sec):(4441561/3485)
 HA last key lifetime sent(k):(4441561)
 ike_cookies:00000000 00000000 00000000 00000000
 replay detection support:Y
 Status:STANDBY
outbound pcp sas:

```

Router# **show crypto session standby**

```

Crypto session current status
Interface:Ethernet0/0
Session status:UP-STANDBY
Peer:209.165.200.225 port 500
 IKE SA:local 209.165.201.3/500 remote 209.165.200.225/500 Active
 IPSEC FLOW:permit ip host 192.168.0.1 host 172.16.0.1
 Active SAs:4, origin:crypto map

```

Router# **show crypto ha**

```

IKE VIP:209.165.201.3
 stamp:74 BA 70 27 9C 4F 7F 81 3A 70 13 C9 65 22 E7 76

```

```

IPSec VIP:209.165.201.3
IPSec VIP:255.255.255.253
IPSec VIP:255.255.255.254
ha-R2#

```

### Verifying the Active and Standby SAs: Example

The following sample output shows SAs of both the active and standby devices:

Router# **show crypto isakmp sa**

| dst           | src             | state   | conn-id | slot | status |
|---------------|-----------------|---------|---------|------|--------|
| 209.165.201.3 | 209.165.200.225 | QM_IDLE | 2       | 0    | STDBY  |
| 10.0.0.1      | 10.0.0.2        | QM_IDLE | 1       | 0    | ACTIVE |

# Configuration Examples for Stateful Failover

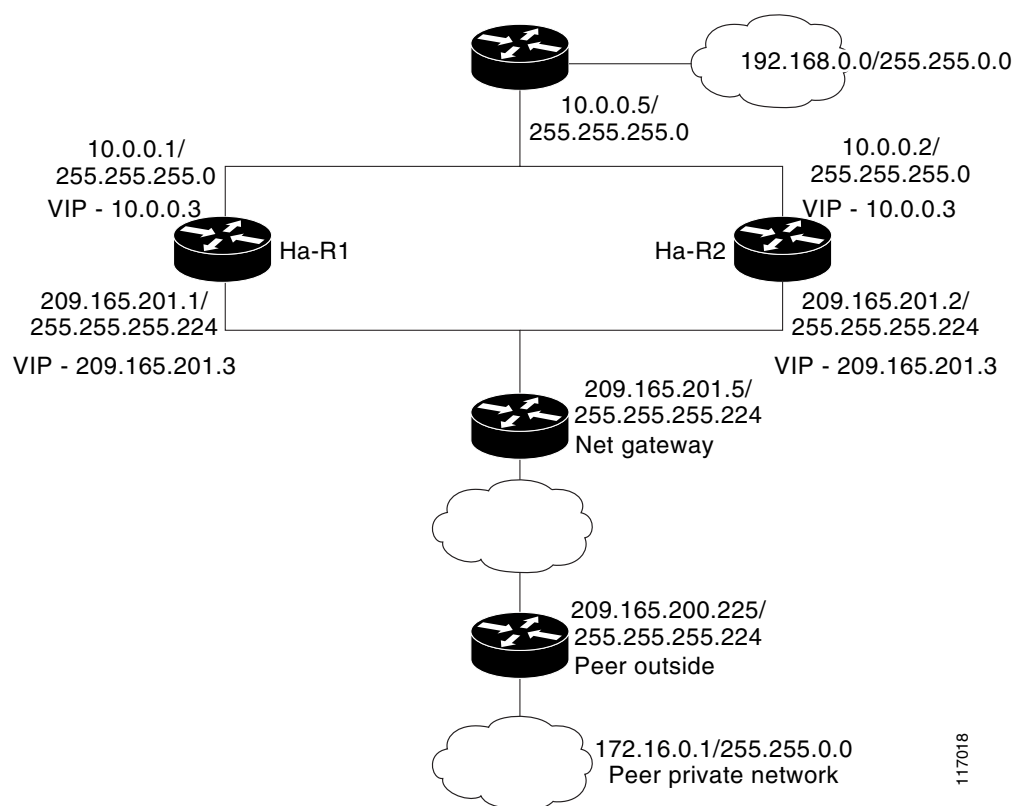
This section contains the following comprehensive IPSec stateful failover configuration examples:

- [Configuring IPSec Stateful Failover: Example, page 27](#)
- [Configuring IPSec Stateful Failover for an Easy VPN Server: Example, page 31](#)

## Configuring IPSec Stateful Failover: Example

Figure 3 and the following sample outputs from the show running-config command illustrate how to configure stateful failover on two devices—Ha-R1 and Ha-R2.

**Figure 95** *IPSec Stateful Failover Sample Topology*



### Stateful Failover Configuration on Ha-R1

Ha-R1# **show running-config**

Building configuration...

Current configuration :2086 bytes

!

version 12.3

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname ha-R1

```
!
boot-start-marker
boot-end-marker
!
!
redundancy inter-device
 scheme standby HA-out
 security ipsec sso-secure
!
logging buffered 10000000 debugging
logging rate-limit console 10000
!
!
ipc zone default
 association 1
 no shutdown
 protocol sctp
 local-port 5000
 local-ip 10.0.0.1
 remote-port 5000
 remote-ip 10.0.0.2
!
clock timezone PST 0
no aaa new-model
ip subnet-zero
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0 no-xauth
!
!
crypto ipsec transform-set trans1 ah-md5-hmac esp-3des
crypto ipsec transform-set trans2 ah-md5-hmac esp-aes
!
crypto ipsec profile sso-secure
 set transform-set trans2
!
!
crypto map to-peer-outside redundancy replay-interval inbound 1000 outbound 10000
crypto map to-peer-outside 10 ipsec-isakmp
 set peer 209.165.200.225
 set transform-set trans1
 match address peer-outside
!
!
!
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 preempt
 standby 1 name HA-out
 standby 1 track Ethernet1/0
 standby delay reload 120
 crypto map to-peer-outside redundancy HA-out stateful
!
interface Ethernet1/0
 ip address 10.0.0.1 255.255.255.0
 standby 2 ip 10.0.0.3
 standby 2 preempt
 standby 2 name HA-in
 standby delay reload 120
 standby 2 track Ethernet0/0
!
interface Serial12/0
```

```

no ip address
shutdown
serial restart-delay 0
!
interface Serial3/0
no ip address
shutdown
serial restart-delay 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.201.5
ip route 192.168.0.0 255.255.0.0
no ip http server
no ip http secure-server
!
!
!
ip access-list extended peer-outside
permit ip host 192.168.0.1 host 172.16.0.1
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
transport preferred all
transport output all
line aux 0
transport preferred all
transport output all
line vty 0 4
login
transport preferred all
transport input all
transport output all
!
end

```

### Stateful Failover Configuration on Ha-R2

Ha-R2# **show running-config**

Building configuration...

```

Current configuration :2100 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ha-R2
!
boot-start-marker
boot-end-marker
!
!
redundancy inter-device
scheme standby HA-out
security ipsec sso-secure
!
logging buffered 10000000 debugging
logging rate-limit console 10000

```

```
!
!
ipc zone default
 association 1
 no shutdown
 protocol sctp
 local-port 5000
 local-ip 10.0.0.2
 remote-port 5000
 remote-ip 10.0.0.1
!
clock timezone PST 0
no aaa new-model
ip subnet-zero
!
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 120
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0 no-xauth
!
!
crypto ipsec transform-set trans1 ah-md5-hmac esp-3des
crypto ipsec transform-set trans2 ah-md5-hmac esp-aes
!
crypto ipsec profile sso-secure
 set transform-set trans2
!
!
crypto map to-peer-outside redundancy replay-interval inbound 1000 outbound 10000
crypto map to-peer-outside 10 ipsec-isakmp
 set peer 209.165.200.225
 set transform-set trans1
 match address peer-outside
!
!
!
interface Ethernet0/0
 ip address 209.165.201.2 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 preempt
 standby 1 name HA-out
 standby 1 track Ethernet1/0
 standby delay reload 120
 crypto map to-peer-outside redundancy HA-out stateful
!
interface Ethernet1/0
 ip address 10.0.0.2 255.255.255.0
 standby 2 ip 10.0.0.3
 standby 2 preempt
 standby 2 name HA-in
 standby delay reload 120
 standby 2 track Ethernet0/0
!
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/0
 no ip address
 shutdown
 serial restart-delay 0
!
```

```

ip classless
ip route 0.0.0.0 0.0.0.0 209.165.201.5
ip route 192.168.0.0 255.255.0.0
no ip http server
no ip http secure-server
!
!
!
ip access-list extended peer-outside
 permit ip host 192.168.0.1 host 172.16.0.1
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 transport preferred all
 transport output all
line aux 0
 transport preferred all
 transport output all
line vty 0 4
 login
 transport preferred all
 transport input all
 transport output all
!
end

Ha-R2#

```

## Configuring IPSec Stateful Failover for an Easy VPN Server: Example

The following sample outputs from the **show running-config** command show how to configure stateful failover for a remote access connection via an Easy VPN server:

### Stateful Failover for an Easy VPN Server Configuration on RAHA-R1

```

RAHA-R1# show running-config
Building configuration...

Current configuration :3829 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RAHA-R1
!
boot-start-marker
boot-end-marker
!
redundancy inter-device
 scheme standby HA-out
!
username remote_user password 0 letmein
!
ipc zone default
 association 1

```

```
no shutdown
protocol sctp
 local-port 5000
 local-ip 10.0.0.1
 remote-port 5000
 remote-ip 10.0.0.2
!
aaa new-model
!
!
! Enter the following command if you are doing Xauth locally.
aaa authentication login local_xauth local
!
! Enter the following command if you are doing Xauth remotely via RADIUS.
!aaa authentication login radius_xauth group radius
!
! Enter the following command if you are not doing Xauth
!aaa authentication login no_xauth none
!
! Enter the following command if you are doing local group authentication.
aaa authorization network local_auth local
!
! Enter the following command if you are doing group authentication remotely via RADIUS.
!aaa authorization network radius_auth group radius
!
!
! Enter the following command if you are doing Xauth remotely via RADIUS.
!
aaa accounting network radius_accounting start-stop group radius
aaa session-id common
ip subnet-zero
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
!
!
! Enter the following command if you are doing group authentication locally.
crypto isakmp client configuration group unity
 key cisco123
 domain cisco.com
 pool client-address-pool
!
!
crypto ipsec transform-set trans1 esp-3des esp-sha-hmac
!
crypto dynamic-map to-remote-client 10
 set transform-set trans1
 reverse-route remote-peer
!
! Use this map if you want to do local group authentication and Xauth.
crypto map to_peer_outside_local_xauth client authentication list local_xauth
crypto map to_peer_outside_local_xauth isakmp authorization list local_auth
crypto map to_peer_outside_local_xauth client configuration address respond
crypto map to_peer_outside_local_xauth 10 ipsec-isakmp dynamic to-remote-client
!
! Use this map if you want to use Radius for group authentication and Xauth.
!crypto map to_peer_outside_radius_xauth isakmp client authentication list radius_xauth
!crypto map to_peer_outside_radius_xauth client accounting list radius_accounting
!crypto map to_peer_outside_radius_xauth isakmp authorization list radius_auth
!crypto map to_peer_outside_radius_xauth isakmp client configuration address respond
!crypto map to_peer_outside_radius_xauth isakmp 10 ipsec-isakmp dynamic to-remote-client
```

```

!
! Use this map if you want to do local group authentication and no Xauth
!crypto map to_peer_outside_no_xauth isakmp authorization list local_auth
!crypto map to_peer_outside_no_xauth configuration address respond
!crypto map to_peer_outside_no_xauth 10 ipsec-isakmp dynamic to-remote-client
!
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 preempt
 standby 1 name HA-out
 standby 1 track Ethernet1/0
 standby delay reload 120
 crypto map to_peer_outside_local_xauth redundancy HA-out stateful
!
interface Ethernet1/0
 ip address 10.0.0.1 255.255.255.0
 standby 2 ip 10.0.0.3
 standby 2 preempt
 standby 2 name HA-in
 standby 2 track Ethernet0/0
 standby delay reload 120
!
! Enable loopback0 if you are using radius for Xauth, group auth, or accounting with
! crypto HA
!interface loopback0
! ip address 192.168.100.1 255.255.255.255
!
! Enable this command if you are using radius for Xauth, group auth, or accounting with
! crypto HA
!ip radius source-interface loopback0
!
ip local pool client-address-pool 50.0.0.1 50.0.0.254
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.201.5
ip route 192.168.0.0 255.255.255.0 10.0.0.5
!
radius-server host 192.168.0.0 255.255.0.0 auth-port 1845 acct-port 1846
radius-server key radius123
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
end

```

### Stateful Failover for an Easy VPN Server Configuration on RAHA-R2

RAHA-R2# **show running-config**

Building configuration...

Current configuration :3829 bytes

```

!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RAHA-R2

```



```
!
boot-start-marker
boot-end-marker
!
redundancy inter-device
 scheme standby HA-out
!
username remote_user password 0 letmein
!
ipc zone default
 association 1
 no shutdown
 protocol sctp
 local-port 5000
 local-ip 10.0.0.2
 remote-port 5000
 remote-ip 10.0.0.1
!
aaa new-model
!
!
! Enter the following command if you are doing Xauth locally.
aaa authentication login local_xauth local
!
! Enter the following command if you are doing Xauth remotely via RADIUS.
!aaa authentication login radius_xauth group radius
!
! Enter the following command if you are not doing Xauth.
!aaa authentication login no_xauth none
!
! Enter the following command if you are doing local group authentication.
aaa authorization network local_auth local
!
! Enter the following command if you are doing group authentication remotely via RADIUS.
!aaa authorization network radius_auth group radius
!
!
! Enter the following command if you are doing Xauth remotely via RADIUS.
!aaa accounting network radius_accounting start-stop group radius
aaa session-id common
ip subnet-zero
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
!
!
! Enter the following commands if you are doing group authentication locally.
crypto isakmp client configuration group unity
 key cisco123
 domain cisco.com
 pool client-address-pool
!
!
crypto ipsec transform-set trans1 esp-3des esp-sha-hmac
!
crypto dynamic-map to-remote-client 10
 set transform-set trans1
 reverse-route remote-peer
!
!
! Use this map if you want to do local group authentication and Xauth.
```

```

crypto map to_peer_outside_local_xauth client authentication list local_xauth
crypto map to_peer_outside_local_xauth isakmp authorization list local_auth
crypto map to_peer_outside_local_xauth client configuration address respond
crypto map to_peer_outside_local_xauth 10 ipsec-isakmp dynamic to-remote-client
!
! Use this map if you want to use Radius for group authentication and Xauth.
!crypto map to_peer_outside_radius_xauth isakmp client authentication list radius_xauth
!crypto map to_peer_outside_radius_xauth client accounting list radius_accounting
!crypto map to_peer_outside_radius_xauth isakmp authorization list radius_auth
!crypto map to_peer_outside_radius_xauth isakmp client configuration address respond
!crypto map to_peer_outside_radius_xauth isakmp 10 ipsec-isakmp dynamic to-remote-client
!
!
! Use this map if you want to do local authentication and no Xauth.
!crypto map to_peer_outside_no_xauth isakmp authorization list local_auth
!crypto map to_peer_outside_no_xauth configuration address respond
!crypto map to_peer_outside_no_xauth 10 ipsec-isakmp dynamic to-remote-client
!
interface Ethernet0/0
 ip address 209.165.201.2 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 preempt
 standby 1 name HA-out
 standby 1 track Ethernet1/0
 standby delay reload
 crypto map to_peer_outside_local_xauth redundancy HA-out stateful
!
interface Ethernet1/0
 ip address 10.0.0.2 255.255.255.0
 standby 2 ip 10.0.0.3
 standby 2 preempt
 standby 2 name HA-in
 standby 2 track Ethernet0/0
 standby delay reload
!
! Enable loopback0 if you are using radius for Xauth, group auth, or accounting with
! crypto HA
!interface loopback0
! ip address 192.168.100.1 255.255.255.255
!
! Enable this command if you are using radius for Xauth, group auth, or accounting with
! crypto HA
!ip radius source-interface loopback0
!
ip local pool client-address-pool 50.0.0.1 50.0.0.254
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.201.5
ip route 192.168.0.0 255.255.0.0
!
radius-server host 192.168.0.200 auth-port 1845 acct-port 1846
radius-server key radius123
!
control-plane
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
end

```

# Additional References

The following sections provide references related to stateful failover for IPSec.

## Related Documents

| Related Topic          | Document Title                                                                                                                          |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| RRI                    | The section “ <a href="#">IPSec VPN High Availability Enhancements</a> ” in the <i>Cisco IOS Security Configuration Guide</i> .         |
| HSRP                   | The section “ <a href="#">Configuring the Hot Standby Router Protocol</a> ” in the <i>Cisco IOS IP Configuration Guide</i> .            |
| Easy VPN Server        | The section “ <a href="#">Cisco Easy VPN Remote</a> ” in the <i>Cisco IOS Security Configuration Guide</i> .                            |
| IKE configuration      | The section “ <a href="#">Configuring Internet Key Exchange for IPSec VPNs</a> ” in the <i>Cisco IOS Security Configuration Guide</i> . |
| IPSec configuration    | The section “ <a href="#">Configuring Security for VPNs with IPSec</a> ” in the <i>Cisco IOS Security Configuration Guide</i> .         |
| IPSec and IKE commands | <a href="#">Cisco IOS Security Command Reference</a> .                                                                                  |

## Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

## MIBs

| MIBs | MIBs Link                                                                                                                                                                                                                  |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs | Title |
|------|-------|
| None | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or a Cisco IOS master commands list.

### New Commands

- **crypto map redundancy replay-interval**
- **debug crypto ha**
- **debug crypto ipsec ha**
- **debug crypto isakmp ha**
- **local-ip (IPC transport-SCTP local)**
- **local-port**
- **redundancy inter-device**
- **redundancy stateful**
- **remote-ip (IPC transport-SCTP remote)**
- **remote-port**
- **scheme**
- **security ipsec**
- **show crypto ha**

### Modified Commands

- **clear crypto isakmp**
- **clear crypto sa**
- **clear crypto session**

- **crypto map (interface IPSec)**
- **show crypto ipsec sa**
- **show crypto isakmp sa**
- **show crypto session**
- **show redundancy**

---

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)

---

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.





## VRF-Aware IPSec

---

The VRF-Aware IPSec feature introduces IP Security (IPSec) tunnel mapping to Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). Using the VRF-Aware IPSec feature, you can map IPSec tunnels to Virtual Routing and Forwarding (VRF) instances using a single public-facing address.

### Feature Specifications for VRF-Aware IPSec

---

#### Feature History

| Release   | Modification                 |
|-----------|------------------------------|
| 12.2(15)T | This feature was introduced. |

---

#### Supported Platforms

---

Cisco 1710, Cisco 1760, Cisco 2610-Cisco 2613, Cisco 2620-Cisco 2621, Cisco 2650-Cisco 2651, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 7100, Cisco 7200, Cisco 7400, Cisco 870 Series

---

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Restrictions for VRF-Aware IPSec, page 2](#)
- [Information About VRF-Aware IPSec, page 2](#)
- [How to Configure VRF-Aware IPSec, page 4](#)
- [Configuration Examples for VRF-Aware IPSec, page 22](#)
- [Additional References, page 34](#)
- [Command Reference, page 35](#)
- [Glossary, page 37](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

## Restrictions for VRF-Aware IPsec

- If you are configuring VRF-Aware IPsec using a crypto map configuration and the Inside VRF (IVRF) is not the same as the Front Door VRF (FVRF), this feature is not interoperable with unicast reverse path forwarding (uRPF) if uRPF is enabled on the crypto map interface. If your network requires uRPF, it is recommended that you use Virtual Tunnel Interface (VTI) for IPsec instead of crypto maps.
- The VRF-Aware IPsec feature does not allow IPsec tunnel mapping between VRFs. For example, it does not allow IPsec tunnel mapping from VRF vpn1 to VRF vpn2.

## Information About VRF-Aware IPsec

The VRF-Aware IPsec feature maps an IPsec tunnel to a MPLS VPN. To configure and use the feature, you need to understand the following concepts:

- [VRF Instance, page 2](#)
- [MPLS Distribution Protocol, page 2](#)
- [VRF-Aware IPsec Functional Overview, page 2](#)

### VRF Instance

A VRF instance is a per-VPN routing information repository that defines the VPN membership of a customer site attached to the Provider Edge (PE) router. A VRF comprises an IP routing table, a derived Cisco Express Forwarding (CEF) table, a set of interfaces that use the forwarding table, and a set of rules and routing protocol parameters that control the information that is included in the routing table. A separate set of routing and CEF tables is maintained for each VPN customer.

### MPLS Distribution Protocol

The MPLS distribution protocol is a high-performance packet-forwarding technology that integrates the performance and traffic management capabilities of data link layer switching with the scalability, flexibility, and performance of network-layer routing.

### VRF-Aware IPsec Functional Overview

Front Door VRF (FVRF) and Inside VRF (IVRF) are central to understanding the feature.

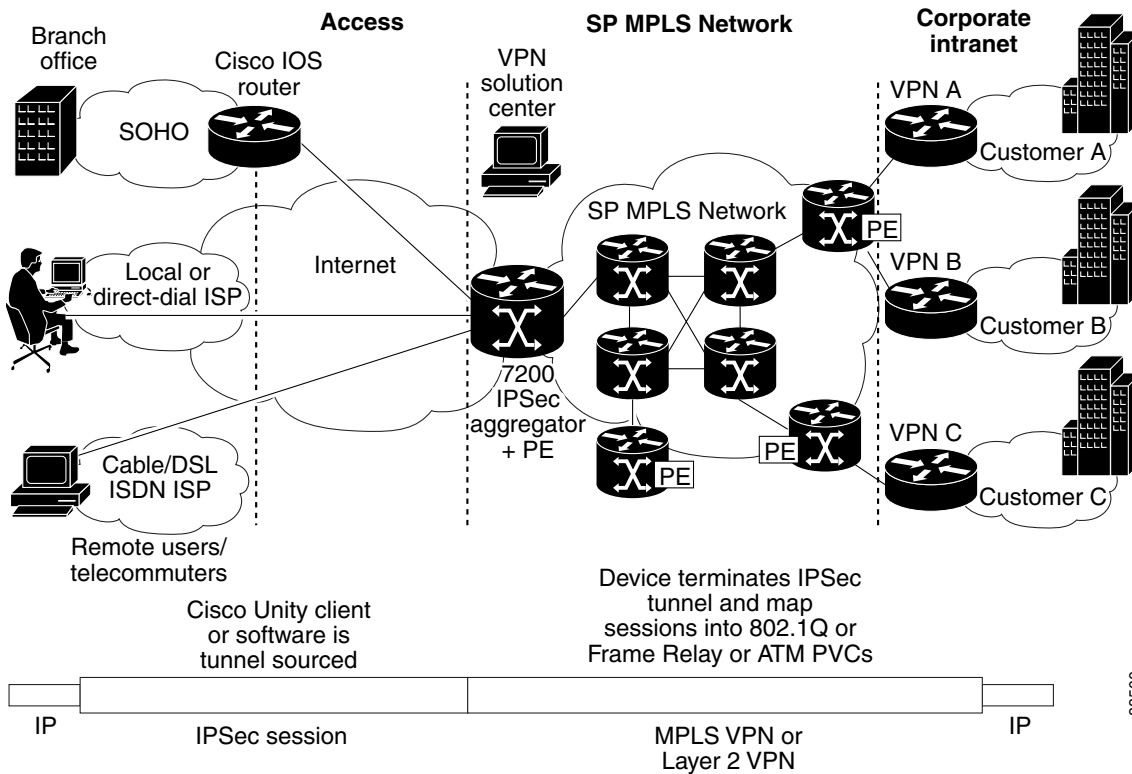
Each IPsec tunnel is associated with two VRF domains. The outer encapsulated packet belongs to one VRF domain, which we shall call the FVRF, while the inner, protected IP packet belongs to another domain called the IVRF. Another way of stating the same thing is that the local endpoint of the IPsec tunnel belongs to the FVRF while the source and destination addresses of the inside packet belong to the IVRF.

One or more IPsec tunnels can terminate on a single interface. The FVRF of all these tunnels is the same and is set to the VRF that is configured on that interface. The IVRF of these tunnels can be different and depends on the VRF that is defined in the Internet Security Association and Key Management Protocol (ISAKMP) profile that is attached to a crypto map entry.



Figure 96 is an illustration of a scenario showing IPSec to MPLS and Layer 2 VPNs.

**Figure 96** *IPSec to MPLS and Layer 2 VPNs*



## Packet Flow into the IPSec Tunnel

- A VPN packet arrives from the Service Provider MPLS backbone network to the PE and is routed through an interface facing the Internet.
- The packet is matched against the Security Policy Database (SPD), and the packet is IPSec encapsulated. The SPD includes the IVRF and the access control list (ACL).
- The IPSec encapsulated packet is then forwarded using the FVRF routing table.

## Packet Flow from the IPSec Tunnel

- An IPSec-encapsulated packet arrives at the PE router from the remote IPSec endpoint.
- IPSec performs the Security Association (SA) lookup for the Security Parameter Index (SPI), destination, and protocol.
- The packet is decapsulated using the SA and is associated with IVRF.
- The packet is further forwarded using the IVRF routing table.

# How to Configure VRF-Aware IPSec

This section contains the following procedures:

- [Configuring Crypto Keyrings, page 4](#) (Optional)
- [Configuring ISAKMP Profiles, page 6](#) (Required)
- [Configuring an ISAKMP Profile on a Crypto Map, page 10](#) (Required)
- [Configuring to Ignore Extended Authentication During IKE Phase 1 Negotiation, page 11](#) (Optional)
- [Verifying VRF-Aware IPSec, page 12](#)
- [Clearing Security Associations, page 13](#)
- [Troubleshooting VRF-Aware IPSec, page 13](#)

## Configuring Crypto Keyrings

A crypto keyring is a repository of preshared and Rivest, Shamir, and Adelman (RSA) public keys. There can be zero or more keyrings on the Cisco IOS router.

Perform the following optional task to configure a crypto keyring.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto keyring** *keyring-name* [**vrf** *fvr-f-name*]
4. **description** *string* (Optional)
5. **pre-shared-key** {**address** *address* [*mask*] | **hostname** *hostname*} **key** *key* (Optional)
6. **rsa-pubkey** {**address** *address* | **name** *fqdn*} [**encryption** | **signature**] (Optional)
7. **address** *ip-address* (Optional)
8. **serial-number** *serial-number* (Optional)
9. **key-string**
10. **text**
11. **quit**
12. **exit**
13. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                             |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                 | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 3 | <b>crypto keyring</b> <i>keyring-name</i> [ <b>vrf</b> <i>fvrf-name</i> ]<br><br><b>Example:</b><br>Router (config)# crypto keyring VPN1                                                                                       | Defines a keyring with <i>keyring-name</i> as the name of the keyring and enters keyring configuration mode. <ul style="list-style-type: none"> <li>(Optional) The <b>vrf</b> keyword and <i>fvrf-name</i> argument imply that the keyring is bound to Front Door Virtual Routing and Forwarding (FVRF). The key in the keyring is searched if the local endpoint is in FVRF. If <b>vrf</b> is not specified, the keyring is bound to the global.</li> </ul>                 |
| Step 4 | <b>description</b> <i>string</i><br><br>Router (config-keyring)# description The keys for VPN1                                                                                                                                 | (Optional) Specifies a one-line description of the keyring.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 5 | <b>pre-shared-key</b> { <b>address</b> <i>address</i> [ <i>mask</i> ]   <b>hostname</b> <i>hostname</i> } <b>key</b> <i>key</i><br><br><b>Example:</b><br>Router (config-keyring)# pre-shared-key address 10.72.23.11 key VPN1 | (Optional) Defines a preshared key by address or host name.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 6 | <b>rsa-pubkey</b> { <b>address</b> <i>address</i>   <b>name</b> <i>fqdn</i> } [ <b>encryption</b>   <b>signature</b> ]<br><br><b>Example:</b><br>Router(config-keyring)# rsa-pubkey name host.vpn.com                          | (Optional) Defines a Rivest, Shamir, and Adelman (RSA) public key by address or host name and enters rsa-pubkey configuration mode. <ul style="list-style-type: none"> <li>By default, the key is used for signature.</li> <li>The optional <b>encryption</b> keyword specifies that the key should be used for encryption. The optional <b>signature</b> keyword specifies that the key should be used for signature. By default, the key is used for signature.</li> </ul> |
| Step 7 | <b>address</b> <i>ip-address</i><br><br><b>Example:</b><br>Router(config-pubkey-key)# address 10.5.5.1                                                                                                                         | (Optional) Defines the RSA public key IP address.                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 8 | <b>serial-number</b> <i>serial-number</i><br><br><b>Example:</b><br>Router(config-pubkey-key)# serial-number 1000000                                                                                                           | (Optional) Specifies the serial number of the public key. The value is from 0 through infinity.                                                                                                                                                                                                                                                                                                                                                                              |

|         | Command or Action                                                                                    | Purpose                                                                                 |
|---------|------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| Step 9  | <b>key-string</b><br><br><b>Example:</b><br>Router (config-pubkey-key)# key-string                   | Enters into the text mode in which you define the public key.                           |
| Step 10 | <b>text</b><br><br><b>Example:</b><br>Router (config-pubkey)# 00302017 4A7D385B<br>1234EF29 335FC973 | Specifies the public key.<br><b>Note</b> Only one public key may be added in this step. |
| Step 11 | <b>quit</b><br><br><b>Example:</b><br>Router (config-pubkey)# quit                                   | Quits to the public key configuration mode.                                             |
| Step 12 | <b>exit</b><br><br><b>Example:</b><br>Router (config-pubkey)# exit                                   | Exits to the keyring configuration mode.                                                |
| Step 13 | <b>exit</b><br><br><b>Example:</b><br>Router(config-keyring)# exit#                                  | Exits to global configuration mode.                                                     |

## Configuring ISAKMP Profiles

An ISAKMP profile is a repository for IKE Phase 1 and IKE Phase 1.5 configuration for a set of peers. An ISAKMP profile defines items such as keepalive, trustpoints, peer identities, and XAUTH AAA list during the IKE Phase 1 and Phase 1.5 exchange. There can be zero or more ISAKMP profiles on the Cisco IOS router.



### Note

- If traffic from the router to a certification authority (CA) (for authentication, enrollment, or for obtaining a certificate revocation list [CRL]) or to an Lightweight Directory Access Protocol (LDAP) server (for obtaining a CRL) needs to be routed via a VRF, the **vrf** command must be added to the trustpoint. Otherwise, such traffic will use the default routing table.
- If a profile does not specify one or more trustpoints, all trustpoints in the router will be used to attempt to validate the certificate of the peer (Internet Key Exchange (IKE) main mode or signature authentication). If one or more trustpoints are specified, only those trustpoints will be used.

## Restriction

A router initiating IKE and a router responding to the IKE request should have symmetrical trustpoint configurations. For example, a responding router (in IKE Main Mode) performing RSA signature encryption and authentication might use trustpoints that were defined in the global configuration when sending the CERT-REQ payloads. However, the router might use a restricted list of trustpoints that were defined in the ISAKMP profile for the certificate verification. If the peer (the IKE initiator) is configured

to use a certificate whose trustpoint is in the global list of the responding router but not in ISAKMP profile of the responding router, the certificate will be rejected. (However, if the initiating router does not know about the trustpoints in the global configuration of the responding router, the certificate can still be authenticated.)

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp profile** *profile-name*
4. **description** *string* (Optional)
5. **vrf** *ivrf-name* (Optional)
6. **keepalive** *seconds* **retry** *retry-seconds* (Optional)
7. **self-identity** {**address** | **fqdn** | **user-fqdn** *user-fqdn*} (Optional)
8. **keyring** *keyring-name* (Optional)
9. **ca trust-point** *trustpoint-name* (Optional)
10. **match identity** {**group** *group-name* | **address** *address* [*mask*] [*fvr*] | **host** *host-name* | **host domain** *domain-name* | **user** *user-fqdn* | **user domain** *domain-name*}
11. **client configuration address** {**initiate** | **respond**} (Optional)
12. **client authentication list** *list-name* (Optional)
13. **isakmp authorization list** *list-name* (Optional)
14. **initiate mode aggressive**
15. **exit**

## DETAILED STEPS

|        | Command or Action                                                       | Purpose                                                                                                                                  |
|--------|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                                           | Enables privileged EXEC mode.                                                                                                            |
|        | <b>Example:</b><br>Router> enable                                       | <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                       |
| Step 2 | <b>configure terminal</b>                                               | Enters global configuration mode.                                                                                                        |
|        | <b>Example:</b><br>Router# configure terminal                           |                                                                                                                                          |
| Step 3 | <b>crypto isakmp profile</b> <i>profile-name</i>                        | Defines an Internet Security Association and Key Management Protocol (ISAKMP) profile and enters into isakmp profile configuration mode. |
|        | <b>Example:</b><br>Router (config)# crypto isakmp profile<br>vpnprofile |                                                                                                                                          |

|        | Command or Action                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <b>description</b> <i>string</i><br><br><b>Example:</b><br>Router (conf-isa-prof)# description<br>configuration for VPN profile                                      | (Optional) Specifies a one-line description of an ISAKMP profile.                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 5 | <b>vrf</b> <i>ivrf-name</i><br><br><b>Example:</b><br>Router (conf-isa-prof)# vrf VPN1                                                                               | (Optional) Maps the IPSec tunnel to a Virtual Routing and Forwarding (VRF) instance.<br><br><b>Note</b> The VRF also serves as a selector for matching the Security Policy Database (SPD). If the VRF is not specified in the ISAKMP profile, the IVRF of the IPSec tunnel will be the same as its FVRF.                                                                                                                                              |
| Step 6 | <b>keepalive</b> <i>seconds</i> <b>retry</b> <i>retry-seconds</i><br><br><b>Example:</b><br>Router (conf-isa-prof)# keepalive 60 retry 5                             | (Optional) Allows the gateway to send dead peer detection (DPD) messages to the peer. <ul style="list-style-type: none"> <li>If not defined, the gateway uses the global configured value.</li> <li><i>seconds</i>—Number of seconds between DPD messages. The range is from 10 to 3600 seconds.</li> <li><b>retry</b> <i>retry-seconds</i>—Number of seconds between retries if the DPD message fails. The range is from 2 to 60 seconds.</li> </ul> |
| Step 7 | <b>self-identity</b> { <i>address</i>   <i>fqdn</i>   <i>user-fqdn</i><br><i>user-fqdn</i> }<br><br><b>Example:</b><br>Router (conf-isa-prof)# self-identity address | (Optional) Specifies the identity that the local Internet Key Exchange (IKE) should use to identify itself to the remote peer. <ul style="list-style-type: none"> <li>If not defined, IKE uses the global configured value.</li> <li><b>address</b>—Uses the IP address of the egress interface.</li> <li><b>fqdn</b>—Uses the fully qualified domain name (FQDN) of the router.</li> <li><b>user-fqdn</b>—Uses the specified value.</li> </ul>       |
| Step 8 | <b>keyring</b> <i>keyring-name</i><br><br><b>Example:</b><br>Router (conf-isa-prof)# keyring VPN1                                                                    | (Optional) Specifies the keyring to use for Phase 1 authentication. <ul style="list-style-type: none"> <li>If the keyring is not specified, the global key definitions are used.</li> </ul>                                                                                                                                                                                                                                                           |
| Step 9 | <b>ca trust-point</b> { <i>trustpoint-name</i> }<br><br><b>Example:</b><br>Router (conf-isa-prof)# ca trustpoint<br>VPN1-trustpoint                                  | (Optional) Specifies a trustpoint to validate a Rivest, Shamir, and Adelman (RSA) certificate. <ul style="list-style-type: none"> <li>If no trustpoint is specified in the ISAKMP profile, all the trustpoints that are configured on the Cisco IOS router are used to validate the certificate.</li> </ul>                                                                                                                                           |

|         | Command or Action                                                                                                                                                                                                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 10 | <p><b>match identity</b> {<b>group</b> <i>group-name</i>   <b>address</b> <i>address</i> [<i>mask</i>] [<i>fvrfl</i>]   <b>host</b> <i>host-name</i>   <b>host domain</b> <i>domain-name</i>   <b>user</b> <i>user-fqdn</i>   <b>user domain</b> <i>domain-name</i>}</p> <p><b>Example:</b><br/>Router (conf-isa-prof)# match identity address 10.1.1.1</p> | <p>Specifies the client IKE Identity (ID) that is to be matched.</p> <ul style="list-style-type: none"> <li>• <b>group</b> <i>group-name</i>—Matches the <i>group-name</i> with the ID type ID_KEY_ID. It also matches the <i>group-name</i> with the Organizational Unit (OU) field of the Distinguished Name (DN).</li> <li>• <b>address</b> <i>address</i> [<i>mask</i>] <i>fvrfl</i>—Matches the <i>address</i> with the ID type ID_IPV4_ADDR. The <i>mask</i> argument can be used to specify a range of addresses. The <i>fvrfl</i> argument specifies that the address is in Front Door Virtual Routing and Forwarding (FVRF).</li> <li>• <b>host</b> <i>hostname</i>—Matches the <i>hostname</i> with the ID type ID_FQDN.</li> <li>• <b>host domain</b> <i>domainname</i>—Matches the <i>domainname</i> to the ID type ID_FQDN whose domain name is the same as the <i>domainname</i>. Use this command to match all the hosts in the domain.</li> <li>• <b>user</b> <i>username</i>—Matches the <i>username</i> with the ID type ID_USER_FQDN.</li> <li>• <b>user domain</b> <i>domainname</i>—Matches the ID type ID_USER_FQDN whose domain name matches the <i>domainname</i>.</li> </ul> |
| Step 11 | <p><b>client configuration address</b> {<b>initiate</b>   <b>respond</b>}</p> <p><b>Example:</b><br/>Router (conf-isa-prof)# client configuration address initiate</p>                                                                                                                                                                                      | <p>(Optional) Specifies whether to initiate the mode configuration exchange or responds to mode configuration requests.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 12 | <p><b>client authentication list</b> <i>list-name</i></p> <p><b>Example:</b><br/>Router (conf-isa-prof)# client authentication list xauthlist</p>                                                                                                                                                                                                           | <p>(Optional) Authentication, authorization, and accounting (AAA) to use for authenticating the remote client during the extended authentication (XAUTH) exchange.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 13 | <p><b>isakmp authorization list</b> <i>list-name</i></p> <p><b>Example:</b><br/>Router (conf-isa-prof)# isakmp authorization list ikessaaalist</p>                                                                                                                                                                                                          | <p>(Optional) Network authorization server for receiving the Phase 1 preshared key and other attribute-value (AV) pairs.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 14 | <p><b>initiate mode aggressive</b></p> <p><b>Example:</b><br/>Router (conf-isa-prof)# initiate mode aggressive</p>                                                                                                                                                                                                                                          | <p>(Optional) Initiates aggressive mode exchange.</p> <ul style="list-style-type: none"> <li>• If not specified, IKE always initiates Main Mode exchange.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 15 | <p><b>exit</b></p> <p><b>Example:</b><br/>Router (conf-isa-prof)# exit</p>                                                                                                                                                                                                                                                                                  | <p>Exits to global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## What to Do Next

Go to the section “[Configuring an ISAKMP Profile on a Crypto Map](#).”

## Configuring an ISAKMP Profile on a Crypto Map

An ISAKMP profile must be applied to the crypto map. The IVRF on the ISAKMP profile is used as a selector when matching the VPN traffic. If there is no IVRF on the ISAKMP profile, the IVRF will be equal to the FVRF. Perform this required task to configure an ISAKMP profile on a crypto map.

## Prerequisites

Before configuring an ISAKMP profile on a crypto map, you must first have configured your router for basic IPSec.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name* **isakmp-profile** *isakmp-profile-name* (*Optional*)
4. **set isakmp-profile** *profile-name* (*Optional*)
5. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                            | Purpose                                                                                                                                                                                                                                                                |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                       | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                    |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                               | Enters global configuration mode.                                                                                                                                                                                                                                      |
| Step 3 | <b>crypto map</b> <i>map-name</i> <b>isakmp-profile</b> <i>isakmp-profile-name</i><br><br><b>Example:</b><br>Router (config)# crypto map vpnmap<br>isakmp-profile vpnprofile | (Optional) Specifies the Internet Key Exchange and Key Management Protocol (ISAKMP) profile for the crypto map set and enters crypto map configuration mode.<br><ul style="list-style-type: none"><li>• The ISAKMP profile will be used during IKE exchange.</li></ul> |



|        | Command or Action                                                                                                                 | Purpose                                                                                       |
|--------|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Step 4 | <b>set isakmp-profile</b> <i>profile-name</i><br><br><b>Example:</b><br>Router (config-crypto-map)# set isakmp-profile vpnprofile | (Optional) Specifies the ISAKMP profile to use when the traffic matches the crypto map entry. |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router (config-crypto-map)# exit                                                            | Exits to global configuration mode.                                                           |

## Configuring to Ignore Extended Authentication During IKE Phase 1 Negotiation

To ignore XAUTH during an IKE Phase 1 negotiation, use the **no crypto xauth** command. Use the **no crypto xauth** command if you do not require extended authentication for the Unity clients.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no crypto xauth** *interface*

### DETAILED STEPS

|        | Command or Action                                                                                           | Purpose                                                                                                                                                       |
|--------|-------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                      | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                            |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                              | Enters global configuration mode.                                                                                                                             |
| Step 3 | <b>no crypto xauth</b> <i>interface</i><br><br><b>Example:</b><br>Router(config)# no crypto xauth ethernet0 | Ignores XAUTH proposals for requests that are destined to the IP address of the interface. By default, Internet Key Exchange (IKE) processes XAUTH proposals. |

## Verifying VRF-Aware IPSec

To verify your VRF-Aware IPSec configurations, use the following **show** commands. These **show** commands allow you to list configuration information and security associations (SAs):

### SUMMARY STEPS

- **enable**
- **show crypto ipsec sa** [**map** *map-name* | **address** | **identity** | **interface** *interface* | **peer** [**vrf** *fvrf-name*] **address** | **vrf** *ivrf-name*] [**detail**]
- **show crypto isakmp key**
- **show crypto isakmp profile**
- **show crypto key pubkey-chain rsa**

### DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                              | Purpose                                                                                                                                                                                                                             |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                  |
| Step 2 | <b>show crypto ipsec sa</b> [ <b>map</b> <i>map-name</i>   <b>address</b>   <b>identity</b>   <b>interface</b> <i>interface</i>   <b>peer</b> [ <b>vrf</b> <i>fvrf-name</i> ] <b>address</b>   <b>vrf</b> <i>ivrf-name</i> ] [ <b>detail</b> ]<br><br><b>Example:</b><br>Router# show crypto ipsec sa vrf vpn1 | Allows you to view the settings used by current security associations (SAs).                                                                                                                                                        |
| Step 3 | <b>show crypto isakmp key</b><br><br><b>Example:</b><br>Router# show crypto isakmp key                                                                                                                                                                                                                         | Lists all the keyrings and their preshared keys. <ul style="list-style-type: none"> <li>• Use this command to verify your crypto keyring configuration.</li> </ul>                                                                  |
| Step 4 | <b>show crypto isakmp profile</b><br><br><b>Example:</b><br>Router# show crypto isakmp profile                                                                                                                                                                                                                 | Lists all ISAKMP profiles and their configurations.                                                                                                                                                                                 |
| Step 5 | <b>show crypto key pubkey-chain rsa</b><br><br><b>Example:</b><br>Router# show crypto key pubkey-chain rsa                                                                                                                                                                                                     | Views the Rivest, Shamir, and Adelman (RSA) public keys of the peer that are stored on your router. <ul style="list-style-type: none"> <li>• The output is extended to show the keyring to which the public key belongs.</li> </ul> |

## Clearing Security Associations

The following **clear** commands allow you to clear SAs.

### SUMMARY STEPS

- **enable**
- **clear crypto sa** [**counters** | **map** *map-name* | **peer** [**vrf** *fvrf-name*] *address* | **spi** *address* {**ah** | **esp**} *spi* | **vrf** *ivrf-name*]

### DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                               | Purpose                                                                                                            |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                          | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>clear crypto sa</b> [ <b>counters</b>   <b>map</b> <i>map-name</i>   <b>peer</b> [ <b>vrf</b> <i>fvrf-name</i> ] <i>address</i>   <b>spi</b> <i>address</i> { <b>ah</b>   <b>esp</b> } <i>spi</i>   <b>vrf</b> <i>ivrf-name</i> ]<br><br><b>Example:</b><br>Router# clear crypto sa vrf VPN1 | Clears the IPSec security associations (SAs).                                                                      |

## Troubleshooting VRF-Aware IPSec

To troubleshoot VRF-Aware IPSec, use the following **debug** commands:

### SUMMARY STEPS

1. **enable**
2. **debug crypto ipsec**
3. **debug crypto isakmp**

## DETAILED STEPS

|        | Command or Action                                                                        | Purpose                                                                                                          |
|--------|------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>debug crypto ipsec</b><br><br><b>Example:</b><br>Router# debug crypto ipsec           | Displays IP security (IPSec) events.                                                                             |
| Step 3 | <b>debug crypto isakmp</b><br><br><b>Example:</b><br>Router(config)# debug crypto isakmp | Displays messages about Internet Key Exchange (IKE) events.                                                      |

## Debug Examples for VRF-Aware IPSec

The following sample debug outputs are for a VRF-aware IPSec configuration:

## IPSec PE

Router# **debug crypto ipsec**

```

Crypto IPSEC debugging is on
IPSEC-PE#debug crypto isakmp
Crypto ISAKMP debugging is on
IPSEC-PE#debug crypto isakmp d
04:31:28: ISAKMP (0:12): purging SA., sa=6482B354, delme=6482B354
04:31:28: ISAKMP: Unlocking IKE struct 0x63C142F8 for declare_sa_dead(), count 0
IPSEC-PE#debug crypto isakmp detail
Crypto ISAKMP internals debugging is on
IPSEC-PE#
IPSEC-PE#
IPSEC-PE#
04:32:07: ISAKMP: Deleting peer node by peer_reap for 10.1.1.1: 63C142F8
04:32:55: ISAKMP cookie gen for src 172.16.1.1 dst 10.1.1.1
04:32:55: ISAKMP cookie 3123100B DC887D4E
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.68.1.1
04:32:55: ISAKMP cookie AA8F7B41 49A60E88
04:32:55: ISAKMP cookie gen for src 172.16.1.1 dst 10.1.1.1
04:32:55: ISAKMP cookie 3123100B DBC8E125
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 B4BDB5B7
04:32:55: ISAKMP (0:0): received packet from 10.1.1.1 dport 500 sport 500 Global (N) NEW
SA
04:32:55: ISAKMP: local port 500, remote port 500
04:32:55: ISAKMP: hash from 729FA94 for 619 bytes
04:32:55: ISAKMP: Packet hash:
64218CC0: B91E2C70 095A1346 9.,p.Z.F
64218CD0: 0EDB4CA6 8A46784F B314FD3B 00 .[L&.FxO.};;.
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:32:55: ISAKMP cookie AA8F7B41 F7ACF384
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:32:55: ISAKMP cookie AA8F7B41 0C07C670
04:32:55: ISAKMP: insert sa successfully sa = 6482B354
04:32:55: ISAKMP (0:13): processing SA payload. message ID = 0

```

```

04:32:55: ISAKMP (0:13): processing ID payload. message ID = 0
04:32:55: ISAKMP (0:13): peer matches vpn2-ra profile
04:32:55: ISAKMP: Looking for a matching key for 10.1.1.1 in default
04:32:55: ISAKMP: Created a peer struct for 10.1.1.1, peer port 500
04:32:55: ISAKMP: Locking peer struct 0x640BBB18, IKE refcount 1 for
crypto_ikmp_config_initialize_sa
04:32:55: ISAKMP (0:13): Setting client config settings 648252B0
04:32:55: ISAKMP (0:13): (Re)Setting client xauth list and state
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 157 mismatch
04:32:55: ISAKMP (0:13): vendor ID is NAT-T v3
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 123 mismatch
04:32:55: ISAKMP (0:13): vendor ID is NAT-T v2
04:32:55: ISAKMP (0:13): Authentication by xauth preshared
04:32:55: ISAKMP (0:13): Checking ISAKMP transform 1 against priority 1 policy
04:32:55: ISAKMP: encryption 3DES-CBC
04:32:55: ISAKMP: hash SHA
04:32:55: ISAKMP: default group 2
04:32:55: ISAKMP: auth XAUTHInitPreShared
04:32:55: ISAKMP: life type in seconds
04:32:55: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
04:32:55: ISAKMP (0:13): atts are acceptable. Next payload is 3
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 157 mismatch
04:32:55: ISAKMP (0:13): vendor ID is NAT-T v3
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 123 mismatch
04:32:55: ISAKMP (0:13): vendor ID is NAT-T v2
04:32:55: ISAKMP (0:13): processing KE payload. message ID = 0
04:32:55: ISAKMP (0:13): processing NONCE payload. message ID = 0
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID is DPD
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID seems Unity/DPD but major 175 mismatch
04:32:55: ISAKMP (0:13): vendor ID is XAUTH
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): claimed IOS but failed authentication
04:32:55: ISAKMP (0:13): processing vendor id payload
04:32:55: ISAKMP (0:13): vendor ID is Unity
04:32:55: ISAKMP (0:13): Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
04:32:55: ISAKMP (0:13): Old State = IKE_READY New State = IKE_R_AM_AAA_AWAIT

04:32:55: ISAKMP cookie gen for src 11.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 7AE6E1DF
04:32:55: ISAKMP: isadb_post_process_list: crawler: 4 AA 31 (6482B354)
04:32:55: crawler my_cookie AA8F7B41 F7ACF384
04:32:55: crawler his_cookie E46E088D F227FE4D
04:32:55: ISAKMP: got callback 1
04:32:55: ISAKMP (0:13): SKEYID state generated
04:32:55: ISAKMP: Unity/DPD ID: vendor_id_payload:
next: 0xD, reserved: 0x0, len 0x14
04:32:55: ISAKMP: Unity/DPD ID payload dump:
63E66D70: 0D000014
63E66D80: 12F5F28C 457168A9 702D9FE2 74CC0100 .ur.Eqh)p-.btL..
63E66D90: 00 .
04:32:55: ISAKMP: Unity/DPD ID: vendor_id_payload:
next: 0xD, reserved: 0x0, len 0x14
04:32:55: ISAKMP: Unity/DPD ID payload dump:
63E66D90: 0D000014 AFCAD713 68A1F1C9 6B8696FCJW.h!qIk..|
63E66DA0: 77570100 00 wW...
04:32:55: ISAKMP (0:13): constructed NAT-T vendor-03 ID
04:32:55: ISAKMP (0:13): SA is doing pre-shared key authentication plus XAUTH using id
type ID_IPV4_ADDR

```

```

04:32:55: ISAKMP (13): ID payload
 next-payload : 10
 type : 1
 addr : 172.16.1.1
 protocol : 17
 port : 0
 length : 8
04:32:55: ISAKMP (13): Total payload length: 12
04:32:55: ISAKMP (0:13): constructed HIS NAT-D
04:32:55: ISAKMP (0:13): constructed MINE NAT-D
04:32:55: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R)
AG_INIT_EXCH
04:32:55: ISAKMP (0:13): Input = IKE_MSG_FROM_AAA, PRESHARED_KEY_REPLY
04:32:55: ISAKMP (0:13): Old State = IKE_R_AM_AAA_AWAIT New State = IKE_R_AM2

04:32:55: ISAKMP cookie gen for src 172.16.1.1 dst 10.1.1.1
04:32:55: ISAKMP cookie 3123100B D99DA70D
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 9C69F917
04:32:55: ISAKMP: isadb_post_process_list: crawler: 5 21FF 1 (6482B354)
04:32:55: crawler my_cookie AA8F7B41 F7ACF384
04:32:55: crawler his_cookie E46E088D F227FE4D
04:32:55: ISAKMP cookie gen for src 172.16.1.1 dst 10.1.1.1
04:32:55: ISAKMP cookie 3123100B 00583224
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 C1B006EE
04:32:55: ISAKMP: isadb_post_process_list: crawler: 5 21FF 1 (6482B354)
04:32:55: crawler my_cookie AA8F7B41 F7ACF384
04:32:55: crawler his_cookie E46E088D F227FE4D
04:32:55: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R)
AG_INIT_EXCH
04:32:55: ISAKMP: hash from 7003A34 for 132 bytes
04:32:55: ISAKMP: Packet hash:
64218CC0: D1202D99 2BB49D38 Q -.+4.8
64218CD0: B8FBB1BE 7CDC67D7 4E26126C 63 8{1>|\gWN&.lc
04:32:55: ISAKMP (0:13): processing HASH payload. message ID = 0
04:32:55: ISAKMP:received payload type 17
04:32:55: ISAKMP (0:13): Detected NAT-D payload
04:32:55: ISAKMP (0:13): recalc my hash for NAT-D
04:32:55: ISAKMP (0:13): NAT match MINE hash
04:32:55: ISAKMP:received payload type 17
04:32:55: ISAKMP (0:13): Detected NAT-D payload
04:32:55: ISAKMP (0:13): recalc his hash for NAT-D
04:32:55: ISAKMP (0:13): NAT match HIS hash
04:32:55: ISAKMP (0:13): processing NOTIFY INITIAL_CONTACT protocol 1
 spi 0, message ID = 0, sa = 6482B354
04:32:55: ISAKMP (0:13): Process initial contact,
bring down existing phase 1 and 2 SA's with local 172.16.1.1 remote 10.1.1.1 remote port
500
04:32:55: ISAKMP (0:13): returning IP addr to the address pool
04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 05D315C5
04:32:55: ISAKMP cookie gen for src 172.16.1.1 dst 10.1.1.1
04:32:55: ISAKMP cookie 3123100B 041A85A6
04:32:55: ISAKMP (0:13): SA has been authenticated with 10.1.1.1
04:32:55: ISAKMP: Trying to insert a peer 172.16.1.1/10.1.1.1/500/, and inserted
successfully.
04:32:55: ISAKMP: set new node -803402627 to CONF_XAUTH
04:32:55: IPSEC(key_engine): got a queue event...
04:32:55: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R) QM_IDLE
04:32:55: ISAKMP (0:13): purging node -803402627
04:32:55: ISAKMP: Sending phase 1 responder lifetime 86400

04:32:55: ISAKMP (0:13): Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH

```

```

04:32:55: ISAKMP (0:13): Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE

04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.168.1.1
04:32:55: ISAKMP cookie AA8F7B41 25EEF256
04:32:55: ISAKMP: isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:32:55: crawler my_cookie AA8F7B41 F7ACF384
04:32:55: crawler his_cookie E46E088D F227FE4D
04:32:55: ISAKMP (0:13): Need XAUTH
04:32:55: ISAKMP (0:13): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
04:32:55: ISAKMP (0:13): Old State = IKE_P1_COMPLETE New State =
IKE_XAUTH_AAA_START_LOGIN_AWAIT

04:32:55: ISAKMP cookie gen for src 10.1.1.1 dst 172.16.1.1
04:32:55: ISAKMP cookie AA8F7B41 2CCFA491
04:32:55: ISAKMP: isadb_post_process_list: crawler: B 27FF 12 (6482B354)
04:32:55: crawler my_cookie AA8F7B41 F7ACF384
04:32:55: crawler his_cookie E46E088D F227FE4D
04:32:55: ISAKMP: got callback 1
04:32:55: ISAKMP: set new node -1447732198 to CONF_XAUTH
04:32:55: ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2
04:32:55: ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2
04:32:55: ISAKMP (0:13): initiating peer config to 10.1.1.1. ID = -1447732198
04:32:55: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R)
CONF_XAUTH
04:32:55: ISAKMP (0:13): Input = IKE_MSG_FROM_AAA, IKE_AAA_START_LOGIN
04:32:55: ISAKMP (0:13): Old State = IKE_XAUTH_AAA_START_LOGIN_AWAIT New State =
IKE_XAUTH_REQ_SENT

04:33:00: ISAKMP (0:13): retransmitting phase 2 CONF_XAUTH -1447732198 ...
04:33:00: ISAKMP (0:13): incrementing error counter on sa: retransmit phase 2
04:33:00: ISAKMP (0:13): incrementing error counter on sa: retransmit phase 2
04:33:00: ISAKMP (0:13): retransmitting phase 2 -1447732198 CONF_XAUTH
04:33:00: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R)
CONF_XAUTH

04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 124D4618
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 B0C91917
04:33:03: ISAKMP: isadb_post_process_list: crawler: B 27FF 2 (6482B354)
04:33:03: crawler my_cookie AA8F7B41 F7ACF384
04:33:03: crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 0E294692
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 091A7695
04:33:03: ISAKMP: isadb_post_process_list: crawler: B 27FF 2 (6482B354)
04:33:03: crawler my_cookie AA8F7B41 F7ACF384
04:33:03: crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R)
CONF_XAUTH
04:33:03: ISAKMP: hash from 7292D74 for 92 bytes
04:33:03: ISAKMP: Packet hash:
64218CC0: 84A1AF24 5D92B116 .!/$}.1.
64218CD0: FC2C6252 A472C5F8 152AC860 63 |,bR$rEx.*H`c
04:33:03: ISAKMP (0:13): processing transaction payload from 11.1.1.1. message ID =
-1447732198
04:33:03: ISAKMP: Config payload REPLY
04:33:03: ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2
04:33:03: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2
04:33:03: ISAKMP (0:13): deleting node -1447732198 error FALSE reason "done with xauth
request/reply exchange"
04:33:03: ISAKMP (0:13): Input = IKE_MSG_FROM_PEER, IKE_CFG_REPLY
04:33:03: ISAKMP (0:13): Old State = IKE_XAUTH_REQ_SENT New State =
IKE_XAUTH_AAA_CONT_LOGIN_AWAIT

```

```

04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 A1B3E684
04:33:03: ISAKMP: isadb_post_process_list: crawler: B 27FF 12 (6482B354)
04:33:03: crawler my_cookie AA8F7B41 F7ACF384
04:33:03: crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP: got callback 1
04:33:03: ISAKMP: set new node 524716665 to CONF_XAUTH
04:33:03: ISAKMP (0:13): initiating peer config to 10.1.1.1. ID = 524716665
04:33:03: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R)
CONF_XAUTH
04:33:03: ISAKMP (0:13): Input = IKE_MSG_FROM_AAA, IKE_AAA_CONT_LOGIN
04:33:03: ISAKMP (0:13): Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT New State =
IKE_XAUTH_SET_SENT
04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 5C83A09D
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 2BEBEFD4
04:33:03: ISAKMP: isadb_post_process_list: crawler: B 27FF 2 (6482B354)
04:33:03: crawler my_cookie AA8F7B41 F7ACF384
04:33:03: crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B DA00A46B
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 FDD27773
04:33:03: ISAKMP: isadb_post_process_list: crawler: B 27FF 2 (6482B354)
04:33:03: crawler my_cookie AA8F7B41 F7ACF384
04:33:03: crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R)
CONF_XAUTH
04:33:03: ISAKMP: hash from 7292A34 for 68 bytes
04:33:03: ISAKMP: Packet hash:
64218CC0: 5034B99E B8BA531F P49.8:S.
64218CD0: 6267B8BD F3006989 DC118796 63 bg8=s.i.\...c
04:33:03: ISAKMP (0:13): processing transaction payload from 11.1.1.1. message ID =
524716665
04:33:03: ISAKMP: Config payload ACK
04:33:03: ISAKMP (0:13): XAUTH ACK Processed
04:33:03: ISAKMP (0:13): deleting node 524716665 error FALSE reason "done with
transaction"
04:33:03: ISAKMP (0:13): Input = IKE_MSG_FROM_PEER, IKE_CFG_ACK
04:33:03: ISAKMP (0:13): Old State = IKE_XAUTH_SET_SENT New State = IKE_P1_COMPLETE

04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 E0BB50E9
04:33:03: ISAKMP: isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:03: crawler my_cookie AA8F7B41 F7ACF384
04:33:03: crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP (0:13): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
04:33:03: ISAKMP (0:13): Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 7794EF6E
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 C035AAE5
04:33:03: ISAKMP: isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:03: crawler my_cookie AA8F7B41 F7ACF384
04:33:03: crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B F1FCC25A
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 31744F44
04:33:03: ISAKMP: isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:03: crawler my_cookie AA8F7B41 F7ACF384

```



```

04:33:03: crawler his_cookie E46E088D F207FE4D
04:33:03: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R)
QM_IDLE
04:33:03: ISAKMP: set new node -1639992295 to QM_IDLE
04:33:03: ISAKMP: hash from 7293A74 for 100 bytes
04:33:03: ISAKMP: Packet hash:
64218CC0: 9D7DF4DF FE3A6403 .)t_~:d.
64218CD0: 3F1D1C59 C5D138CE 50289B79 07 ?..YEQ8NP(.y.
04:33:03: ISAKMP (0:13): processing transaction payload from 10.1.1.1. message ID =
-1639992295
04:33:03: ISAKMP: Config payload REQUEST
04:33:03: ISAKMP (0:13): checking request:
04:33:03: ISAKMP: IP4_ADDRESS
04:33:03: ISAKMP: IP4_NETMASK
04:33:03: ISAKMP: IP4_DNS
04:33:03: ISAKMP: IP4_DNS
04:33:03: ISAKMP: IP4_NBNS
04:33:03: ISAKMP: IP4_NBNS
04:33:03: ISAKMP: SPLIT_INCLUDE
04:33:03: ISAKMP: DEFAULT_DOMAIN
04:33:03: ISAKMP (0:13): Input = IKE_MESG_FROM_PEER, IKE_CFG_REQUEST
04:33:03: ISAKMP (0:13): Old State = IKE_P1_COMPLETE New State =
IKE_CONFIG_AUTHOR_AAA_AWAIT

04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 B02E0D67
04:33:03: ISAKMP: isadb_post_process_list: crawler: C 27FF 12 (6482B354)
04:33:03: crawler my_cookie AA8F7B41 F7ACF384
04:33:03: crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP: got callback 1
04:33:03: ISAKMP (0:13): attributes sent in message:
04:33:03: Address: 10.2.0.0
04:33:03: ISAKMP (0:13): allocating address 10.4.1.4
04:33:03: ISAKMP: Sending private address: 10.4.1.4
04:33:03: ISAKMP: Sending DEFAULT_DOMAIN default domain name: vpn2.com
04:33:03: ISAKMP (0:13): responding to peer config from 10.1.1.1. ID = -1639992295
04:33:03: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R)
CONF_ADDR
04:33:03: ISAKMP (0:13): deleting node -1639992295 error FALSE reason ""
04:33:03: ISAKMP (0:13): Input = IKE_MESG_FROM_AAA, IKE_AAA_GROUP_ATTR
04:33:03: ISAKMP (0:13): Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New State =
IKE_P1_COMPLETE

04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 881D5411
04:33:03: ISAKMP cookie gen for src 11.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 6FD82541
04:33:03: ISAKMP: isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:03: crawler my_cookie AA8F7B41 F7ACF384
04:33:03: crawler his_cookie E46E088D F227FE4D
04:33:03: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:03: ISAKMP cookie 3123100B 8A94C1BE
04:33:03: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:03: ISAKMP cookie AA8F7B41 F3BA766D
04:33:03: ISAKMP: isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:03: crawler my_cookie AA8F7B41 F7ACF384
04:33:03: crawler his_cookie E46E088D F207FE4D
04:33:03: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R)
QM_IDLE
04:33:03: ISAKMP: set new node 17011691 to QM_IDLE
04:33:03: ISAKMP: hash from 70029F4 for 540 bytes
04:33:03: ISAKMP: Packet hash:
64218CC0: AFBA30B2 55F5BC2D /:02Uu<-
64218CD0: 3A86B1C9 00D2F5BA 77BF5589 07 :.1I.Ru:w?U..

```

```

04:33:03: ISAKMP (0:13): processing HASH payload. message ID = 17011691
04:33:03: ISAKMP (0:13): processing SA payload. message ID = 17011691
04:33:03: ISAKMP (0:13): Checking IPSec proposal 1
04:33:03: ISAKMP: transform 1, ESP_3DES
04:33:03: ISAKMP: attributes in transform:
04:33:03: ISAKMP: encaps is 1
04:33:03: ISAKMP: SA life type in seconds
04:33:03: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
04:33:03: ISAKMP: SA life type in kilobytes
04:33:03: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
04:33:03: ISAKMP: authenticator is HMAC-SHA
04:33:03: ISAKMP (0:13): atts are acceptable.
04:33:03: IPSEC(validate_proposal_request): proposal part #1,
 (key eng. msg.) INBOUND local= 172.18.1.1, remote= 10.1.1.1,
 local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
 remote_proxy= 10.4.1.4/255.255.255.255/0/0 (type=1),
 protocol= ESP, transform= esp-3des esp-sha-hmac ,
 lifedur= 0s and 0kb,
 spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
04:33:03: IPSEC(kei_proxy): head = ra, map->ivrf = vpn1, kei->ivrf = vpn2
04:33:03: IPSEC(kei_proxy): head = ra, map->ivrf = vpn2, kei->ivrf = vpn2
04:33:03: IPSEC(validate_transform_proposal): transform proposal not supported for
identity:
 {esp-3des esp-sha-hmac }
04:33:03: ISAKMP (0:13): IPSec policy invalidated proposal
04:33:03: ISAKMP (0:13): Checking IPSec proposal 2
04:33:03: ISAKMP: transform 1, ESP_3DES
04:33:03: ISAKMP: attributes in transform:
04:33:03: ISAKMP: encaps is 1
04:33:03: ISAKMP: SA life type in seconds
04:33:03: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
04:33:03: ISAKMP: SA life type in kilobytes
04:33:03: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
04:33:03: ISAKMP: authenticator is HMAC-MD5
04:33:03: ISAKMP (0:13): atts are acceptable.
04:33:03: IPSEC(validate_proposal_request): proposal part #1,
 (key eng. msg.) INBOUND local= 172.18.1.1, remote= 10.1.1.1,
 local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
 remote_proxy= 10.4.1.4/255.255.255.255/0/0 (type=1),
 protocol= ESP, transform= esp-3des esp-md5-hmac ,
 lifedur= 0s and 0kb,
 spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
04:33:03: IPSEC(kei_proxy): head = ra, map->ivrf = vpn1, kei->ivrf = vpn2
04:33:03: IPSEC(kei_proxy): head = ra, map->ivrf = vpn2, kei->ivrf = vpn2
04:33:03: ISAKMP (0:13): processing NONCE payload. message ID = 17011691
04:33:03: ISAKMP (0:13): processing ID payload. message ID = 17011691
04:33:03: ISAKMP (0:13): processing ID payload. message ID = 17011691
04:33:03: ISAKMP (0:13): asking for 1 spis from ipsec
04:33:03: ISAKMP (0:13): Node 17011691, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
04:33:03: ISAKMP (0:13): Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE
04:33:03: IPSEC(key_engine): got a queue event...
04:33:03: IPSEC(spi_response): getting spi 2749516541 for SA
 from 172.18.1.1 to 10.1.1.1 for prot 3
04:33:03: ISAKMP: received ke message (2/1)
04:33:04: ISAKMP (13): ID payload
 next-payload : 5
 type : 1
 addr : 10.4.1.4
 protocol : 0
 port : 0
04:33:04: ISAKMP (13): ID payload
 next-payload : 11
 type : 4
 addr : 0.0.0.0

```

```

 protocol : 0
 port : 0
04:33:04: ISAKMP (0:13): sending packet to 10.1.1.1 my_port 500 peer_port 500 (R) QM_IDLE
04:33:04: ISAKMP (0:13): Node 17011691, Input = IKE_MSG_FROM_IPSEC, IKE_SPI_REPLY
04:33:04: ISAKMP (0:13): Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2
04:33:04: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:04: ISAKMP cookie 3123100B 93DE46D2
04:33:04: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:04: ISAKMP cookie AA8F7B41 088A0A16
04:33:04: ISAKMP: isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:04: crawler my_cookie AA8F7B41 F7ACF384
04:33:04: crawler his_cookie E46E088D F227FE4D
04:33:04: ISAKMP cookie gen for src 172.18.1.1 dst 10.1.1.1
04:33:04: ISAKMP cookie 3123100B A8F23F73
04:33:04: ISAKMP cookie gen for src 10.1.1.1 dst 172.18.1.1
04:33:04: ISAKMP cookie AA8F7B41 93D8D879
04:33:04: ISAKMP: isadb_post_process_list: crawler: 9 27FF 2 (6482B354)
04:33:04: crawler my_cookie AA8F7B41 F7ACF384
04:33:04: crawler his_cookie E46E088D F227FE4D
04:33:04: ISAKMP (0:13): received packet from 10.1.1.1 dport 500 sport 500 Global (R)
QM_IDLE
04:33:04: ISAKMP: hash from 7290DB4 for 60 bytes
04:33:04: ISAKMP: Packet hash:
64218CC0: 4BB45A92 7181A2F8 K4Z.q."x
64218CD0: 73CC12F8 091875C0 054F77CD 63 sL.x..u@.OwMc
04:33:04: ISAKMP: Locking peer struct 0x640BBB18, IPSEC refcount 1 for for stuff_ke
04:33:04: ISAKMP (0:13): Creating IPsec SAs
04:33:04: inbound SA from 10.1.1.1 to 172.18.1.1 (f/i) 0/ 2
 (proxy 10.4.1.4 to 0.0.0.0)
04:33:04: has spi 0xA3E24AFD and conn_id 5127 and flags 2
04:33:04: lifetime of 2147483 seconds
04:33:04: lifetime of 4608000 kilobytes
04:33:04: has client flags 0x0
04:33:04: outbound SA from 172.18.1.1 to 10.1.1.1 (f/i) 0/ 2 (proxy
0.0.0.0 to 10.4.1.4)
04:33:04: has spi 1343294712 and conn_id 5128 and flags A
04:33:04: lifetime of 2147483 seconds
04:33:04: lifetime of 4608000 kilobytes
04:33:04: has client flags 0x0
04:33:04: ISAKMP (0:13): deleting node 17011691 error FALSE reason "quick mode done
(await)"
04:33:04: ISAKMP (0:13): Node 17011691, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
04:33:04: ISAKMP (0:13): Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE
04:33:04: IPSEC(key_engine): got a queue event...
04:33:04: IPSEC(initialize_sas): ,
 (key eng. msg.) INBOUND local= 172.18.1.1, remote= 10.1.1.1,
 local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
 remote_proxy= 10.4.1.4/0.0.0.0/0/0 (type=1),
 protocol= ESP, transform= esp-3des esp-md5-hmac ,
 lifedur= 2147483s and 4608000kb,
 spi= 0xA3E24AFD(2749516541), conn_id= 5127, keysize= 0, flags= 0x2
04:33:04: IPSEC(initialize_sas): ,
 (key eng. msg.) OUTBOUND local= 172.18.1.1, remote= 10.1.1.1,
 local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
 remote_proxy= 10.4.1.4/0.0.0.0/0/0 (type=1),
 protocol= ESP, transform= esp-3des esp-md5-hmac ,
 lifedur= 2147483s and 4608000kb,
 spi= 0x50110CF8(1343294712), conn_id= 5128, keysize= 0, flags= 0xA
04:33:04: IPSEC(kei_proxy): head = ra, map->ivrf = vpn1, kei->ivrf = vpn2
04:33:04: IPSEC(kei_proxy): head = ra, map->ivrf = vpn2, kei->ivrf = vpn2
04:33:04: IPSEC(rte_mgr): VPN Route Added 10.4.1.4 255.255.255.255 via 10.1.1.1 in vpn2
04:33:04: IPSEC(add mtree): src 0.0.0.0, dest 10.4.1.4, dest_port 0

04:33:04: IPSEC(create_sa): sa created,

```

```
(sa) sa_dest= 172.18.1.1, sa_prot= 50,
 sa_spi= 0xA3E24AFD(2749516541),
 sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 5127
04:33:04: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.1.1.1, sa_prot= 50,
 sa_spi= 0x50110CF8(1343294712),
 sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 5128
04:33:53: ISAKMP (0:13): purging node -1639992295
04:33:54: ISAKMP (0:13): purging node 17011691
```

## Configuration Examples for VRF-Aware IPSec

The following examples show how to configure VRF-Aware IPSec:

- [Static IPSec-to-MPLS VPN Example, page 22](#)
- [IPSec-to-MPLS VPN Using RSA Encryption Example, page 24](#)
- [IPSec-to-MPLS VPN with RSA Signatures Example, page 25](#)
- [Upgrade from Previous Versions of the Cisco Network-Based IPSec VPN Solution, page 28](#)

### Static IPSec-to-MPLS VPN Example

The following sample shows a static configuration that maps IPSec tunnels to MPLS VPNs. The configurations map IPSec tunnels to MPLS VPNs “VPN1” and “VPN2.” Both of the IPSec tunnels terminate on a single public-facing interface.

#### IPSec PE Configuration

```
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
ip vrf vpn2
 rd 101:1
 route-target export 101:1
 route-target import 101:1
!
crypto keyring vpn1
 pre-shared-key address 172.16.1.1 key vpn1
crypto keyring vpn2
 pre-shared-key address 10.1.1.1 key vpn2
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp profile vpn1
 vrf vpn1
 keyring vpn1
 match identity address 172.16.1.1 255.255.255.255
!
crypto isakmp profile vpn2
 vrf vpn2
 keyring vpn2
 match identity address 10.1.1.1 255.255.255.255
!
```

```

crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
crypto ipsec transform-set vpn2 esp-3des esp-md5-hmac
!
crypto map crypmap 1 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set vpn1
 set isakmp-profile vpn1
 match address 101
crypto map crypmap 3 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set vpn2
 set isakmp-profile vpn2
 match address 102
!
interface Ethernet1/1
 ip address 172.17.1.1 255.255.0.0
 tag-switching ip
!
interface Ethernet1/2
 ip address 172.18.1.1 255.255.255.0
 crypto map crypmap
!
ip route 172.16.1.1 255.255.255.255 172.168.1.2
ip route 10.1.1.1 255.255.255.255 172.18.1.2
ip route vrf vpn1 10.2.0.0 255.255.0.0 172.18.1.2 global
ip route vrf vpn2 10.2.0.0 255.255.0.0 172.18.1.2 global
!
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
access-list 102 permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255

```

### IPSec Customer Provided Edge (CPE) Configuration for VPN1

```

crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key vpn1 address 172.18.1.1
!
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
crypto map vpn1 1 ipsec-isakmp
 set peer 172.18.1.1
 set transform-set vpn1
 match address 101
!
interface FastEthernet1/0
 ip address 172.16.1.1 255.255.255.0
 crypto map vpn1
!
interface FastEthernet1/1
 ip address 10.2.1.1 255.255.0.0
!
access-list 101 permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!

```

### IPSec CPE Configuration for VPN2

```

crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp key vpn2 address 172.18.1.1

```

```

!
!
crypto ipsec transform-set vpn2 esp-3des esp-md5-hmac
!
crypto map vpn2 1 ipsec-isakmp
 set peer 172.18.1.1
 set transform-set vpn2
 match address 101
!
interface FastEthernet0
 ip address 10.1.1.1 255.255.255.0
 crypto map vpn2
!
interface FastEthernet1
 ip address 10.2.1.1 255.255.0.0
!
access-list 101 permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255

```

## IPSec-to-MPLS VPN Using RSA Encryption Example

The following example shows an IPSec-to-MPLS configuration using RSA encryption:

### PE Router Configuration

```

ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
crypto isakmp policy 10
 authentication rsa-encr
!
crypto keyring vpn1
 rsa-publickey address 172.16.1.1 encryption
 key-string
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00DBF381 00DDECC8
 DC4AA490 40320C52 9912D876 EB36717C 63DCA95C 7E5EC02A 84F276CE 292B42D7
 D664F324 3726F4E0 39D33093 ECB81B95 482511A5 F064C4B3 D5020301 0001
 quit
!
crypto isakmp profile vpn1
 vrf vpn1
 keyring vpn1
 match identity address 172.16.1.1 255.255.255.255
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
crypto map crypmap 1 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set vpn1
 set isakmp-profile vpn1
 match address 101
!
interface Ethernet1/1
 ip address 172.17.1.1 255.255.0.0
 tag-switching ip
!
interface Ethernet1/2
 ip address 172.18.1.1 255.255.255.0
 crypto map crypmap
!
ip route 172.16.1.1 255.255.255.255 172.18.1.2

```

```
ip route vrf vpn1 10.2.0.0 255.255.0.0 172.18.1.2 global
!
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
```

### IPSec CPE Configuration for VPN1

```
crypto isakmp policy 10
 authentication rsa-encr
!
crypto key pubkey-chain rsa
 addressed-key 172.18.1.1 encryption
 key-string
 3082011B 300D0609 2A864886 F70D0101 01050003 82010800 30820103 0281FB00
 C90CC78A 6002BDBA 24683396 B7D7877C 16D08C47 E00C3C10 63CF13BC 4E09EA23
 92EB8A48 4113F5A4 8796C8BE AD7E2DC1 3B0742B6 7118CE7C 1B0E21D1 AA9724A4
 4D74FCEA 562FF225 A2B11F18 E53C4415 61C3B741 3A06E75D B4F9102D 6163EE40
 16C68FD7 6532F660 97B59118 9C8DE3E5 4E2F2925 BBB87FCB 95223D4E A5E362DB
 215CB35C 260080805 17BBE1EF C3050E13 031F3D5B 5C22D16C FC8B1EC5 074F07A5
 D050EC80 7890D9C5 EC20D6F0 173FE2BA 89F5B5F9 2EADC9A6 D461921E 3D5B60016
 ABB8B6B9 E2124A21 93F0E4AE B487461B E7F1F1C4 032A0B0E 80DC3E15 CB268EC9
 5D76B9BD 3C78CB75 CE9F68C6 484D6573 CBC3EB59 4B5F3999 8F9D0203 010001
 quit
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
crypto map vpn1 1 ipsec-isakmp
 set peer 172.18.1.1
 set transform-set vpn1
 match address 101
!
interface FastEthernet1/0
 ip address 172.16.1.1 255.255.255.0
 crypto map vpn1
!
interface FastEthernet1/1
 ip address 10.2.1.1 255.255.0.0
!
access-list 101 permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!
```

## IPSec-to-MPLS VPN with RSA Signatures Example

The following shows an IPSec-to-MPLS VPN configuration using RSA signatures:

### PE Router Configuration

```
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
crypto ca trustpoint bombo
 enrollment url http://172.31.68.59:80
 crl optional
!
crypto ca certificate chain bombo
 certificate 03C0
 308203BF 308202A7 A0030201 02020203 C0300D06 092A8648 86F70D01 01050500
 . . .
 quit
 certificate ca 01
 30820379 30820261 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
```

```

. . .
quit
!
crypto isakmp profile vpn1
 vrf vpn1
 ca trust-point bombo
 match identity address 172.16.1.1 255.255.255.255
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
crypto map crypmap 1 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set vpn1
 set isakmp-profile vpn1
 match address 101
!
interface Ethernet1/1
 ip address 172.31.1.1 255.255.0.0
 tag-switching ip
!
interface Ethernet1/2
 ip address 172.18.1.1 255.255.255.0
 crypto map crypmap
!
ip route 172.16.1.1 255.255.255.255 172.18.1.2
ip route vrf vpn1 10.2.0.0 255.255.0.0 172.18.1.2 global
!
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
!

```

### IPSec CPE Configuration for VPN1

```

crypto ca trustpoint bombo
 enrollment url http://172.31.68.59:80
 crl optional
!
crypto ca certificate chain bombo
 certificate 03BF
 308203BD 308202A5 A0030201 02020203 BF300D06 092A8648 86F70D01 01050500
 . . .
 quit
 certificate ca 01
 30820379 30820261 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
 . . .
 quit
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
crypto map vpn1 1 ipsec-isakmp
 set peer 172.18.1.1
 set transform-set vpn1
 match address 101
!
interface FastEthernet1/0
 ip address 172.16.1.1 255.255.255.0
 crypto map vpn1
!
interface FastEthernet1/1
 ip address 10.2.1.1 255.255.0.0
!
access-list 101 permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!

```



## IPSec Remote Access-to-MPLS VPN Example

The following shows an IPSec remote access-to-MPLS VPN configuration. The configuration maps IPSec tunnels to MPLS VPNs. The IPSec tunnels terminate on a single public-facing interface.

### PE Router Configuration

```

aaa new-model
!
aaa group server radius vpn1
 server-private 10.1.1.1 auth-port 1645 acct-port 1646 timeout 5 retransmit 3 key vpn1
!
aaa group server radius vpn2
 server-private 10.1.1.1 auth-port 1645 acct-port 1646 timeout 5 retransmit 3 key vpn2
!
aaa authorization network aaa-list group radius
!
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
ip vrf vpn2
 rd 101:1
 route-target export 101:1
 route-target import 101:1
!
crypto isakmp profile vpn1-ra
 vrf vpn1
 match identity group vpn1-ra
 client authentication list vpn1
 isakmp authorization list aaa-list
 client configuration address initiate
 client configuration address respond
crypto isakmp profile vpn2-ra
 vrf vpn2
 match identity group vpn2-ra
 client authentication list vpn2
 isakmp authorization list aaa-list
 client configuration address initiate
 client configuration address respond
!
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
crypto ipsec transform-set vpn2 esp-3des esp-md5-hmac
!
crypto dynamic-map vpn1 1
 set transform-set vpn1
 set isakmp-profile vpn1-ra
 reverse-route
!
crypto dynamic-map vpn2 1
 set transform-set vpn2
 set isakmp-profile vpn2-ra
 reverse-route
!
!
crypto map ra 1 ipsec-isakmp dynamic vpn1
crypto map ra 2 ipsec-isakmp dynamic vpn2
!
interface Ethernet1/1
 ip address 172.17.1.1 255.255.0.0
 tag-switching ip

```

```

!
interface Ethernet1/2
 ip address 172.18.1.1 255.255.255.0
 crypto map ra
!
ip local pool vpn1-ra 10.4.1.1 10.4.1.254 group vpn1-ra
ip local pool vpn2-ra 10.4.1.1 10.4.1.254 group vpn2-ra
!

```

## Upgrade from Previous Versions of the Cisco Network-Based IPSec VPN Solution

The VRF-Aware IPSec feature in the Cisco network-based IPSec VPN solution release 1.5 requires that you change your existing configurations.

The sample configurations that follow indicate the changes you must make to your existing configurations. These samples include the following:

- [Site-to-Site Configuration Upgrade, page 28](#)
- [Remote Access Configuration Upgrade, page 29](#)
- [Combination Site-to-Site and Remote Access Configuration Upgrade, page 31](#)

### Site-to-Site Configuration Upgrade

The following configurations show the changes that are necessary for a site-to-site configuration upgrade from a previous version of the network-based IPSec VPN solution to the Cisco network-based IPSec VPN solution release 1.5:

#### Previous Version Site-to-Site Configuration

```

crypto isakmp key VPN1 address 172.21.25.74
crypto isakmp key VPN2 address 172.21.21.74
!
crypto ipsec transform-set VPN1 esp-des esp-sha-hmac
crypto ipsec transform-set VPN2 esp-3des esp-sha-hmac
!
crypto map VPN1 10 ipsec-isakmp
 set peer 172.21.25.74
 set transform-set VPN1
 match address 101
!
crypto map VPN2 10 ipsec-isakmp
 set peer 172.21.21.74
 set transform-set VPN2
 match address 102
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding VPN1
 ip address 172.21.25.73 255.255.255.0
 crypto map VPN1
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2 native
 ip vrf forwarding VPN2
 ip address 172.21.21.74 255.255.255.0
 crypto map VPN2

```

## New Version Site-to-Site Configuration

The following is an upgraded version of the same site-to-site configuration to the Cisco network-based IPSec VPN solution release 1.5 solution:



### Note

You must change to keyrings. The VRF-Aware IPSec feature requires that keys be associated with a VRF if the IKE local endpoint is in the VRF.

```
crypto keyring VPN1-KEYS vrf VPN1
 pre-shared-key address 172.21.25.74 key VPN1
!
crypto keyring VPN2-KEYS vrf VPN2
 pre-shared-key address 172.21.21.74 key VPN2
!
crypto ipsec transform-set VPN1 esp-des esp-sha-hmac
crypto ipsec transform-set VPN2 esp-3des esp-sha-hmac
!
crypto map VPN1 10 ipsec-isakmp
 set peer 172.21.25.74
 set transform-set VPN1
 match address 101
!
crypto map VPN2 10 ipsec-isakmp
 set peer 172.21.21.74
 set transform-set VPN2
 match address 102
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding VPN1
 ip address 172.21.25.73 255.255.255.0
 crypto map VPN1
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2 native
 ip vrf forwarding VPN2
 ip address 172.21.21.74 255.255.255.0
 crypto map VPN2
```

## Remote Access Configuration Upgrade

The following configurations show the changes that are necessary for a remote access configuration upgrade from a previous version of the network-based IPSec VPN solution to the Cisco network-based IPSec VPN solution release 1.5:

### Previous Version Remote Access Configuration

```
crypto isakmp client configuration group VPN1-RA-GROUP
 key VPN1-RA
 pool VPN1-RA
!
crypto isakmp client configuration group VPN2-RA-GROUP
 key VPN2-RA
 pool VPN2-RA
!
crypto ipsec transform-set VPN1-RA esp-3des esp-sha-hmac
crypto ipsec transform-set VPN2-RA esp-3des esp-md5-hmac
!
crypto dynamic-map VPN1-RA 1
```

```

 set transform-set VPN1-RA
reverse-route
!
crypto dynamic-map VPN2-RA 1
set transform-set VPN2-RA
reverse-route
!
!
crypto map VPN1 client authentication list VPN1-RA-LIST
crypto map VPN1 isakmp authorization list VPN1-RA-LIST
crypto map VPN1 client configuration address initiate
crypto map VPN1 client configuration address respond
crypto map VPN1 10 ipsec-isakmp dynamic VPN1-RA
!
crypto map VPN2 client authentication list VPN2-RA-LIST
crypto map VPN2 isakmp authorization list VPN2-RA-LIST
crypto map VPN2 client configuration address initiate
crypto map VPN2 client configuration address respond
crypto map VPN2 10 ipsec-isakmp dynamic VPN2-RA
!
interface FastEthernet0/0.1
encapsulation dot1Q 1 native
ip vrf forwarding VPN1
ip address 172.21.25.73 255.255.255.0
crypto map VPN1
!
interface FastEthernet0/0.2
encapsulation dot1Q 2 native
ip vrf forwarding VPN2
ip address 172.21.21.74 255.255.255.0
crypto map VPN2

```

## New Version Remote Access Configuration

In the following instance, there is no upgrade; it is recommended that you change to the following configuration:

```

crypto isakmp client configuration group VPN1-RA-GROUP
key VPN1-RA
pool VPN1-RA
!
crypto isakmp client configuration group VPN2-RA-GROUP
key VPN2-RA
pool VPN2-RA
!
crypto isakmp profile VPN1-RA
match identity group VPN1-RA-GROUP
client authentication list VPN1-RA-LIST
isakmp authorization list VPN1-RA-LIST
client configuration address initiate
client configuration address respond
!
crypto isakmp profile VPN2-RA
match identity group VPN2-RA-GROUP
client authentication list VPN2-RA-LIST
isakmp authorization list VPN2-RA-LIST
client configuration address initiate
client configuration address respond
!
crypto ipsec transform-set VPN1-RA esp-3des esp-sha-hmac
crypto ipsec transform-set VPN2-RA esp-3des esp-md5-hmac
!
crypto dynamic-map VPN1-RA 1

```

```

set transform-set VPN1-RA
set isakmp-profile VPN1-RA
reverse-route
!
crypto dynamic-map VPN2-RA 1
set transform-set VPN2-RA
set isakmp-profile VPN2-RA
reverse-route
!
crypto map VPN1 10 ipsec-isakmp dynamic VPN1-RA
!
crypto map VPN2 10 ipsec-isakmp dynamic VPN2-RA
!
interface FastEthernet0/0.1
encapsulation dot1Q 1 native
ip vrf forwarding VPN1
ip address 172.21.25.73 255.255.255.0
crypto map VPN1
!
interface FastEthernet0/0.2
encapsulation dot1Q 2 native
ip vrf forwarding VPN2
ip address 172.21.21.74 255.255.255.0
crypto map VPN2

```

## Combination Site-to-Site and Remote Access Configuration Upgrade

The following configurations show the changes that are necessary for a site-to-site and remote access configuration upgrade from a previous version of the network-based IPSec VPN solution to the Cisco network-based IPSec VPN solution release 1.5:

### Previous Version Site-to-Site and Remote Access Configuration

```

crypto isakmp key VPN1 address 172.21.25.74 no-xauth
crypto isakmp key VPN2 address 172.21.21.74 no-xauth
!
crypto isakmp client configuration group VPN1-RA-GROUP
key VPN1-RA
pool VPN1-RA
!
crypto isakmp client configuration group VPN2-RA-GROUP
key VPN2-RA
pool VPN2-RA
!
crypto ipsec transform-set VPN1 esp-des esp-sha-hmac
crypto ipsec transform-set VPN2 esp-3des esp-sha-hmac
!
crypto ipsec transform-set VPN1-RA esp-3des esp-sha-hmac
crypto ipsec transform-set VPN2-RA esp-3des esp-md5-hmac
!
crypto dynamic-map VPN1-RA 1
set transform-set VPN1-RA
reverse-route
!
crypto dynamic-map VPN2-RA 1
set transform-set VPN2-RA
reverse-route
!
crypto map VPN1 client authentication list VPN1-RA-LIST
crypto map VPN1 isakmp authorization list VPN1-RA-LIST
crypto map VPN1 client configuration address initiate

```

```

crypto map VPN1 client configuration address respond
crypto map VPN1 10 ipsec-isakmp
set peer 172.21.25.74
set transform-set VPN1
match address 101
crypto map VPN1 20 ipsec-isakmp dynamic VPN1-RA
!
crypto map VPN2 client authentication list VPN2-RA-LIST
crypto map VPN2 isakmp authorization list VPN2-RA-LIST
crypto map VPN2 client configuration address initiate
crypto map VPN2 client configuration address respond
crypto map VPN2 10 ipsec-isakmp
set peer 172.21.21.74
set transform-set VPN2
match address 102
crypto map VPN2 20 ipsec-isakmp dynamic VPN2-RA
!
interface FastEthernet0/0.1
encapsulation dot1Q 1 native
ip vrf forwarding VPN1
ip address 172.21.25.73 255.255.255.0
crypto map VPN1
!
interface FastEthernet0/0.2
encapsulation dot1Q 2 native
ip vrf forwarding VPN2
ip address 172.21.21.74 255.255.255.0
crypto map VPN2

```

## New Version Site-to-Site and Remote Access Configuration

You must upgrade to this configuration:



### Note

For site-to-site configurations that do not require XAUTH, configure an ISAKMP profile without XAUTH configuration. For remote access configurations that require XAUTH, configure an ISAKMP profile with XAUTH.

```

crypto keyring VPN1-KEYS vrf VPN1
pre-shared-key address 172.21.25.74 key VPN1
!
crypto keyring VPN2-KEYS vrf VPN2
pre-shared-key address 172.21.21.74 key VPN2
!
crypto isakmp client configuration group VPN1-RA-GROUP
key VPN1-RA
pool VPN1-RA
!
crypto isakmp client configuration group VPN2-RA-GROUP
key VPN2-RA
pool VPN2-RA
!
crypto isakmp profile VPN1
keyring VPN1-KEYS
match identity address 172.21.25.74 VPN1
!
crypto isakmp profile VPN2
keyring VPN2-KEYS
match identity address 172.21.21.74 VPN2
!
crypto isakmp profile VPN1-RA

```

```
match identity group VPN1-RA-GROUP
client authentication list VPN1-RA-LIST
isakmp authorization list VPN1-RA-LIST
client configuration address initiate
client configuration address respond
!
crypto isakmp profile VPN2-RA
match identity group VPN2-RA-GROUP
client authentication list VPN2-RA-LIST
isakmp authorization list VPN2-RA-LIST
client configuration address initiate
client configuration address respond
!
crypto ipsec transform-set VPN1 esp-des esp-sha-hmac
crypto ipsec transform-set VPN2 esp-3des esp-sha-hmac
!
crypto ipsec transform-set VPN1-RA esp-3des esp-sha-hmac
crypto ipsec transform-set VPN2-RA esp-3des esp-md5-hmac
!
crypto dynamic-map VPN1-RA 1
set transform-set VPN1-RA
set isakmp-profile VPN1-RA
reverse-route
!
crypto dynamic-map VPN2-RA 1
set transform-set VPN2-RA
set isakmp-profile VPN2-RA
reverse-route
!
crypto map VPN1 10 ipsec-isakmp
set peer 172.21.25.74
set transform-set VPN1
set isakmp-profile VPN1
match address 101
crypto map VPN1 20 ipsec-isakmp dynamic VPN1-RA
!
crypto map VPN2 10 ipsec-isakmp
set peer 172.21.21.74
set transform-set VPN2
set isakmp-profile VPN2
match address 102
crypto map VPN2 20 ipsec-isakmp dynamic VPN2-RA
!
interface FastEthernet0/0.1
encapsulation dot1Q 1 native
ip vrf forwarding VPN1
ip address 172.21.25.73 255.255.255.0
crypto map VPN1
!
interface FastEthernet0/0.2
encapsulation dot1Q 2 native
ip vrf forwarding VPN2
ip address 172.21.21.74 255.255.255.0
crypto map VPN2
```

## Additional References

For additional information related to VRF-Aware IPSec, refer to the following references:

### Related Documents

| Related Topic                                           | Document Title                                                                                                      |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| IPSec configuration tasks                               | The chapter “Configuring Security for VPNs with IPSec” in the <i>Cisco IOS Security Configuration Guide</i>         |
| IPSec commands                                          | <i>Cisco IOS Security Command Reference</i>                                                                         |
| IKE Phase 1 and Phase 2, aggressive mode, and main mode | The chapter “Configuring Internet Key Exchange for IPSec VPNs” in the <i>Cisco IOS Security Configuration Guide</i> |
| IKE dead peer detection                                 | <i>Easy VPN Server</i>                                                                                              |

### Standards

| Standards <sup>1</sup>                                                                                                                | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |
|                                                                                                                                       |       |

1. Not all supported standards are listed.

### MIBs

| MIBs <sup>1</sup>                                                                                                                                                             | MIBs Link                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</li> </ul> | <p>To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:</p> <p><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></p> |

1. Not all supported MIBs are listed.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>



To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

## RFCs

| RFCs <sup>1</sup>                                                                                                           | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |
|                                                                                                                             |       |

1. Not all supported RFCs are listed.

## Technical Assistance

| Description                                                                                                                                                                                                                                                                         | Link                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module:

### New Commands

- **address**
- **ca trust-point**
- **client authentication list**
- **client configuration address**
- **crypto isakmp profile**
- **crypto keyring**
- **crypto map isakmp-profile**
- **initiate-mode**
- **isakmp authorization list**
- **keepalive (isakmp profile)**

- **keyring**
- **key-string**
- **match identity**
- **no crypto xauth**
- **pre-shared-key**
- **quit**
- **rsa-pubkey**
- **self-identity**
- **serial-number**
- **set isakmp-profile**
- **show crypto isakmp key**
- **show crypto isakmp profile**
- **vrf**

**Modified Commands**

- **clear crypto sa**
- **crypto isakmp peer**
- **crypto map isakmp-profile**
- **show crypto dynamic-map**
- **show crypto ipsec sa**
- **show crypto isakmp sa**
- **show crypto map (IPSec)**

For information about these commands, see the *Cisco IOS Security Command Reference* at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

# Glossary

**CA**—certification authority. CA is an entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.

**CLI**—command-line-interface. CLI is an interface that allows the user to interact with the operating system by entering commands and optional arguments. The UNIX operating system and DOS provide CLIs.

**client**—Corresponding IPSec IOS peer of the UUT in the Multi Protocol Label Switching (MPLS) network.

**dead peer**—IKE peer that is no longer reachable.

**DN**—Distinguished Name. A DN is the global, authoritative name of an entry in the Open System Interconnection (OSI Directory [X.500]).

**FQDN**—fully qualified domain name. A FQDN is the full name of a system rather than just its host name. For example, aldebaran is a host name, and aldebaran.interop.com is an FQDN.

**FR**—Frame Relay. FR is an industry-standard, switch-data-link-layer protocol that handles multiple virtual circuits using high-level data link (HDLC) encapsulation between connected devices. Frame Relay is more efficient than X.25, the protocol for which it generally is considered a replacement.

**FVRF**—Front Door Virtual Routing and Forwarding (VRF) repository. FVRF is the VRF used to route the encrypted packets to the peer.

**IDB**—Interface descriptor block. An IDB subblock is an area of memory that is private to an application. This area stores private information and states variables that an application wants to associate with an IDB or an interface. The application uses the IDB to register a pointer to its subblock, not to the contents of the subblock itself.

**IKE**—Internet Key Exchange. IKE establishes a shared security policy and authenticates keys for services (such as IPSec) that require keys. Before any IPSec traffic can be passed, each router, firewall, and host must verify the identity of its peer. This can be done by manually entering preshared keys into both hosts or by a CA service.

**IKE keepalive**—Bidirectional mechanism for determining the liveliness of an IKE peer.

**IPSec**—Security protocol for IP.

**IVRF**—Inside Virtual Routing and Forwarding. IVRF is the VRF of the plaintext packets.

**MPLS**—Multiprotocol Label Switching. MPLS is a switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

**RSA**—Rivest, Shamir, and Adelman are the inventors of the RSA technique. The RSA technique is a public-key cryptographic system that can be used for encryption and authentication.

**SA**—Security Association. SA is an instance of security policy and keying material applied to a data flow.

**VPN**—Virtual Private Network. A VPN enables IP traffic to travel securely over a public TCP or IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.

**VRF**—Virtual Route Forwarding. VRF is A VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

**XAUTH**—Extended authentication. XAUTH is an optional exchange between IKE Phase 1 and IKE Phase 2, in which the router demands additional authentication information in an attempt to authenticate the actual user (as opposed to authenticating the peer).

**Note**

Refer to the [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



# IPsec Usability Enhancements

---

**First Published: July 11, 2008**

**Last Updated: July 11, 2008**

The IPsec Usability Enhancements feature introduces functionality that eases the configuration and monitoring of your IPsec virtual private network (VPN). Benefits of this feature include intelligent defaults for IPsec and Internet Key Exchange (IKE) and the ability to easily verify and troubleshoot IPsec VPNs.

## **Finding Feature Information in This Module**

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for IPsec Usability Enhancements](#)” section on page 24.

## **Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images**

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for IPsec Usability Enhancements, page 2](#)
- [Information About IPsec Usability Enhancements, page 2](#)
- [How to Utilize IPsec Usability Enhancements, page 3](#)
- [Configuration Examples for IPsec Usability Enhancements, page 18](#)
- [Additional References, page 21](#)
- [Command Reference, page 23](#)
- [Feature Information for IPsec Usability Enhancements, page 24](#)



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

# Prerequisites for IPsec Usability Enhancements

- You must be familiar with IPsec, IKE, and encryption.
- You must have configured IPsec and enabled IKE on your router.
- You must be running Cisco IOS k9 crypto image on your router.

## Information About IPsec Usability Enhancements

To utilize the IPsec Usability Enhancements feature, you should understand the following concepts:

- [IPsec Overview, page 2](#)
- [IPsec Operation, page 2](#)

## IPsec Overview

IPsec is a framework of open standards developed by the Internet Engineering Task Force (IETF), which provides security for transmission of sensitive information over public networks. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (peers), such as Cisco routers.

IPsec provides secure tunnels between two peers. You may define which packets are considered sensitive and should be sent through these secure tunnels. You may also define the parameters that should be used to protect these sensitive packets by specifying characteristics of the tunnels. When an IPsec peer detects a sensitive packet, it sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer.

## IPsec Operation

An IPsec operation involves five basic steps: identifying interesting traffic, IKE phase-1, IKE phase-2, establishing the tunnel or IPsec session, and finally tearing down the tunnel.

### Step 1: Identifying Interesting Traffic

The VPN devices recognize the traffic, or sensitive packets, to detect. IPsec is either applied to the sensitive packet, the packet is bypassed, or the packet is dropped. Based on the traffic type, if IPsec is applied then IKE phase-1 is initiated.

### Step 2: IKE Phase-1

There are three exchanges between the VPN devices to negotiate an IKE security policy and establish a secure channel.

During the first exchange, the VPN devices negotiate matching IKE transform sets to protect the IKE exchange resulting in establishing an Internet Security Association and Key Management Protocol (ISAKMP) policy to utilize. The ISAKMP policy consists of an encryption algorithm, a hash algorithm, an authentication algorithm, a Diffie-Hellman (DH) group, and a lifetime parameter.

There are eight default ISAKMP policies supported. For more information on default ISAKMP policies, see the section “[Verifying IKE Phase-1, ISAKMP, Default Policies](#).”

The second exchange consists of a Diffie-Hellman exchange, which establishes a shared secret.

The third exchange authenticates peer identity. After the peers are authenticated, IKE phase-2 begins.

### Step 3: IKE Phase-2

The VPN devices negotiate the IPsec security policy used to protect the IPsec data. IPsec transform sets are negotiated.

A transform set is a combination of algorithms and protocols that enact a security policy for network traffic. For more information on default transform sets, see the section “[Verifying Default IPsec Transform-Sets](#).” A VPN tunnel is ready to be established.

### Step 4: Establishing the Tunnel—IPsec Session

The VPN devices apply security services to IPsec traffic and then transmit the IPsec data. Security associations (SAs) are exchanged between peers. The negotiated security services are applied to the tunnel traffic while the IPsec session is active.

### Step 5: Terminating the Tunnel

The tunnel is torn down when an IPsec SA lifetime time-out occurs or if the packet counter is exceeded. The IPsec SA is removed.

## How to Utilize IPsec Usability Enhancements

This section contains the following optional procedures:

- [Verifying IKE Phase-1, ISAKMP, Default Policies](#), page 3
- [Verifying Default IPsec Transform-Sets](#), page 7
- [Verifying and Troubleshooting IPsec VPNs](#), page 9

## Verifying IKE Phase-1, ISAKMP, Default Policies

When IKE negotiation begins, the peers try to find a common policy, starting with the highest priority policy as specified on the remote peer. The peers negotiate the policy sets until there is a match. If peers have more than one policy set in common, the lowest priority number is used.

There are three groups of IKE phase-1, ISAKMP, policies as defined by policy priority ranges and behavior:

- Default ISAKMP policies, which are automatically enabled.
- User configured ISAKMP policies, which you may configure with the **crypto isakmp policy** command.
- Easy VPN (EzVPN) ISAKMP policies, which are made available during EzVPN configuration.

This section describes the three groups of ISAKMP policies, how they behave in relationship to one another, how to determine which policies are in use with the appropriate **show** command, and how to disable the default ISAKMP policies.

### Default IKE Phase-1 Policies

There are eight default IKE phase-1, ISAKMP, policies supported (see [Table 1](#)) that are enabled automatically. If you have neither manually configured IKE policies with the **crypto isakmp policy** command nor disabled the default IKE policies with the **no crypto isakmp default policy** command,

the default IKE policies will be used during peer IKE negotiations. You can verify that the default IKE policies are in use by issuing either the **show crypto isakmp policy** command or the **show crypto isakmp default policy** command.

The default IKE policies define the following policy set parameters:

- The priority, 65507–65514, where 65507 is the highest priority and 65514 is the lowest priority.
- The authentication method, Rivest, Shamir, and Adelman (RSA) or preshared keys (PSK).
- The encryption method, Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES).
- The hash function, Secure Hash Algorithm (SHA-1) or Message-Digest algorithm 5 (MD5).
- The DH group specification DH2 or DH5
  - DH2 specifies the 768-bit DH group.
  - DH5 specifies the 1536-bit DH group.

**Table 1**     *Default IKE Phase-1, ISAKMP, Policies*

| Priority | Authentication | Encryption | Hash | Diffie-Hellman |
|----------|----------------|------------|------|----------------|
| 65507    | RSA            | AES        | SHA  | DH5            |
| 65508    | PSK            | AES        | SHA  | DH5            |
| 65509    | RSA            | AES        | MD5  | DH5            |
| 65510    | PSK            | AES        | MD5  | DH5            |
| 65511    | RSA            | 3DES       | SHA  | DH2            |
| 65512    | PSK            | 3DES       | SHA  | DH2            |
| 65513    | RSA            | 3DES       | MD5  | DH2            |
| 65514    | PSK            | 3DES       | MD5  | DH2            |

## User Configured IKE Policies

You may configure IKE policies with the **crypto isakmp policy** command. User configured IKE policies are uniquely identified and configured with a priority number ranging from 1–10000, where 1 is the highest priority and 10000 the lowest priority.

Once you have configured one or more IKE policies with a priority of 1–10000:

- The user configured policies will be used during peer IKE negotiations.
- The default IKE policies will no longer be used during peer IKE negotiations.
- The user configured policies may be displayed by issuing the **show crypto isakmp policy** command.

## EzVPN ISAKMP Policies

If you have configured EzVPN (see [Related Documents](#)), the default EzVPN ISAKMP policies in use are uniquely identified with a priority number ranging from 65515–65535, where 65515 is the highest priority and 65535 is the lowest priority.



Once a user has configured EzVPN:

- The default EzVPN ISAKMP policies and the default IKE policies will be used during peer IKE negotiations.
- The EzVPN ISAKMP policies and the default IKE policies will be displayed by issuing the **show crypto isakmp policy** command.
- Default ISAKMP policies will be displayed by issuing the **show crypto isakmp default policy** command unless they have been disabled by issuing the **no crypto isakmp default policy** command.

## SUMMARY STEPS

1. **enable**
2. **show crypto isakmp default policy**
3. **configure terminal**
4. **no crypto isakmp default policy**

## DETAILED STEPS

|        | Command or Action                                                                                                | Purpose                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                           | Enables privileged EXEC mode.<br><br>• Enter your password if prompted.                            |
| Step 2 | <b>show crypto isakmp default policy</b><br><br><b>Example:</b><br>Router# show crypto isakmp default policy     | (Optional) Displays default ISAKMP policies if no policy with a priority of 1–10000 is configured. |
| Step 3 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                   | Enters global configuration mode.                                                                  |
| Step 4 | <b>no crypto isakmp default policy</b><br><br><b>Example:</b><br>Router(config)# no crypto isakmp default policy | (Optional) Turns off default ISAKMP policies with priorities 65507–65514.                          |

## Examples

The following is sample output of the **show crypto isakmp default policy** command. The default policies are displayed because the default policies have not been disabled.

```
Router# show crypto isakmp default policy
```

```
Default IKE policy
Default protection suite of priority 65507
 encryption algorithm: AES - Advanced Encryption Standard (128 bit key).
 hash algorithm: Secure Hash Standard
 authentication method: Rivest-Shamir-Adleman Signature
 Diffie-Hellman group: #5 (1536 bit)
 lifetime: 86400 seconds, no volume limit
```

```

Default protection suite of priority 65508
 encryption algorithm: AES - Advanced Encryption Standard (128 bit key).
 hash algorithm: Secure Hash Standard
 authentication method: Pre-Shared Key
 Diffie-Hellman group: #5 (1536 bit)
 lifetime: 86400 seconds, no volume limit
Default protection suite of priority 65509
 encryption algorithm: AES - Advanced Encryption Standard (128 bit key).
 hash algorithm: Message Digest 5
 authentication method: Rivest-Shamir-Adleman Signature
 Diffie-Hellman group: #5 (1536 bit)
 lifetime: 86400 seconds, no volume limit
Default protection suite of priority 65510
 encryption algorithm: AES - Advanced Encryption Standard (128 bit key).
 hash algorithm: Message Digest 5
 authentication method: Pre-Shared Key
 Diffie-Hellman group: #5 (1536 bit)
 lifetime: 86400 seconds, no volume limit
Default protection suite of priority 65511
 encryption algorithm: Three key triple DES
 hash algorithm: Secure Hash Standard
 authentication method: Rivest-Shamir-Adleman Signature
 Diffie-Hellman group: #2 (1024 bit)
 lifetime: 86400 seconds, no volume limit
Default protection suite of priority 65512
 encryption algorithm: Three key triple DES
 hash algorithm: Secure Hash Standard
 authentication method: Pre-Shared Key
 Diffie-Hellman group: #2 (1024 bit)
 lifetime: 86400 seconds, no volume limit
Default protection suite of priority 65513
 encryption algorithm: Three key triple DES
 hash algorithm: Message Digest 5
 authentication method: Rivest-Shamir-Adleman Signature
 Diffie-Hellman group: #2 (1024 bit)
 lifetime: 86400 seconds, no volume limit
Default protection suite of priority 65514
 encryption algorithm: Three key triple DES
 hash algorithm: Message Digest 5
 authentication method: Pre-Shared Key
 Diffie-Hellman group: #2 (1024 bit)
 lifetime: 86400 seconds, no volume limit

```

The following example disables the default IKE policies then shows the resulting output of the **show crypto isakmp default policy** command, which is blank:

```

Router# configure terminal
Router(config)# no crypto isakmp default policy
Router(config)# exit
Router# show crypto isakmp default policy
Router#
!There is no output since the default IKE policies have been disabled.

```

The following is an example system log message that is generated whenever the default ISAKMP policies are in use:

```
%CRYPTO-6-IKMP_POLICY_DEFAULT: Using ISAKMP Default policies
```

## Verifying Default IPsec Transform-Sets

A transform set represents a certain combination of security protocols and algorithms. During the IPsec SA negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

During IPsec SA negotiations with IKE, the peers search for a transform set that is the same at both peers. When such a transform set is found, it is selected and is applied to the protected traffic as part of the IPsec SAs of both peers.

### Default Transform Sets

A default transform set will be used by any crypto map or IPsec profile where no other transform set has been configured and if the following is true:

- The default transform sets have not been disabled with the **no crypto ipsec default transform-set** command.
- The crypto engine in use supports the encryption algorithm.

The two default transform sets each define an Encapsulation Security Protocol (ESP) encryption transform type and an ESP authentication transform type as shown in [Table 2](#).

**Table 2**    *Default Transform Sets and Parameters*

| Default Transform Name    | ESP Encryption Transform and Description                                   | ESP Authentication Transform and Description                                                                   |
|---------------------------|----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| #!default_transform_set_0 | esp-3des<br>(ESP with the 168-bit 3DES or Triple DES encryption algorithm) | esp-sha-hmac                                                                                                   |
| #!default_transform_set_1 | esp-aes<br>(ESP with the 128-bit AES encryption algorithm)                 | esp-sha-hmac<br>(ESP with the SHA-1, hash message authentication code [HMAC] variant authentication algorithm) |

### SUMMARY STEPS

1. **enable**
2. **show crypto ipsec default transform-set**
3. **configure terminal**
4. **no crypto ipsec default transform-set**

## DETAILED STEPS

|        | Command or Action                                                                                                            | Purpose                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                       | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>show crypto ipsec default transform-set</b><br><br><b>Example:</b><br>Router# show crypto ipsec default transform-set     | (Optional) Displays the default IPsec transform sets currently in use by IKE.                                    |
| Step 3 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                               | Enters global configuration mode.                                                                                |
| Step 4 | <b>no crypto ipsec default transform-set</b><br><br><b>Example:</b><br>Router(config)# no crypto ipsec default transform-set | (Optional) Disables the default IPsec transform sets.                                                            |

## Examples

The following example displays output from the **show crypto ipsec default transform-set** command when the default transform sets are enabled, the default setting:

```
Router# show crypto ipsec default transform-set

Transform set #1!default_transform_set_1: { esp-aes esp-sha-hmac }
 will negotiate = { Transport, },

Transform set #0!default_transform_set_0: { esp-3des esp-sha-hmac }
 will negotiate = { Transport, },
```

The following example displays output from the **show crypto ipsec default transform-set** command when the default transform sets have been disabled with the **no crypto ipsec default transform-set** command.

```
Router(config)# no crypto ipsec default transform-set
Router(config)# exit
Router#
Router# show crypto ipsec default transform-set
! There is no output.
Router#
```

The following is an example system log message that is generated whenever IPsec SAs have negotiated with a default transform set:

```
%CRYPTO-5-IPSEC_DEFAULT_TRANSFORM: Using Default IPsec transform-set
```

## Verifying and Troubleshooting IPsec VPNs

Perform one of the following optional tasks in this section, depending on whether you want to verify IKE phase-1 or IKE phase-2 tunnels or troubleshoot your IPsec VPN:

- [Verifying IKE Phase-1, ISAKMP, page 9](#)
- [Verifying IKE Phase-2, page 13](#)
- [Troubleshooting IPsec VPNs, page 16](#)

### Verifying IKE Phase-1, ISAKMP

To display statistics for ISAKMP tunnels, use the following optional commands.

#### SUMMARY STEPS

1. **show crypto mib isakmp flowmib failure** [*vrf vrf-name*]
2. **show crypto mib isakmp flowmib global** [*vrf vrf-name*]
3. **show crypto mib isakmp flowmib history** [*vrf vrf-name*]
4. **show crypto mib isakmp flowmib peer** [*index peer-mib-index*] [*vrf vrf-name*]
5. **show crypto mib isakmp flowmib tunnel** [*index tunnel-mib-index*] [*vrf vrf-name*]

#### DETAILED STEPS

##### Step 1 **show crypto mib isakmp flowmib failure** [*vrf vrf-name*]

For ISAKMP tunnel failures, this command displays event information. The following is sample output for this command:

```
Router# show crypto mib isakmp flowmib failure
```

```
vrf Global
Index: 1
Reason: peer lost
Failure time since reset: 00:07:27
Local type: ID_IPV4_ADDR
Local value: 192.0.2.1
Remote type: ID_IPV4_ADDR
Remote Value: 192.0.2.2
Local Address: 192.0.2.1
Remote Address: 192.0.2.2
Index: 2
Reason: peer lost
Failure time since reset: 00:07:27
Local type: ID_IPV4_ADDR
Local value: 192.0.3.1
Remote type: ID_IPV4_ADDR
Remote Value: 192.0.3.2
Local Address: 192.0.3.1
Remote Address: 192.0.3.2
Index: 3
Reason: peer lost
Failure time since reset: 00:07:32
Local type: ID_IPV4_ADDR
Remote type: ID_IPV4_ADDR
```

```

Remote Value: 192.0.2.2
Local Address: 192.0.2.1
Remote Address: 192.0.2.2

```

### Step 2 **show crypto mib isakmp flowmib global [vrf vrf-name]**

Global ISAKMP tunnel statistics are displayed by issuing this command. The following is sample output for this command:

```
Router# show crypto mib isakmp flowmib global
```

```

vrf Global
Active Tunnels: 3
Previous Tunnels: 0
In octets: 2856
Out octets: 3396
In packets: 16
Out packets: 19
In packets drop: 0
Out packets drop: 0
In notifys: 4
Out notifys: 7
In P2 exchg: 3
Out P2 exchg: 6
In P2 exchg invalids: 0
Out P2 exchg invalids: 0
In P2 exchg rejects: 0
Out P2 exchg rejects: 0
In IPSEC delete: 0
Out IPSEC delete: 0
SAs locally initiated: 3
SAs locally initiated failed: 0
SAs remotely initiated failed: 0
System capacity failures: 0
Authentication failures: 0
Decrypt failures: 0
Hash failures: 0
Invalid SPI: 0

```

### Step 3 **show crypto mib isakmp flowmib history [vrf vrf-name]**

For information about ISAKMP tunnels that are no longer active, this command displays event information including the reason that the tunnel was terminated. The following is sample output for this command:

```
Router# show crypto mib isakmp flowmib history
```

```

vrf Global
Reason: peer lost
Index: 2
Local type: ID_IPV4_ADDR
Local address: 192.0.2.1
Remote type: ID_IPV4_ADDR
Remote address: 192.0.2.2
Negotiation mode: Main Mode
Diffie Hellman Grp: 2
Encryption algo: des
Hash algo: sha
Auth method: psk
Lifetime: 86400
Active time: 00:06:30
Policy priority: 1
Keepalive enabled: Yes

```

```

In octets: 3024
In packets: 22
In drops: 0
In notifys: 18
In P2 exchanges: 1
In P2 exchg invalids: 0
In P2 exchg rejected: 0
In P2 SA delete reqs: 0
Out octets: 4188
Out packets: 33
Out drops: 0
Out notifys: 28
Out P2 exchgs: 2
Out P2 exchg invalids: 0
Out P2 exchg rejects: 0
Out P2 Sa delete requests: 0
Reason: peer lost
Index: 3
Local type: ID_IPV4_ADDR
Local address: 192.0.3.1
Remote type: ID_IPV4_ADDR
Remote address: 192.0.3.2
Negotiation mode: Main Mode
Diffie Hellman Grp: 2
Encryption algo: des
Hash algo: sha
Auth method: psk
Lifetime: 86400
Active time: 00:06:25
Policy priority: 1
Keepalive enabled: Yes
In octets: 3140
In packets: 23
In drops: 0
In notifys: 19
In P2 exchanges: 1
In P2 exchg invalids: 0
In P2 exchg rejected: 0
In P2 SA delete reqs: 0
Out octets: 4304
Out packets: 34
Out drops: 0
Out notifys: 29
Out P2 exchgs: 2
Out P2 exchg invalids: 0
Out P2 exchg rejects: 0
Out P2 Sa delete requests: 0

```

**Step 4** **show crypto mib isakmp flowmib peer** [*index peer-mib-index*] [*vrf vrf-name*]

For active ISAKMP peer associations, this command displays information including indexes, type of connection, and IP addresses. The following is sample output for this command:

```
Router# show crypto mib isakmp flowmib peer
```

```

vrf Global
Index: 1
Local type: ID_IPV4_ADDR
Local address: 192.0.2.1
Remote type: ID_IPV4_ADDR
Remote address: 192.0.2.2

```

```

Index: 2
Local type: ID_IPV4_ADDR
Local address: 192.0.3.1
Remote type: ID_IPV4_ADDR
Remote address: 192.0.3.1

```

```

Index: 3
Local type: ID_IPV4_ADDR
Local address: 192.0.4.1
Remote type: ID_IPV4_ADDR
Remote address: 192.0.4.1

```

**Step 5** **show crypto mib isakmp flowmib tunnel** [*index tunnel-mib-index*] [*vrf vrf-name*]

For active ISAKMP tunnels, this command displays tunnel statistics. The following is sample output for this command:

```
Router# show crypto mib isakmp flowmib tunnel
```

```

vrf Global
Index: 1
Local type: ID_IPV4_ADDR
Local address: 192.0.2.1
Remote type: ID_IPV4_ADDR
Remote address: 192.0.2.2
Negotiation mode: Main Mode
Diffie Hellman Grp: 2
Encryption algo: des
Hash algo: sha
Auth method: psk
Lifetime: 86400
Active time: 00:03:08
Policy priority: 1
Keepalive enabled: Yes
In octets: 2148
In packets: 15
In drops: 0
In notifys: 11
In P2 exchanges: 1
In P2 exchg invalids: 0
In P2 exchg rejected: 0
In P2 SA delete reqs: 0
Out octets: 2328
Out packets: 16
Out drops: 0
Out notifys: 12
Out P2 exchgs: 2
Out P2 exchg invalids: 0
Out P2 exchg rejects: 0
Out P2 Sa delete requests: 0

```

---



## Verifying IKE Phase-2

To display statistics for IPsec phase-2 tunnels, use the following optional commands.

### SUMMARY STEPS

1. **show crypto mib ipsec flowmib endpoint** [*vrf vrf-name*]
2. **show crypto mib ipsec flowmib failure** [*vrf vrf-name*]
3. **show crypto mib ipsec flowmib global** [*vrf vrf-name*]
4. **show crypto mib ipsec flowmib history** [*vrf vrf-name*]
5. **show crypto mib ipsec flowmib spi** [*vrf vrf-name*]
6. **show crypto mib ipsec flowmib tunnel** [*index tunnel-mib-index*] [*vrf vrf-name*]

### DETAILED STEPS

#### Step 1 **show crypto mib ipsec flowmib endpoint** [*vrf vrf-name*]

Information for each active endpoint, local or remote device, associated with an IPsec phase-2 tunnel is displayed by issuing this command. The following is sample output for this command:

```
Router# show crypto mib ipsec flowmib endpoint

vrf Global
 Index: 1
 Local type: Single IP address
 Local address: 192.1.2.1
 Protocol: 0
 Local port: 0
 Remote type: Single IP address
 Remote address: 192.1.2.2
 Remote port: 0

 Index: 2
 Local type: Subnet
 Local address: 192.1.3.0 255.255.255.0
 Protocol: 0
 Local port: 0
 Remote type: Subnet
 Remote address: 192.1.3.0 255.255.255.0
 Remote port: 0
```

#### Step 2 **show crypto mib ipsec flowmib failure** [*vrf vrf-name*]

For ISAKMP tunnel failures, this command displays event information. The following is sample output for this command:

```
Router# show crypto mib ipsec flowmib failure

vrf Global
 Index: 1
 Reason: Operation request
 Failure time since reset: 00:25:18
 Src address: 192.1.2.1
 Destination address: 192.1.2.2
 SPI: 0
```

**Step 3** **show crypto mib ipsec flowmib global [vrf vrf-name]**

Global IKE phase-2 tunnel statistics are displayed by issuing this command. The following is sample output for this command:

```
Router# show crypto mib ipsec flowmib global
```

```
vrf Global
Active Tunnels: 2
Previous Tunnels: 0
In octets: 800
Out octets: 1408
In packets: 8
Out packets: 8
Uncompressed encrypted bytes: 1408
In packets drops: 0
Out packets drops: 2
In replay drops: 0
In authentications: 8
Out authentications: 8
In decrypts: 8
Out encrypts: 8
Compressed bytes: 0
Uncompressed bytes: 0
In uncompressed bytes: 0
Out uncompressed bytes: 0
In decrypt failures: 0
Out encrypt failures: 0
No SA failures: 0
! Number of SA Failures.
Protocol use failures: 0
System capacity failures: 0
In authentication failures: 0
Out authentication failures: 0
```

**Step 4** **show crypto mib ipsec flowmib history [vrf vrf-name]**

For information about IKE phase-2 tunnels that are no longer active, this command displays event information including the reason that the tunnel was terminated. The following is sample output for this command:

```
Router# show crypto mib ipsec flowmib history
```

```
vrf Global
Reason: Operation request
Index: 1
Local address: 192.1.2.1
Remote address: 192.1.2.2
IPSEC keying: IKE
Encapsulation mode: 1
Lifetime (KB): 4608000
Lifetime (Sec): 3600
Active time: 00:24:32
Lifetime threshold (KB): 423559168
Lifetime threshold (Sec): 3590000
Total number of refreshes: 0
Expired SA instances: 4
Current SA instances: 4
In SA DH group: 1
In sa encrypt algorithm: des
In SA auth algorithm: rsig
In SA ESP auth algo: ESP_HMAC_SHA
In SA uncompress algorithm: None
Out SA DH group: 1
```

```

Out SA encryption algorithm: des
Out SA auth algorithm: ESP_HMAC_SHA
Out SA ESP auth algorithm: ESP_HMAC_SHA
Out SA uncompress algorithm: None
In octets: 400
Decompressed octets: 400
In packets: 4
In drops: 0
In replay drops: 0
In authentications: 4
In authentication failures: 0
In decrypts: 4
In decrypt failures: 0
Out octets: 704
Out uncompressed octets: 704
Out packets: 4
Out drops: 1
Out authentications: 4
Out authentication failures: 0
Out encryptions: 4
Out encryption failures: 0
Compressed octets: 0
Decompressed octets: 0
Out uncompressed octets: 704

```

**Step 5** `show crypto mib ipsec flowmib spi [vrf vrf-name]`

The security protection index (SPI) table contains an entry for each active and expiring security IKE phase-2 association. The following is sample output for this command, which displays the SPI table:

Router# **show crypto mib ipsec flowmib spi**

```

vrf Global
Tunnel Index: 1
SPI Index: 1
SPI Value: 0xCC57D053
SPI Direction: In
SPI Protocol: AH
SPI Status: Active

SPI Index: 2
SPI Value: 0x68612DF
SPI Direction: Out
SPI Protocol: AH
SPI Status: Active

SPI Index: 3
SPI Value: 0x56947526
SPI Direction: In
SPI Protocol: ESP
SPI Status: Active

SPI Index: 4
SPI Value: 0x8D7C2204
SPI Direction: Out
SPI Protocol: ESP
SPI Status: Active

```

**Step 6** `show crypto mib ipsec flowmib tunnel [index tunnel-mib-index] [vrf vrf-name]`

For active IKE phase-2 tunnels, this command displays tunnel statistics. The following is sample output for this command:

```

Router# show crypto mib ipsec flowmib tunnel

vrf Global
 Index: 1
 Local address: 192.0.2.1
 Remote address: 192.0.2.2
 IPSEC keying: IKE
 Encapsulation mode: 1
 Lifetime (KB): 4608000
 Lifetime (Sec): 3600
 Active time: 00:05:46
 Lifetime threshold (KB): 64
 Lifetime threshold (Sec): 10
 Total number of refreshes: 0
 Expired SA instances: 0
 Current SA instances: 4
 In SA DH group: 1
 In sa encrypt algorithm: des
 In SA auth algorithm: rsig
 In SA ESP auth algo: ESP_HMAC_SHA
 In SA uncompress algorithm: None
 Out SA DH group: 1
 Out SA encryption algorithm: des
 Out SA auth algorithm: ESP_HMAC_SHA
 Out SA ESP auth algorithm: ESP_HMAC_SHA
 Out SA uncompress algorithm: None
 In octets: 400
 Decompressed octets: 400
 In packets: 4
 In drops: 0
 In replay drops: 0
 In authentications: 4
 In authentication failures: 0
 In decrypts: 4
 In decrypt failures: 0
 Out octets: 704
 Out uncompressed octets: 704
 Out packets: 4
 Out drops: 1
 Out authentications: 4
 Out authentication failures: 0
 Out encryptions: 4
 Out encryption failures: 0
 Compressed octets: 0
 Decompressed octets: 0
 Out uncompressed octets: 704

```

---

## Troubleshooting IPsec VPNs

The **show tech-support ipsec** command simplifies the collection of the IPsec related information if you are troubleshooting a problem.

### SUMMARY STEPS

1. **show tech-support ipsec [peer *ipv4address* | vrf *vrf-name*]**

## DETAILED STEPS

### Step 1 **show tech-support ipsec**

There are three variations of the **show tech-support ipsec** command:

- **show tech-support ipsec**
- **show tech-support ipsec peer *ipv4address***
- **show tech-support ipsec vrf *vrf-name***

For a sample display of the output from the **show tech-support ipsec** command for the individual **show** commands listed below for each variation see the “[Related Documents](#)” section.

#### **Output of the show tech-support ipsec Command**

If you enter the **show tech-support ipsec** command without any keywords, the command output displays the following **show** commands, in order of output:

- **show version**
- **show running-config**
- **show crypto isakmp sa count**
- **show crypto ipsec sa count**
- **show crypto session summary**
- **show crypto session detail**
- **show crypto isakmp sa detail**
- **show crypto ipsec sa detail**
- **show crypto isakmp peers**
- **show crypto ruleset detail**
- **show processes memory | include Crypto IKMP**
- **show processes cpu | include Crypto IKMP**
- **show crypto eli**
- **show crypto engine accelerator statistic**

#### **Output of the show tech-support ipsec peer Command**

If you enter the **show tech-support ipsec** command with the **peer** keyword and the *ipv4address* argument, the output displays the following **show** commands, in order of output for the specified peer:

- **show version**
- **show running-config**
- **show crypto session remote *ipv4address* detail**
- **show crypto isakmp sa peer *ipv4address* detail**
- **show crypto ipsec sa peer *ipv4address* detail**
- **show crypto isakmp peers *ipv4address***
- **show crypto ruleset detail**
- **show processes memory | include Crypto IKMP**

- **show processes cpu | include Crypto IKMP**
- **show crypto eli**
- **show crypto engine accelerator statistic**

#### Output of the show tech-support ipsec vrf Command

If you enter the **show tech-support ipsec** command with the **vrf** keyword and the *vrf-name* argument, the output displays the following **show** commands, in order of output for the specified Virtual Routing and Forwarding (VRF):

- **show version**
  - **show running-config**
  - **show crypto isakmp sa count vrf *vrf-name***
  - **show crypto ipsec sa count vrf *vrf-name***
  - **show crypto session ivrf *ivrf-name* detail**
  - **show crypto session fvrf *fvrf-name* detail**
  - **show crypto isakmp sa vrf *vrf-name* detail**
  - **show crypto ipsec sa vrf *vrf-name* detail**
  - **show crypto ruleset detail**
  - **show processes memory | include Crypto IKMP**
  - **show processes cpu | include Crypto IKMP**
  - **show crypto eli**
  - **show crypto engine accelerator statistic**
- 

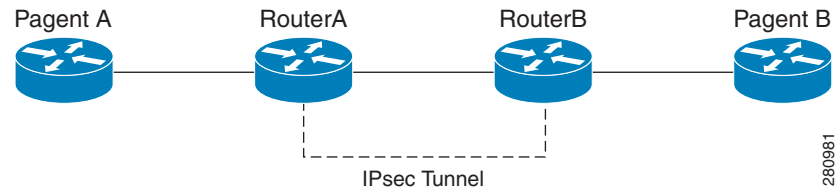
## Configuration Examples for IPsec Usability Enhancements

This section provides the following configuration examples:

- [IKE Default Policies: Example, page 18](#)
- [Default Transform Sets: Example, page 20](#)

### IKE Default Policies: Example

In the following example, crypto maps are configured on RouterA and RouterB and default IKE policies are in use. Traffic is routed from Pagent A to Pagent B. Checking the system log on Peer A and Peer B confirms that the default IKE policies are in use on both peers (see [Figure 1](#)).

**Figure 1** Example Site to Site Topology

```

! Configuring RouterA.
RouterA(config)# crypto isakmp key identity address 209.165.200.226
RouterA(config)# crypto map testmap 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
 and a valid access list have been configured.
RouterA(config-crypto-map)# set peer 209.165.200.226
RouterA(config-crypto-map)# match address 101
RouterA(config-crypto-map)# exit
RouterA(config)# ip route 209.165.200.225 255.255.255.224 209.165.200.226
RouterA(config)# access-list 101 permit ip host 209.165.200.227 host 209.165.200.225
RouterA(config)# end
RouterA(config)# interface Ethernet1/2
RouterA(config-if)# crypto map testmap
RouterA(config-if)# end
RouterA(config)# crypto ipsec transform test_transf esp-aes esp-sha-hmac
RouterA(cfg-crypto-trans)# mode tunnel
RouterA(cfg-crypto-trans)# end
RouterA(config)# crypto map testmap 10
RouterA(config-crypto-map)# set transform-set test_transf
RouterA(config-crypto-map)# end

! Configuring RouterB.
RouterB(config)# crypto isakmp key identity address 209.165.200.228
RouterB(config)# crypto dynamic-map dyn_testmap 10
RouterB(config-crypto-map)# crypto map testmap 10 ipsec-isakmp dynamic dyn_testmap
RouterB(config)# ip route 209.165.200.227 255.255.255.224 209.165.200.228
RouterB(config)# end
RouterB(config)# interface GigabitEthernet0/1
RouterB(config-if)# crypto map testmap
RouterB(config-if)# end
RouterB(config)# crypto ipsec transform test_transf esp-aes esp-sha-hmac
RouterB(cfg-crypto-trans)# mode tunnel
RouterB(cfg-crypto-trans)# end
RouterB(config)# crypto dynamic-map dyn_testmap 10
RouterB(config-crypto-map)# set transform-set test_transf
RouterB(config-crypto-map)# end

! Routing traffic from PagentA to PagentB.
PagentA(config)# ip route 209.165.200.225 255.255.255.224 209.165.200.229
PagentA(config)# end

! Routing traffic from PagentB to PagentA.
PagentB(config)# ip route 209.165.200.227 255.255.255.224 209.165.200.230
PagentB(config)# end

! Checking the system log on RouterA confirms that the default IKE policies are in use.
RouterA# show log | include %CRYPTO-6-IKMP_POLICY_DEFAULT*

Jun 5 09:17:59.251 PDT: %CRYPTO-6-IKMP_POLICY_DEFAULT: Using ISAKMP Default policies

```

```
! Checking the system log on RouterB confirms that the default IKE policies are in use.
RouterB# show log | include %CRYPTO-6-IKMP_POLICY_DEFAULT*
```

```
Jun 5 09:17:59.979 PDT: %CRYPTO-6-IKMP_POLICY_DEFAULT: Using ISAKMP Default policies
```

## Default Transform Sets: Example

In the following example, static crypto maps are configured on RouterA and dynamic crypto maps are configured on RouterB. Traffic is routed from Pagent A to Pagent B. The IPsec SAs negotiate with default transform sets and the traffic is encrypted. Executing the **show crypto map** command on both peers verifies that the default transform sets are in use (see [Figure 1](#)).

```
! Configuring RouterA.
RouterA(config)# crypto isakmp key identify address 209.165.200.225
RouterA(config)# crypto map testmap 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
 and a valid access list have been configured.
RouterA(config-crypto-map)# set peer 209.165.200.225
RouterA(config-crypto-map)# match address 101
RouterA(config-crypto-map)# exit
RouterA(config)# ip route 209.165.200.226 255.255.255.255 209.165.200.225
RouterA(config)# access-list 101 permit ip host 209.165.200.227 host 209.165.200.226
RouterA(config)# end
RouterA(config)# interface Ethernet1/2
RouterA(config-if)# crypto map testmap
RouterA(config-if)# end
RouterA(config)# crypto isakmp policy 10
RouterA(config-isakmp)# encryption aes
RouterA(config-isakmp)# authentication pre-share
RouterA(config-isakmp)# hash sha
RouterA(config-isakmp)# group 5
RouterA(config-isakmp)# end

! Configuring RouterB.
RouterB(config)# crypto isakmp key identity address 209.165.200.229
RouterB(config)# crypto dynamic-map dyn_testmap 10
RouterB(config-crypto-map)# crypto map testmap 10 ipsec-isakmp dynamic dyn_testmap
RouterB(config)# ip route 209.165.200.227 255.255.255.255 209.165.200.229
RouterB(config)# end
RouterB(config)# interface GigabitEthernet0/1
RouterB(config-if)# crypto map testmap
RouterB(config-if)# end
RouterB(config)# crypto isakmp policy 10
RouterB(config-isakmp)# encryption aes
RouterB(config-isakmp)# authentication pre-share
RouterB(config-isakmp)# hash sha
RouterB(config-isakmp)# group 5
RouterB(config-isakmp)# end

! The SA is using the default transform set and traffic is encrypted on RouterA.
RouterA# show crypto isakmp sa detail | include 209.165.200.229.*209.165.200.225.*ACTIVE

13007 209.165.200.229 209.165.200.225 ACTIVE aes sha psk 5 23:59:56
13006 209.165.200.229 209.165.200.225 ACTIVE aes sha psk 5 0
13005 209.165.200.229 209.165.200.225 ACTIVE aes sha psk 5 0

! The SA is using the default transform set and traffic is encrypted on RouterB.
RouterB# show crypto isakmp sa detail | include 209.165.200.225.*209.165.200.229.*ACTIVE
```



```

7007 209.165.200.225 209.165.200.229 ACTIVE aes sha psk 5 23:59:55
7006 209.165.200.225 209.165.200.229 ACTIVE aes sha psk 5 0
7005 209.165.200.225 209.165.200.229 ACTIVE aes sha psk 5 0

```

! Verifying that the default transform sets are in use on RouterA.  
RouterA# **show crypto map**

```

Crypto Map "testmap" 10 ipsec-isakmp
 Peer = 209.165.200.225
 Extended IP access list 101
 access-list 101 permit ip host 209.165.200.227 host 209.165.200.226
 Current peer: 209.165.200.225
 Security association lifetime: 4608000 kilobytes/3600 seconds
 PFS (Y/N): N
 Transform sets={
 #!default_transform_set_1: { esp-aes esp-sha-hmac } ,
 #!default_transform_set_0: { esp-3des esp-sha-hmac } ,
 }
 Interfaces using crypto map testmap:
 Ethernet1/2

```

! Verifying that the default transform sets are in use on RouterB.  
RouterB# **show crypto map**

```

Crypto Map "testmap" 10 ipsec-isakmp
 Dynamic map template tag: dyn_testmap

Crypto Map "testmap" 65536 ipsec-isakmp
 Peer = 209.165.200.229
 Extended IP access list
 access-list permit ip host 209.165.200.226 host 209.165.200.227
 dynamic (created from dynamic map dyn_testmap/10)
 Current peer: 209.165.200.229
 Security association lifetime: 4608000 kilobytes/3600 seconds
 PFS (Y/N): N
 Transform sets={
 #!default_transform_set_1: { esp-aes esp-sha-hmac } ,
 }
 Interfaces using crypto map testmap:
 GigabitEthernet0/1

```

## Additional References

The following sections provide references related to the IPsec Usability Enhancement feature.

## Related Documents

| Related Topic       | Document Title                                                                                                                        |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| IKE configuration   | The section “ <a href="#">Configuring Internet Key Exchange for IPsec VPNs</a> ” in the <i>Cisco IOS Security Configuration Guide</i> |
| IPsec configuration | The section “ <a href="#">Configuring Security for VPNs with IPsec</a> ” in the <i>Cisco IOS Security Configuration Guide</i>         |

| Related Topic               | Document Title                                                                                             |
|-----------------------------|------------------------------------------------------------------------------------------------------------|
| EzVPN server                | The section “ <a href="#">Cisco Easy VPN Remote</a> ” in the <i>Cisco IOS Security Configuration Guide</i> |
| Cisco IOS security commands | <a href="#">Cisco IOS Security Command Reference, 12.4T</a>                                                |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC                                                                                                                         | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

- **crypto ipsec default transform-set**
- **crypto isakmp default policy**
- **crypto isakmp policy**
- **show crypto ipsec default transform-set**
- **show crypto ipsec transform-set**
- **show crypto isakmp default policy**
- **show crypto isakmp policy**
- **show crypto map (IPsec)**
- **show crypto mib ipsec flowmib endpoint**
- **show crypto mib ipsec flowmib failure**
- **show crypto mib ipsec flowmib global**
- **show crypto mib ipsec flowmib history**

- `show crypto mib ipsec flowmib spi`
- `show crypto mib ipsec flowmib tunnel`
- `show crypto mib isakmp flowmib failure`
- `show crypto mib isakmp flowmib global`
- `show crypto mib isakmp flowmib history`
- `show crypto mib isakmp flowmib peer`
- `show crypto mib isakmp flowmib tunnel`
- `show tech-support ipsec`

## Feature Information for IPsec Usability Enhancements

Table 3 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



### Note

Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 3** Feature Information for IPsec Usability Enhancements

| Feature Name                 | Releases  | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IPsec Usability Enhancements | 12.4(20)T | <p>This feature introduces intelligent defaults for IKE and IPsec, and <b>show</b> commands to access MIB statistics and to aid in troubleshooting.</p> <p>The following commands were introduced or modified:<br/> <b>crypto ipsec default transform-set</b>, <b>crypto isakmp default policy</b>, <b>crypto isakmp policy</b>, <b>show crypto ipsec default transform-set</b>, <b>show crypto ipsec transform-set</b>, <b>show crypto isakmp default policy</b>, <b>show crypto isakmp policy</b>, <b>show crypto map (IPsec)</b>, <b>show crypto mib ipsec flowmib endpoint</b>, <b>show crypto mib ipsec flowmib failure</b>, <b>show crypto mib ipsec flowmib global</b>, <b>show crypto mib ipsec flowmib history</b>, <b>show crypto mib ipsec flowmib spi</b>, <b>show crypto mib ipsec flowmib tunnel</b>, <b>show crypto mib isakmp flowmib failure</b>, <b>show crypto mib isakmp flowmib global</b>, <b>show crypto mib isakmp flowmib history</b>, <b>show crypto mib isakmp flowmib peer</b>, <b>show crypto mib isakmp flowmib tunnel</b>, <b>show tech-support ipsec</b>.</p> |

# Glossary

**peer**—In the context of this module, a router or other device that participates in IPsec.

**SA**—security association. Description of how two or more entities use security services in the context of a particular security protocol (AH or ESP) to communicate securely on behalf of a particular data flow. The transform and the shared secret keys are used for protecting the traffic.

**transform**—List of operations performed on a dataflow to provide data authentication, data confidentiality, and data compression. For example, one transform is the ESP protocol with the HMAC-MD5 authentication algorithm; another transform is the AH protocol with the 56-bit DES encryption algorithm and the ESP protocol with the HMAC-SHA authentication algorithm.

**tunnel**—In the context of this module, a secure communication path between two peers, such as two routers. It does not refer to using IPsec in tunnel mode.

---

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.





## **Public Key Infrastructure (PKI)**







# Implementing and Managing PKI Features Roadmap

---

This roadmap lists the features documented in the *Cisco IOS Security Configuration Guide* and maps them to the modules in which they appear.

## Roadmap History

This roadmap was first published on May 2, 2005, and last updated on May 2, 2005.

## Feature and Release Support

[Table 56](#) lists public key infrastructure (PKI) feature support for the following Cisco IOS software release trains:

- [Cisco IOS Releases 12.2T, 12.3, and 12.3T](#)

Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table. *Not all features may be supported in your Cisco IOS software release.*

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



## Note

[Table 56](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

**Table 56**      **Supported PKI Features**

| Release                                          | Feature Name                                               | Feature Description                                                                                                                                                                                                                                                                                                                                         | Where Documented                                                                                                                |
|--------------------------------------------------|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>Cisco IOS Releases 12.2T, 12.3, and 12.3T</b> |                                                            |                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                 |
| 12.3(14)T                                        | Administrative Secure Device Provisioning Introducer       | This feature allows you to act as an administrative introducer to introduce a device into a PKI network and then provide a username as the device name for the record locator in the AAA database.                                                                                                                                                          | “Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI”                                                           |
| 12.3(14)T                                        | Persistent Self-Signed Certificates                        | This feature allows users the HTTPS server to generate and save a self-signed certificate in the router’s startup configuration. Thus, future SSL handshakes between the client and the HTTPS server can use the same self-signed certificate without user intervention.                                                                                    | “Configuring Certificate Enrollment for a PKI”                                                                                  |
| 12.3(14)T                                        | Secure Device Provisioning Certificate-Based Authorization | This feature allows certificates issued by other authority (CA) servers to be used for SDP introductions.                                                                                                                                                                                                                                                   | “Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI”                                                           |
| 12.3(14)T                                        | Subordinate Certificate Server                             | This enhancement allows you to configure a subordinate certificate server to grant all or certain SCEP or manual certificate requests.                                                                                                                                                                                                                      | “Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment”                                                    |
| 12.3(14)T                                        | USB Storage                                                | This feature explains how to store RSA keys on a device external to the router via a USB eToken. The SmartCard technology (which is owned by Aladdin Knowledge Systems) in a USB key form factor (also referred to as a USB eToken) provides secure configuration distribution and allows users to store PKI credentials, such as RSA keys, for deployment. | “Storing PKI Credentials External to the Router”                                                                                |
| 12.3(11)T                                        | The Certificate Server Auto Archive enhancement            | This enhancement enables the CA certificate and CA key to be backed up automatically just once after they are generated by the certificate server. As a result, it is not necessary to generate an exportable CA key if CA backup is desirable.                                                                                                             | “Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment”                                                    |
| 12.3(11)T                                        | PKI AAA Authorization Using the Entire Subject Name        | This feature provides users with the ability to query the AAA server using the entire subject name from the certificate as a unique AAA username.                                                                                                                                                                                                           | “Configuring Revocation and Authorization of Certificates in a PKI”                                                             |
| 12.3(11)T                                        | PKI Status                                                 | This enhancement added the <b>status</b> keyword to the <b>show crypto pki trustpoints</b> command, which allows you to view the current status of the trustpoint. Prior to this enhancement, you had to issue the <b>show crypto pki certificates</b> and the <b>show crypto pki timers</b> commands for the current status.                               | “Configuring Certificate Enrollment for a PKI” and “Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment” |
| 12.3(11)T                                        | Reenroll Using Existing Certificates                       | This feature allows users to reenroll a router with a Cisco IOS CA via existing certificates from a third-party vendor CA.                                                                                                                                                                                                                                  | “Configuring Certificate Enrollment for a PKI”                                                                                  |
| 12.3(8)T                                         | Easy Secure Device Deployment                              | This feature introduces support for SDP (formerly called EzSDD), which offers a web-based enrollment interface that enables network administrators to deploy new devices in large networks.                                                                                                                                                                 | “Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI”                                                           |

**Table 56**      **Supported PKI Features (continued)**

| Release  | Feature Name                                                               | Feature Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Where Documented                                                                     |
|----------|----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| 12.3(8)T | Easy Secure Device Deployment AAA Integration                              | This feature integrates an external AAA database, allowing the introducer to be authenticated against a AAA database instead of having to use the enable password of the local Cisco certificate server.                                                                                                                                                                                                                                                                                                                                                                                                | “Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI”                |
| 12.3(7)T | The Certificate Server Registration Authority (RA) Mode enhancement        | A certificate server can be configured to run in RA mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | “Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment”         |
| 12.3(7)T | The “crypto pki” commands should be a synonym for “crypto ca” commands     | This enhancement changes all commands that begin as “crypto ca” to “crypto pki.” Although the router will still accept crypto ca, all output will be read back as crypto pki.                                                                                                                                                                                                                                                                                                                                                                                                                           | All modules that contain crypto ca commands.                                         |
| 12.3(7)T | Key Rollover for Certificate Renewal                                       | This feature allows the certificate renewal request to be made before the certificate expires and retains the old key and certificate until the new certificate is available.                                                                                                                                                                                                                                                                                                                                                                                                                           | “Configuring Certificate Enrollment for a PKI”                                       |
| 12.3(7)T | PKI: Query Multiple Servers During Certificate Revocation Check            | This feature introduces the ability for Cisco IOS software to make multiple attempts to retrieve the CRL, allowing operations to continue when a particular server is not available. In addition, the ability to override the CDPs in a certificate with a manually configured CDP has been introduced. Manually overriding the CDPs in a certificate can be advantageous when a particular server is unavailable for an extended period of time. The certificate’s CDPs can be replaced with a URL or directory specification without reissuing all of the certificates that contain the original CDP. | “Configuring Revocation and Authorization of Certificates in a PKI”                  |
| 12.3(7)T | Protected Private Key Storage                                              | This feature allows a user to encrypt and lock the RSA private keys that are used on a Cisco IOS router, thereby, preventing unauthorized use of the private keys.                                                                                                                                                                                                                                                                                                                                                                                                                                      | “Deploying RSA Keys Within a PKI”                                                    |
| 12.3(4)T | Import of RSA Key Pair and Certificates in PEM Format                      | This feature allows customers to use PEM-formatted files to import or export RSA key pairs. PEM-formatted files allow customers to directly use existing RSA key pairs on their Cisco IOS routers instead of generating new keys. Also, customers can issue certificate requests and receive issued certificates in PEM-formatted files.                                                                                                                                                                                                                                                                | “Deploying RSA Keys Within a PKI” and “Configuring Certificate Enrollment for a PKI” |
| 12.3(4)T | Using Certificate ACLs to Ignore Revocation Check and Expired Certificates | This feature allows a certificate that meets specified criteria to be accepted regardless of the validity period of the certificate, or if the certificate meets the specified criteria, revocation checking does not have to be performed. Certificate ACLs are used to specify the criteria that the certificate must meet to be accepted or to avoid revocation checking. In addition, if AAA communication is protected by a certificate, this feature provides for the AAA checking of the certificate to be ignored.                                                                              | “Configuring Revocation and Authorization of Certificates in a PKI”                  |

**Table 56**      **Supported PKI Features (continued)**

| Release   | Feature Name                                        | Feature Description                                                                                                                                                                                                                                                                                                                                                                                                                 | Where Documented                                                             |
|-----------|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| 12.3(4)T  | Cisco IOS Certificate Server                        | This feature introduces support for the Cisco IOS CS, which offers users a CA that is directly integrated with Cisco IOS software to more easily deploy basic PKI networks.                                                                                                                                                                                                                                                         | “Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment” |
| 12.3(4)T  | Direct HTTP Enrollment with CA Servers              | This feature allows users to configure an enrollment profile if their CA server does not support SCEP and they do not want to use an RA as a proxy. The enrollment profile allows users to send HTTP requests directly to the CA server instead of the RA proxy.                                                                                                                                                                    | “Configuring Certificate Enrollment for a PKI”                               |
| 12.3(2)T  | Online Certificate Status Protocol (OCSP)           | This feature allows users to enable OCSP instead of CRLs to check certificate status. Unlike CRLs, which provide only periodic certificate status, OCSP can provide timely information regarding the status of a certificate.                                                                                                                                                                                                       | “Configuring Revocation and Authorization of Certificates in a PKI”          |
| 12.3(1)   | PKI Integration with AAA Server                     | This feature provides additional scalability for authorization by generating a AAA username from the certificate presented by the peer. A AAA server is queried to determine whether the certificate is authorized for use by the internal component. The authorization is indicated by a component-specified label that must be present in the AV pair for the user.                                                               | “Configuring Revocation and Authorization of Certificates in a PKI”          |
| 12.2(15)T | Certificate Security Attribute-Based Access Control | Under the IPsec protocol, CA interoperability permits Cisco IOS devices and a CA to communicate so that the Cisco IOS device can obtain and use digital certificates from the CA. Certificates contain several fields that are used to determine whether a device or user is authorized to perform a specified action. This feature adds fields to the certificate that allow specifying an ACL, to create a certificate-based ACL. | “Configuring Revocation and Authorization of Certificates in a PKI”          |
| 12.2(15)T | Exporting and Importing RSA Keys                    | This feature allows you to transfer security credentials between devices by exporting and importing RSA keys. The key pair that is shared between two devices will allow one device to immediately and transparently take over the functionality of the other router.                                                                                                                                                               | “Deploying RSA Keys Within a PKI”                                            |
| 12.2(15)T | Multiple-Tier CA Hierarchy                          | This enhancement enables users to set up a PKI in a hierarchical framework to support multiple CAs. Within a hierarchical PKI, all enrolled peers can validate the certificate of one another as long as the peers share a trusted root CA certificate or a common subordinate CA.                                                                                                                                                  | “Configuring Certificate Enrollment for a PKI”                               |
| 12.2(13)T | Manual Certificate Enrollment (TFTP Cut-and-Paste)  | This feature allows users to generate a certificate request and accept CA certificates as well as the router’s certificates via a TFTP server or manual cut-and-paste operations.                                                                                                                                                                                                                                                   | “Configuring Certificate Enrollment for a PKI”                               |
| 12.2(8)T  | Certificate Autoenrollment                          | This feature introduces certificate autoenrollment, which allows the router to automatically request a certificate from the CA that is using the parameters in the configuration.                                                                                                                                                                                                                                                   | “Configuring Certificate Enrollment for a PKI”                               |

**Table 56**      **Supported PKI Features (continued)**

| Release  | Feature Name                        | Feature Description                                                                                                                                                                                                        | Where Documented                               |
|----------|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| 12.2(8)T | Certificate Enrollment Enhancements | This feature introduces five new <b>crypto ca trustpoint</b> subcommands that provide new options for certificate requests and allow users to specify fields in the configuration instead of having to go through prompts. | “Configuring Certificate Enrollment for a PKI” |
| 12.2(8)T | Multiple RSA Key Pair Support       | This feature allows a user to configure a router to have multiple RSA key pairs. Thus, the Cisco IOS software can maintain a different key pair for each identity certificate.                                             | “Deploying RSA Keys Within a PKI”              |
| 12.2(8)T | Trustpoint CLI                      | This feature introduces the <b>crypto ca trustpoint</b> command, which adds support for trustpoint CAs.                                                                                                                    | “Configuring Certificate Enrollment for a PKI” |

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





# Cisco IOS PKI Overview: Understanding and Planning a PKI

---

Cisco IOS public key infrastructure (PKI) provides certificate management to support security protocols such as IP Security (IPSec), secure shell (SSH), and secure socket layer (SSL).

This module identifies and describes concepts that are needed to understand, plan for, and implement a PKI.

## Module History

This module was first published on May 2, 2005, and last updated on July 17, 2008.

## Contents

- [Information About Cisco IOS PKI, page 1](#)
- [Planning for a PKI, page 5](#)
- [Where to Go Next, page 6](#)
- [Additional References, page 6](#)
- [Glossary, page 8](#)

## Information About Cisco IOS PKI

Before implementing a basic PKI, you should understand the following concepts:

- [What Is Cisco IOS PKI?, page 2](#)
- [RSA Keys Overview, page 3](#)
- [What Are CAs?, page 3](#)
- [Certificate Enrollment: How It Works, page 4](#)
- [Certificate Revocation: Why It Occurs, page 5](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007, 2008 Cisco Systems, Inc. All rights reserved.

## What Is Cisco IOS PKI?

A PKI is composed of the following entities:

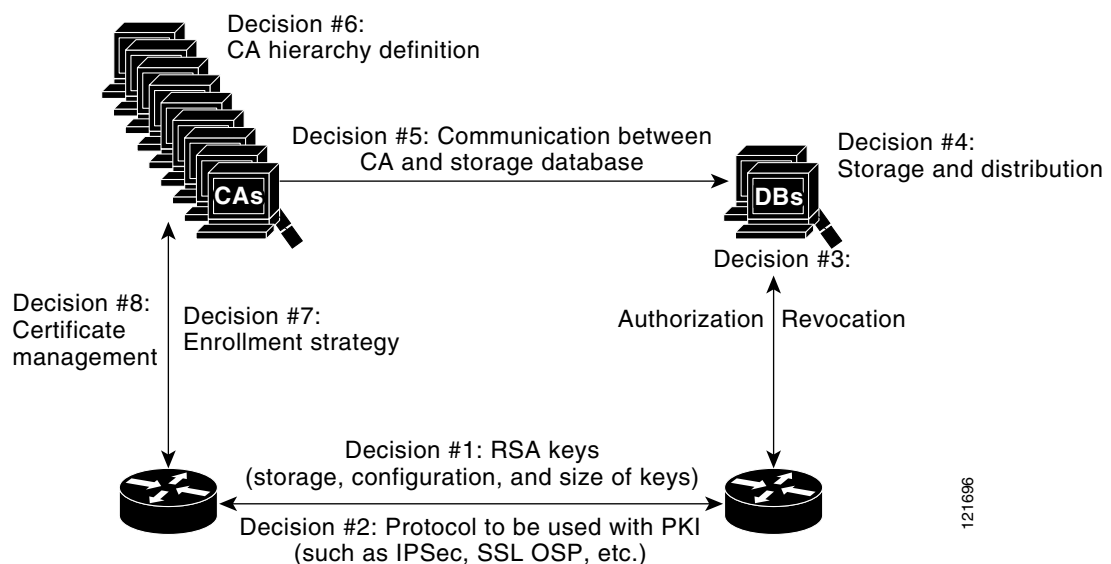
- Peers communicating on a secure network
- At least one certification authority (CA) that grants and maintains certificates
- Digital certificates, which contain information such as the certificate validity period, peer identity information, encryption keys that are used for secure communications, and the signature of the issuing CA
- An optional registration authority (RA) to offload the CA by processing enrollment requests
- A distribution mechanism (such as Lightweight Directory Access Protocol [LDAP] or HTTP) for certificate revocation lists (CRLs)

PKI provides customers with a scalable, secure mechanism for distributing, managing, and revoking encryption and identity information in a secured data network. Every entity (a person or a device) participating in the secured communication is enrolled in the PKI in a process where the entity generates an Rivest, Shamir, and Adelman (RSA) key pair (one private key and one public key) and has their identity validated by a trusted entity (also known as a CA or trustpoint).

After each entity enrolls in a PKI, every peer (also known as an end host) in a PKI is granted a digital certificate that has been issued by a CA. When peers must negotiate a secured communication session, they exchange digital certificates. Based on the information in the certificate, a peer can validate the identity of another peer and establish an encrypted session with the public keys contained in the certificate.

Although you can plan for and set up your PKI in a number of different ways, [Figure 97](#) shows the major components that make up a PKI and suggests an order in which each decision within a PKI can be made. [Figure 97](#) is a suggested approach; you can choose to set up your PKI from a different perspective.

**Figure 97**      **Deciding How to Set Up Your PKI**



121696



## RSA Keys Overview

An RSA key pair consists of a public key and a private key. When setting up your PKI, you must include the public key in the certificate enrollment request. After the certificate has been granted, the public key will be included in the certificate so that peers can use it to encrypt data that is sent to the router. The private key is kept on the router and used both to decrypt the data sent by peers and to digitally sign transactions when negotiating with peers.

RSA key pairs contain a key modulus value. The modulus determines the size of the RSA key. The larger the modulus, the more secure the RSA key. However, keys with large modulus values take longer to generate, and encryption and decryption operations take longer with larger keys.

## What Are CAs?

A CA, also known as a trustpoint, manages certificate requests and issues certificates to participating network devices. These services (managing certificate requests and issuing certificates) provide centralized key management for the participating devices and are explicitly trusted by the receiver to validate identities and to create digital certificates. Before any PKI operations can begin, the CA generates its own public key pair and creates a self-signed CA certificate; thereafter, the CA can sign certificate requests and begin peer enrollment for the PKI.

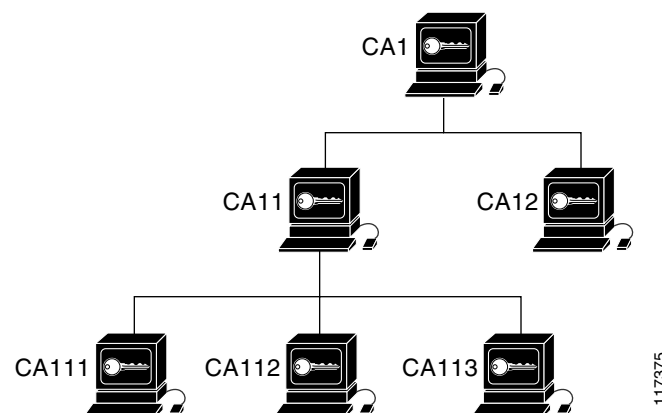
You can use a CA provided by a third-party CA vendor, or you can use an “internal” CA, which is the Cisco IOS Certificate Server.

## Hierarchical PKI: Multiple CAs

PKI can be set up in a hierarchical framework to support multiple CAs. At the top of the hierarchy is a root CA, which holds a self-signed certificate. The trust within the entire hierarchy is derived from the RSA key pair of the root CA. The subordinate CAs within the hierarchy can be enrolled with either the root CA or with another subordinate CA. These enrollment options are how multiple tiers of CAs are configured. Within a hierarchical PKI, all enrolled peers, can validate the certificate of one another if the peers share a trusted root CA certificate or a common subordinate CA.

Figure 98 shows the enrollment relationships among CAs within a three-tiered hierarchy.

**Figure 98** *Three-Tiered CA Hierarchy Sample Topology*



Each CA corresponds to a trustpoint. For example, CA11 and CA12 are subordinate CAs, holding CA certificates that have been issued by CA1; CA111, CA112, and CA113 are also subordinate CAs, but their CA certificates have been issued by CA11.

## When to Use Multiple CAs

Multiple CAs provide users with added flexibility and reliability. For example, subordinate CAs can be placed in branch offices while the root CA is at the office headquarters. Also, different granting policies can be implemented per CA, so you can set up one CA to automatically grant certificate requests while another CA within the hierarchy requires each certificate request to be manually granted.

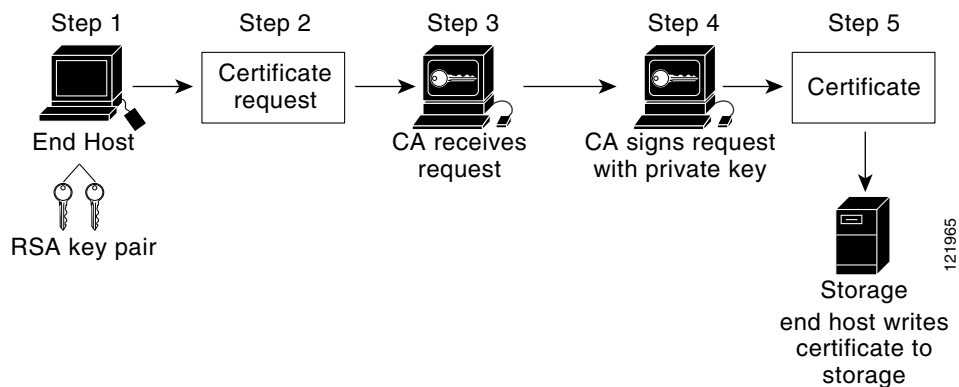
Scenarios in which at least a two-tier CA is recommended are as follows:

- Large and very active networks in which a large number of certificates are revoked and reissued. A multiple tier CA helps to control the size of the CRLs.
- When online enrollment protocols are used, the root CA can be kept offline with the exception of issuing subordinate CA certificates. This scenario provides added security for the root CA.

## Certificate Enrollment: How It Works

Certificate enrollment is the process of obtaining a certificate from a CA. Each end host that wants to participate in the PKI must obtain a certificate. Certificate enrollment occurs between the end host requesting the certificate and the CA. [Figure 99](#) and the following steps describe the certificate enrollment process.

**Figure 99** *Certificate Enrollment Process*



1. The end host generates an RSA key pair.
2. The end host generates a certificate request and forwards it to the CA (or the RA, if applicable).
3. The CA receives the certificate enrollment request, and, depending on your network configuration, one of the following options occurs:
  - c. Manual intervention is required to approve the request.
  - d. The end host is configured to automatically request a certificate from the CA. Thus, operator intervention is no longer required at the time the enrollment request is sent to the CA server.

**Note**

If you configure the end host to automatically request certificates from the CA, you should have an additional authorization mechanism.

4. After the request is approved, the CA signs the request with its private key and returns the completed certificate to the end host.
5. The end host writes the certificate to a storage area such as NVRAM.

## Certificate Enrollment Via Secure Device Provisioning

Secure Device Provisioning (SDP) is a web-based certificate enrollment interface that can be used to easily deploy PKI between two end devices, such as a Cisco IOS client and a Cisco IOS certificate server.

SDP (also referred to as Trusted Transitive Introduction [TTI]) is a communication protocol that provides a bidirectional introduction between two end entities, such as a new network device and a Virtual Private Network (VPN). SDP involves the following three entities:

- **Introducer**—A mutually trusted device that introduces the petitioner to the registrar. The introducer can be a device user, such as a system administrator.
- **Petitioner**—A new device that is joined to the secure domain.
- **Registrar**—A certificate server or other server that authorizes the petitioner.

SDP is implemented over a web browser in three phases—welcome, introduction, and completion. Each phase is shown to the user via a web page. For more information on each phase and how SDP works, see the “Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI” module.

## Certificate Revocation: Why It Occurs

After each participant has successfully enrolled in the PKI, the peers are ready to begin negotiations for a secure connection with each other. Thus, the peers present their certificates for validation followed by a revocation check. After the peer verifies that the other peer’s certificate was issued by an authenticated CA, the CRL or Online Certificate Status Protocol (OCSP) server is checked to ensure that the certificate has not been revoked by the issuing CA. The certificate usually contains a certificate distribution point (CDP) in the form of a URL. Cisco IOS software uses the CDP to locate and retrieve the CRL. If the CDP server does not respond, the Cisco IOS software reports an error, which may result in the peer’s certificate being rejected.

## Planning for a PKI

Planning for a PKI requires evaluating the requirements and expected use for each of the PKI components shown in [Figure 97](#). It is recommended that you (or the network administrator) thoroughly plan the PKI before beginning any PKI configuration.

Although there are a number of approaches to consider when planning the PKI, this document begins with peer-to-peer communication and proceeds as shown in [Figure 97](#). However you or the network administrator choose to plan the PKI, understand that certain decisions influence other decisions within the PKI. For example, the enrollment and deployment strategy could influence the planned CA hierarchy. Thus, it is important to understand how each component functions within the PKI and how certain component options are dependent upon decisions made earlier in the planning process.

## Where to Go Next

As suggested in [Figure 97](#), you begin to configure a PKI by setting up and deploying RSA keys. For more information, see the module “Deploying RSA Keys Within a PKI.”

## Additional References

The following sections provide references related to Cisco IOS PKI.

## Related Documents

| Related Topic                                                                                 | Document Title                                                                                      |
|-----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| PKI commands: complete command syntax, command mode, defaults, usage guidelines, and examples | <a href="#">Cisco IOS Security Command Reference</a>                                                |
| Certificate enrollment: supported methods, enrollment profiles, configuration tasks           | <a href="#">“Configuring Certificate Enrollment for a PKI” module</a>                               |
| Certificate revocation and authorization: configuration tasks                                 | <a href="#">“Configuring Revocation and Authorization of Certificates in a PKI” module</a>          |
| Cisco IOS certificate server overview information and configuration tasks                     | <a href="#">“Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment” module</a> |
| Secure Device Provisioning: functionality overview and configuration tasks                    | <a href="#">“Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI” module</a>        |
| Storing RSA keys and certificates on a USB eToken                                             | <a href="#">“Storing PKI Credentials” module</a>                                                    |

## Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

## MIBs

| MIBs | MIBs Link                                                                                                                                                                                                                  |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs     | Title                                                                                                             |
|----------|-------------------------------------------------------------------------------------------------------------------|
| RFC 2459 | <a href="#">Internet X.509 Public Key Infrastructure Certificate and CRL Profile</a>                              |
| RFC 2511 | <a href="#">Internet X.509 Certificate Request Message Format</a>                                                 |
| RFC 2527 | <a href="#">Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework</a> |
| RFC 2528 | <a href="#">Internet X.509 Public Key Infrastructure</a>                                                          |
| RFC 2559 | <a href="#">Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2</a>                           |
| RFC 2560 | <a href="#">X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP</a>                |

| RFCs     | Title                                                                                                       |
|----------|-------------------------------------------------------------------------------------------------------------|
| RFC 2585 | <a href="#">Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP</a>                |
| RFC 2587 | <a href="#">Internet X.509 Public Key Infrastructure LDAPv2 Schema</a>                                      |
| RFC 2875 | <a href="#">Diffie-Hellman Proof-of-Possession Algorithms</a>                                               |
| RFC 3029 | <a href="#">Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols</a> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                         | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Glossary

**CDP**—certificate distribution point. Field within a digital certificate containing information that describes how to retrieve the CRL for the certificate. The most common CDPs are HTTP and LDAP URLs. A CDP may also contain other types of URLs or an LDAP directory specification. Each CDP contains one URL or directory specification.

**certificates**—Electronic documents that bind a user's or device's name to its public key. Certificates are commonly used to validate a digital signature.

**CRL**—certificate revocation list. Electronic document that contains a list of revoked certificates. The CRL is created and digitally signed by the CA that originally issued the certificates. The CRL contains dates for when the certificate was issued and when it expires. A new CRL is issued when the current CRL expires.

**CA**—certification authority. Service responsible for managing certificate requests and issuing certificates to participating IPsec network devices. This service provides centralized key management for the participating devices and is explicitly trusted by the receiver to validate identities and to create digital certificates.

**peer certificate**—Certificate presented by a peer, which contains the peer's public key and is signed by the trustpoint CA.

**PKI**—public key infrastructure. System that manages encryption keys and identity information for components of a network that participate in secured communications.

**RA**—registration authority. Server that acts as a proxy for the CA so that CA functions can continue when the CA is offline. Although the RA is often part of the CA server, the RA could also be an additional application, requiring an additional device to run it.

**RSA keys**—Public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adleman. An RSA key pair (a public and a private key) is required before you can obtain a certificate for your router.

**Note**

---

Refer to *[Internetworking Terms and Acronyms](#)* for terms not included in this glossary.

---

---

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007, 2008 Cisco Systems, Inc. All rights reserved.







# Deploying RSA Keys Within a PKI

---

**First Published: May 2, 2005**

**Last Updated: November 17, 2006**

This module explains how to set up and deploy Rivest, Shamir, and Adelman (RSA) keys within a public key infrastructure (PKI). An RSA key pair (a public and a private key) is required before you can obtain a certificate for your router; that is, the end host must generate a pair of RSA keys and exchange the public key with the certification authority (CA) to obtain a certificate and enroll in a PKI.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all of the features documented in this module.* To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for RSA Keys Within a PKI”](#) section on page 20.

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for Configuring RSA Keys for a PKI, page 2](#)
- [Information About RSA Keys Configuration, page 2](#)
- [How to Set Up and Deploy RSA Keys Within a PKI, page 4](#)
- [Configuration Examples for RSA Key Pair Deployment, page 14](#)
- [Where to Go Next, page 19](#)
- [Additional References, page 19](#)
- [Feature Information for RSA Keys Within a PKI, page 20](#)



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

# Prerequisites for Configuring RSA Keys for a PKI

- Before setting up and deploying RSA keys for a PKI, you should be familiar with the module “Cisco IOS PKI Overview: Understanding and Planning a PKI.”
- As of Cisco IOS Release 12.3(7)T, all commands that begin as “crypto ca” have been changed to begin as “crypto pki.” Although the router will still accept crypto ca commands, all output will be read back as crypto pki.

## Information About RSA Keys Configuration

To deploy RSA keys within a PKI, you should understand the following concepts:

- [RSA Keys Overview, page 2](#)
- [Reasons to Store Multiple RSA Keys on a Router, page 3](#)
- [Benefits of Exportable RSA Keys, page 3](#)
- [Passphrase Protection While Importing and Exporting RSA Keys, page 4](#)

## RSA Keys Overview

An RSA key pair consists of a public key and a private key. When setting up your PKI, you must include the public key in the certificate enrollment request. After the certificate has been granted, the public key will be included in the certificate so that peers can use it to encrypt data that is sent to the router. The private key is kept on the router and used both to decrypt the data sent by peers and to digitally sign transactions when negotiating with peers.

RSA key pairs contain a key modulus value. The modulus determines the size of the RSA key. The larger the modulus, the more secure the RSA key. However, keys with large modulus values take longer to generate, and encryption and decryption operations take longer with larger keys.

If you want a modulus value between 512 and 1024, enter an integer value that is a multiple of 64. If you want a value higher than 1024, enter 1536 or 2048. If you enter a value greater than 512, key generation may take a minute or longer.

**Note**

---

As of Cisco IOS Release 12.4(11)T, peer *public* RSA key modulus values up to 4096 bits are automatically supported.

The largest private RSA key modulus is 2048 bits. Therefore, the largest RSA private key a router may generate or import is 2048 bits.

The recommended modulus value for a CA is 2048 bits; the recommended modulus value for a client is 1024 bits.

---

## Usage RSA Keys Versus General-Purpose RSA Keys

There are two mutually exclusive types of RSA key pairs—usage keys and general-purpose keys. When you generate RSA key pairs (via the **crypto key generate rsa** command), you will be prompted to select either usage keys or general-purpose keys.

### Usage RSA Keys

Usage keys consist of two RSA key pairs—one RSA key pair is generated and used for encryption and one RSA key pair is generated and used for signatures. With usage keys, each key is not unnecessarily exposed. (Without usage keys, one key is used for both authentication methods, increasing the exposure of that key.)

### General-Purpose RSA Keys

General-purpose keys consist of only one RSA key pair that used for both encryption and signatures. General-purpose key pairs are used more frequently than usage key pairs.

## Reasons to Store Multiple RSA Keys on a Router

Configuring multiple RSA key pairs allows the Cisco IOS software to maintain a different key pair for each CA with which it is dealing or the software can maintain multiple key pairs and certificates with the same CA. Thus, the Cisco IOS software can match policy requirements for each CA without compromising the requirements specified by the other CAs, such as key length, key lifetime, and general-purpose versus usage keys.

Named key pairs (which are specified via the **label** *key-label* option) allow you to have multiple RSA key pairs, enabling the Cisco IOS software to maintain a different key pair for each identity certificate.

## Benefits of Exportable RSA Keys



### Caution

Exportable RSA keys should be carefully evaluated before use because using exportable RSA keys introduces the risk that these keys might be exposed.

Any existing RSA keys are *not* exportable. New keys are generated as nonexportable by default. It is not possible to convert an existing nonexportable key to an exportable key.

As of Cisco IOS Release 12.2(15)T, users can share the private RSA key pair of a router with standby routers, therefore transferring the security credentials between networking devices. The key pair that is shared between two routers will allow one router to immediately and transparently take over the functionality of the other router. If the main router were to fail, the standby router could be dropped into the network to replace the failed router without the need to regenerate keys, reenroll with the CA, or manually redistribute keys.

Exporting and importing an RSA key pair also enables users to place the same RSA key pair on multiple routers so that all management stations using Secure Shell (SSH) can be configured with a single public RSA key.

### Exportable RSA Keys in PEM-Formatted Files

Using privacy-enhanced mail (PEM)-formatted files to import or export RSA keys can be helpful for customers who are running Cisco IOS software Release 12.3(4)T or later and who are using secure socket layer (SSL) or secure shell (SSH) applications to manually generate RSA key pairs and import the keys back into their PKI applications. PEM-formatted files allow customers to directly use existing RSA key pairs on their Cisco IOS routers instead of generating new keys.

## Passphrase Protection While Importing and Exporting RSA Keys

You have to include a passphrase to encrypt the PKCS12 file or the PEM file that will be exported, and when the PKCS12 or PEM file is imported, the same passphrase has to be entered to decrypt it. Encrypting the PKCS12 or PEM file when it is being exported, deleted, or imported protects the file from unauthorized access and use while it is being transported or stored on an external device.

The passphrase can be any phrase that is at least eight characters in length; it can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser.

### How to Convert an Exportable RSA Key Pair to a Nonexportable RSA Key Pair

Passphrase protection protects the external PKCS12 or PEM file from unauthorized access and use. To prevent an RSA key pair from being exported, it must be labeled “nonexportable.” To convert an exportable RSA key pair into a nonexportable key pair, the key pair must be exported and then reimported without specifying the “exportable” keyword.

## How to Set Up and Deploy RSA Keys Within a PKI

This section contains the following procedures:

- [Generating an RSA Key Pair, page 4](#)
- [Generating and Storing Multiple RSA Key Pairs, page 5](#)
- [Exporting and Importing RSA Keys, page 6](#)
- [Encrypting and Locking Private Keys on a Router, page 10](#)
- [Removing RSA Key Pair Settings, page 13](#)

## Generating an RSA Key Pair

Perform this task to manually generate an RSA key pair.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto key generate rsa {general-keys | usage-keys} [label *key-label*] [modulus *modulus-size*] [exportable]**
4. **exit**
5. **show crypto key mypubkey rsa**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                           | Purpose                                                                                                                                                                                                                |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                      | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                       |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                              | Enters global configuration mode.                                                                                                                                                                                      |
| Step 3 | <b>crypto key generate rsa {general-keys   usage-keys} [label key-label] [modulus modulus-size] [exportable]</b><br><br><b>Example:</b><br>Router(config)# crypto key generate rsa general-keys modulus 360 | Generates RSA key pairs. <ul style="list-style-type: none"> <li>If a <i>key-label</i> argument is not specified, the default value, which is the fully qualified domain name (FQDN) of the router, is used.</li> </ul> |
| Step 4 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                                                                                                  | Exits global configuration mode.                                                                                                                                                                                       |
| Step 5 | <b>show crypto key mypubkey rsa</b><br><br><b>Example:</b><br>Router# show crypto key mypubkey rsa                                                                                                          | (Optional) Displays the RSA public keys of your router.<br><br>This step allows you to verify that the RSA key pair has been successfully generated.                                                                   |

## What to Do Next

After you have successfully generated an RSA key pair, you can proceed to any of the additional tasks in this module to generate additional RSA key pairs, perform export and import of RSA key pairs, or configure additional security parameters for the RSA key pair (such as encrypting or locking the private key).

## Generating and Storing Multiple RSA Key Pairs

Perform this task to configure the router to generate and store multiple RSA key pairs and associate the key pairs with a trustpoint.

A trustpoint (also known as a CA) manages certificate requests and issues certificates to participating network devices. These services provide centralized key management for the participating devices and are explicitly trusted by the receiver to validate identities and to create digital certificates. Before any PKI operations can begin, the CA generates its own public key pair and creates a self-signed CA certificate; thereafter, the CA can sign certificate requests and begin peer enrollment for the PKI.

## Prerequisites

You must have already generated an RSA key pair as shown in the task “[Generating an RSA Key Pair](#).”

## SUMMARY STEPS

1. **crypto pki trustpoint *name***
2. **rsa-keypair *key-label* [*key-size* [*encryption-key-size*]]**
3. **exit**
4. **exit**
5. **show crypto key mypubkey rsa**

## DETAILED STEPS

|        | Command or Action                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>crypto pki trustpoint <i>name</i></b><br><br><b>Example:</b><br>Router(config)# crypto pki trustpoint fancy-ca                                          | Creates a trustpoint and enters ca-trustpoint configuration mode.                                                                                                                                                                                                                                  |
| Step 2 | <b>rsa-keypair <i>key-label</i> [<i>key-size</i> [<i>encryption-key-size</i>]]</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# rsa-keypair fancy-keys | Specifies the key pair that is to be used with the trustpoint. <ul style="list-style-type: none"> <li>Specify the <i>key-size</i> argument for generating the key and specify the <i>encryption-key-size</i> argument to request separate encryption, signature keys, and certificates.</li> </ul> |
| Step 3 | <b>exit</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# exit                                                                                          | Exits ca-trustpoint configuration mode.                                                                                                                                                                                                                                                            |
| Step 4 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                                                 | Exits global configuration mode.                                                                                                                                                                                                                                                                   |
| Step 5 | <b>show crypto key mypubkey rsa</b><br><br><b>Example:</b><br>Router# show crypto key mypubkey rsa                                                         | (Optional) Displays the RSA public keys of your router.<br><br>This step allows you to verify that the RSA key pair has been successfully generated.                                                                                                                                               |

## Exporting and Importing RSA Keys

This section contains the following tasks that can be used for exporting and importing RSA keys. Whether you are using PKCS12 files or PEM files, exportable RSA keys allow you to use existing RSA keys on Cisco IOS routers instead of having to generate new RSA keys if the main router were to fail.

- [Exporting and Importing RSA Keys in PKCS12 Files, page 7](#)
- [Exporting and Importing RSA Keys in PEM-Formatted Files, page 8](#)

## Exporting and Importing RSA Keys in PKCS12 Files

Exporting and importing RSA key pairs enables users to transfer security credentials between devices. The key pair that is shared between two devices allows one device to immediately and transparently take over the functionality of the other router.

### Prerequisites for Exporting and Importing RSA Key in PKCS12 Files

You must generate an RSA key pair and mark it “exportable” as specified in the task “[Generating an RSA Key Pair](#).”

### Restrictions for Exporting and Importing RSA Keys in PKCS12 Files

- You cannot export RSA keys that existed on the router before your system was upgraded to Cisco IOS Release 12.2(15)T or later. You have to generate new RSA keys and label them as “exportable” after you upgrade the Cisco IOS software.
- When you import a PKCS12 file that was generated by a third-party application, the PKCS12 file must include a CA certificate.
- If you want reexport an RSA key pair after you have already exported the key pair and imported them to a target router, you must specify the **exportable** keyword when you are importing the RSA key pair.
- The largest RSA key a router may import is 2048-bits.

### SUMMARY STEPS

1. **crypto pki trustpoint** *name*
2. **rsa***keypair* *key-label* [*key-size* [*encryption-key-size*]]
3. **exit**
4. **crypto pki export** *trustpointname* **pkcs12** *destination-url* *passphrase*
5. **crypto pki import** *trustpointname* **pkcs12** *source-url* *passphrase*
6. **exit**
7. **show crypto key mypubkey** *rsa*

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <pre>crypto pki trustpoint <i>name</i></pre> <p><b>Example:</b><br/>Router(config)# crypto pki trustpoint my-ca</p>                                                                                                     | Creates the trustpoint name that is to be associated with the RSA key pair and enters ca-trustpoint configuration mode.                                                                                                                                 |
| Step 2 | <pre>rsakeypair <i>key-label</i> [<i>key-size</i><br/>[<i>encryption-key-size</i>]]</pre> <p><b>Example:</b><br/>Router(ca-trustpoint)# rsakeypair my-keys</p>                                                          | Specifies the key pair that is to be used with the trustpoint.                                                                                                                                                                                          |
| Step 3 | <pre>exit</pre> <p><b>Example:</b><br/>Router(ca-trustpoint)# exit</p>                                                                                                                                                  | Exits ca-trustpoint configuration mode.                                                                                                                                                                                                                 |
| Step 4 | <pre>crypto pki export <i>trustpointname</i> pkcs12<br/><i>destination-url</i> <i>passphrase</i></pre> <p><b>Example:</b><br/>Router(config)# crypto pki export my-ca pkcs12<br/>tftp://tftpserver/my-keys PASSWORD</p> | <p>Exports the RSA keys via the trustpoint name.</p> <p><b>Note</b> You can export the trustpoint using any of the following file system types: flash, FTP, null, NVRAM, remote file copying (RCP), SCP, system, TFTP, Webflash, Xmodem, or Ymodem.</p> |
| Step 5 | <pre>crypto pki import <i>trustpointname</i> pkcs12<br/><i>source-url</i> <i>passphrase</i></pre> <p><b>Example:</b><br/>Router(config)# crypto pki import my-ca pkcs12<br/>tftp://tftpserver/my-keys PASSWORD</p>      | Imports the RSA keys to the target router.                                                                                                                                                                                                              |
| Step 6 | <pre>exit</pre> <p><b>Example:</b><br/>Router(config)# exit</p>                                                                                                                                                         | Exits global configuration mode.                                                                                                                                                                                                                        |
| Step 7 | <pre>show crypto key mypubkey rsa</pre> <p><b>Example:</b><br/>Router# show crypto key mypubkey rsa</p>                                                                                                                 | (Optional) Displays the RSA public keys of your router.                                                                                                                                                                                                 |

## Exporting and Importing RSA Keys in PEM-Formatted Files

Perform this task to export or import RSA key pairs in PEM files.

## Prerequisites for Exporting and Importing RSA Keys in PEM-Formatted Files

You must generate an RSA key pair and mark it “exportable” as specified in the task “[Generating an RSA Key Pair](#).”



## Restrictions for Exporting and Importing RSA Keys in PEM Formatted Files

- You cannot export and import RSA keys that were generated without an exportable flag before your system was upgraded to Cisco IOS Release 12.3(4)T or a later release. You have to generate new RSA keys after you upgrade the Cisco IOS software.
- The largest RSA key a router may import is 2048 bits.

## SUMMARY STEPS

1. **crypto key generate rsa** {usage-keys | general-keys} label *key-label* [exportable]
2. **crypto key export rsa** *key-label* **pem** {terminal | url *url*} {3des | des} *passphrase*
3. **crypto key import rsa** *key-label* **pem** [usage-keys] {terminal | url *url*} [exportable] *passphrase*

4. **exit**
5. **show crypto key mypubkey rsa**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                         | Purpose                                                                                                                                                                                                                                    |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>crypto key generate rsa</b> {usage-keys   general-keys} <b>label</b> key-label [ <b>exportable</b> ]<br><br><b>Example:</b><br>Router(config)# crypto key generate rsa general-keys label mykey exportable             | Generates RSA key pairs.<br><br>To use PEM files, the RSA key pair must be labeled exportable.                                                                                                                                             |
| Step 2 | <b>crypto key export rsa</b> key-label <b>pem</b> {terminal   url url} {3des   des} <i>passphrase</i><br><br><b>Example:</b><br>Router(config)# crypto key export rsa mycs pem url nvram: 3des PASSWORD                   | Exports the generated RSA key pair.<br><br><b>Tip</b> Be sure to keep the PEM file safe. For example, you may want to store it on another backup router.                                                                                   |
| Step 3 | <b>crypto key import rsa</b> key-label <b>pem</b> [usage-keys] {terminal   url url} [ <b>exportable</b> ] <i>passphrase</i><br><br><b>Example:</b><br>Router(config)# crypto key import rsa mycs2 pem url nvram: PASSWORD | Imports the generated RSA key pair.<br><br><b>Note</b> If you do not want the key to be exportable from your CA, import it back to the CA after it has been exported as a nonexportable key pair. Thus, the key cannot be taken off again. |
| Step 4 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                                                                                                                | Exits global configuration mode.                                                                                                                                                                                                           |
| Step 5 | <b>show crypto key mypubkey rsa</b><br><br><b>Example:</b><br>Router# show crypto key mypubkey rsa                                                                                                                        | (Optional) Displays the RSA public keys of your router.                                                                                                                                                                                    |

## Encrypting and Locking Private Keys on a Router

Digital signatures are used to authenticate one device to another device. To use digital signatures, private information (the private key) must be stored on the device that is providing the signature. The stored private information may aid an attacker who steals the hardware device that contains the private key; for example, a thief might be able to use the stolen router to initiate a secure connection to another site by using the RSA private keys stored in the router.



### Note

RSA keys are lost during password recovery operations. If you lose your password, the RSA keys will be deleted when you perform the password recovery operation. (This function prevents an attacker from performing password recovery and then using the keys.)

To protect the private RSA key from an attacker, a user can encrypt the private key that is stored in NVRAM via a passphrase. Users can also “lock” the private key, which blocks new connection attempts from a running router and protects the key in the router if the router is stolen by an attempted attacker.

Perform this task to encrypt and lock the private key that is saved to NVRAM.

## Prerequisites

Before encrypting or locking a private key, you should perform the following tasks:

- Generate an RSA key pair as shown in the task “[Generating an RSA Key Pair](#).”
- Optionally, you can authenticate and enroll each router with the CA server.



### Note

The RSA keys must be unlocked while enrolling the CA. The keys can be locked while authenticating the router with the CA because the private key of the router is not used during authentication.

## Restrictions for Encrypting and Locking Private Keys

### Backward Compatibility Restriction

Any image prior to Cisco IOS Release 12.3(7)T does not support encrypted keys. To prevent your router from losing all encrypted keys, ensure that only unencrypted keys are written to NVRAM before booting an image prior to Cisco IOS Release 12.3(7)T.

If you must download an image prior to Cisco IOS Release 12.3(7)T, decrypt the key and immediately save the configuration so the downloaded image does not overwrite the configuration.

### Interaction with Applications

An encrypted key is not effective after the router boots up until you manually unlock the key (via the **crypto key unlock rsa** command). Depending on which key pairs are encrypted, this functionality may adversely affect applications such as IP security (IPsec), SSH, and SSL; that is, management of the router over a secure channel may not be possible until the necessary key pair is unlocked.

## SUMMARY STEPS

1. **crypto key encrypt [write] rsa [name *key-name*] passphrase *passphrase***
2. **exit**
3. **show crypto key mypubkey rsa**
4. **crypto key lock rsa [name *key-name*] passphrase *passphrase***
5. **show crypto key mypubkey rsa**
6. **crypto key unlock rsa [name *key-name*] passphrase *passphrase***
7. **configure terminal**
8. **crypto key decrypt [write] rsa [name *key-name*] passphrase *passphrase***

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>crypto key encrypt</b> [ <b>write</b> ] <b>rsa</b> [ <b>name</b> <i>key-name</i> ]<br><b>passphrase</b> <i>passphrase</i><br><br><b>Example:</b><br>Router(config)# crypto key encrypt write rsa<br>name pki.company.com passphrase password | Encrypts the RSA keys.<br><br>After this command is issued, the router can continue to use the key; the key remains unlocked.<br><br><b>Note</b> If the <b>write</b> keyword is not issued, the configuration must be manually written to NVRAM; otherwise, the encrypted key will be lost next time the router is reloaded.                                                                                            |
| Step 2 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                                                                                                                                      | Exits global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 3 | <b>show crypto key mypubkey rsa</b><br><br><b>Example:</b><br>Router# show crypto key mypubkey rsa                                                                                                                                              | (Optional) Shows that the private key is encrypted (protected) and unlocked.<br><br><b>Note</b> You can also use this command to verify that applications such as Internet Key Exchange (IKE) and SSH are properly working after the key has been encrypted.                                                                                                                                                            |
| Step 4 | <b>crypto key lock rsa</b> [ <b>name</b> <i>key-name</i> ] <b>passphrase</b> <i>passphrase</i><br><br><b>Example:</b><br>Router# crypto key lock rsa name<br>pki.company.com passphrase password                                                | (Optional) Locks the encrypted private key on a running router.<br><br><b>Note</b> After the key is locked, it cannot be used to authenticate the router to a peer device. This behavior disables any IPsec or SSL connections that use the locked key.<br><br>Any existing IPsec tunnels created on the basis of the locked key will be closed.<br><br>If all RSA keys are locked, SSH will automatically be disabled. |
| Step 5 | <b>show crypto key mypubkey rsa</b><br><br><b>Example:</b><br>Router# show crypto key mypubkey rsa                                                                                                                                              | (Optional) Shows that the private key is protected and locked.<br><br>The output will also show failed connection attempts via applications such as IKE, SSH, and SSL.                                                                                                                                                                                                                                                  |
| Step 6 | <b>crypto key unlock rsa</b> [ <b>name</b> <i>key-name</i> ]<br><b>passphrase</b> <i>passphrase</i><br><br><b>Example:</b><br>Router# crypto key unlock rsa name<br>pki.company.com passphrase password                                         | (Optional) Unlocks the private key.<br><br><b>Note</b> After this command is issued, you can continue to establish IKE tunnels.                                                                                                                                                                                                                                                                                         |

|        | Command or Action                                                                                                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                              |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7 | <code>configure terminal</code><br><br><b>Example:</b><br>Router# <code>configure terminal</code>                                                                                                                                                           | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                    |
| Step 8 | <code>crypto key decrypt [write] rsa [name key-name]</code><br><code>passphrase passphrase</code><br><br><b>Example:</b><br>Router(config)# <code>crypto key decrypt write rsa</code><br>name <code>pki.company.com</code> <code>passphrase password</code> | (Optional) Deletes the encrypted key and leaves only the unencrypted key.<br><br><b>Note</b> The <b>write</b> keyword immediately saves the unencrypted key to NVRAM. If the <b>write</b> keyword is not issued, the configuration must be manually written to NVRAM; otherwise, the key will remain encrypted the next time the router is reloaded. |

## Removing RSA Key Pair Settings

You might want to remove an RSA key pair for one of the following reasons:

- During manual PKI operations and maintenance, old RSA keys can be removed and replaced with new keys.
- An existing CA is replaced and the new CA requires newly generated keys; for example, the required key size might have changed in an organization so you would have to delete the old 1024-bit keys and generate new 2048-bit keys.

Perform this task to remove all RSA keys or the specified RSA key pair that has been generated by your router.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `crypto key zeroize rsa [key-pair-label]`
4. `exit`
5. `show crypto key mypubkey rsa`

**DETAILED STEPS**

|        | Command or Action                                                                                                                      | Purpose                                                                                                                                                                                                                    |
|--------|----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                 | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                         | Enters global configuration mode.                                                                                                                                                                                          |
| Step 3 | <b>crypto key zeroize rsa</b> [ <i>key-pair-label</i> ]<br><br><b>Example:</b><br>Router(config)# crypto key zeroize rsa<br>fancy-keys | Deletes RSA key pairs from your router.<br><ul style="list-style-type: none"><li>• If the <i>key-pair-label</i> argument is not specified, all RSA keys that have been generated by your router will be deleted.</li></ul> |
| Step 4 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                             | Exits global configuration mode.                                                                                                                                                                                           |
| Step 5 | <b>show crypto key mypubkey rsa</b><br><br><b>Example:</b><br>Router# show crypto key mypubkey rsa                                     | (Optional) Displays the RSA public keys of your router.<br>This step allows you to verify that the RSA key pair has been successfully generated.                                                                           |

## Configuration Examples for RSA Key Pair Deployment

This section contains the following configuration examples:

- [Generating and Specifying RSA Keys: Example, page 14](#)
- [Exporting and Importing RSA Keys: Examples, page 14](#)
- [Encrypting and Locking Private Keys on a Router: Examples, page 18](#)

### Generating and Specifying RSA Keys: Example

The following example is a sample trustpoint configuration that shows how to generate and specify the RSA key pair “exampleCAkeys”:

```
crypto key generate rsa general-purpose exampleCAkeys
crypto ca trustpoint exampleCAkeys
 enroll url http://exampleCAkeys/certsrv/mscep/mscep.dll
 rsakeypair exampleCAkeys 1024 1024
```

### Exporting and Importing RSA Keys: Examples

This section contains the following configuration examples:

- [Exporting and Importing RSA Keys in PKCS12 Files: Example, page 15](#)
- [Generating, Exporting, Importing, and Verifying RSA Keys in PEM Files: Example, page 15](#)
- [Exporting Router RSA Key Pairs and Certificates from PEM Files: Example, page 16](#)
- [Importing Router RSA Key Pairs and Certificate from PEM Files: Example, page 18](#)

## Exporting and Importing RSA Keys in PKCS12 Files: Example

In the following example, an RSA key pair “mynewkp” is generated on Router A, and a trustpoint name “mynewtp” is created and associated with the RSA key pair. The trustpoint is exported to a TFTP server, so that it can be imported on Router B. By importing the trustpoint “mynewtp” to Router B, the user has imported the RSA key pair “mynewkp” to Router B.

### Router A

```
crypto key generate rsa general label mykeys exportable
! The name for the keys will be:mynewkp
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]
!
crypto pki trustpoint mynewtp
 rsakeypair mykeys
exit

crypto pki export mytp pkcs12 flash:myexport companyname
Destination filename [myexport]?
Writing pkcs12 file to tftp://mytftpserver/myexport
CRYPTO_PKI:Exported PKCS12 file successfully.
Verifying checksum... OK (0x3307)
!
Feb 18 17:30:09 GMT:%CRYPTO-6-PKCS12EXPORT_SUCCESS:PKCS #12 Successfully Exported.
```

### Router B

```
crypto pki import mynewtp pkcs12 flash:myexport companyname
Source filename [myexport]?
CRYPTO_PKI:Imported PKCS12 file successfully.

!
Feb 18 18:07:50 GMT:%CRYPTO-6-PKCS12IMPORT_SUCCESS:PKCS #12 Successfully Imported.
```

## Generating, Exporting, Importing, and Verifying RSA Keys in PEM Files: Example

The following example shows how to generate, export, bring the key back (import), and verify the status of the RSA key pair “mycs”:

```
! Generate the key pair
!
Router(config)# crypto key generate rsa general-purpose label mycs exportable
The name for the keys will be: mycs

Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys ...[OK]
!
```

```

! Archive the key pair to a remote location, and use a good password.
!
Router(config)# crypto key export rsa mycs pem url nvram:3des PASSWORD

% Key name:mycs
Usage:General Purpose Key
Exporting public key...
Destination filename [mycs.pub]?
Writing file to nvram:mycs.pub
Exporting private key...
Destination filename [mycs.prv]?
Writing file to nvram:mycs.prv
!
! Import the key as a different name.
!
Router(config)# crypto key import rsa mycs2 pem url nvram:mycs PASSWORD

% Importing public key or certificate PEM file...
Source filename [mycs.pub]?
Reading file from nvram:mycs.pub
% Importing private key PEM file...
Source filename [mycs.prv]?
Reading file from nvram:mycs.prv% Key pair import succeeded.
!
! After the key has been imported, it is no longer exportable.
!
! Verify the status of the key.
!
Router# show crypto key mypubkey rsa

% Key pair was generated at:18:04:56 GMT Jun 6 2003
Key name:mycs
Usage:General Purpose Key
Key is exportable.
Key Data:
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E65253
9C30C12E 295AB73F B1DF9FAD 86F88192 7D4FA4D2 8BA7FB49 9045BAB9 373A31CB
A6B1B8F4 329F2E7E 8A50997E AADBCFAA 23C29E19 C45F4F05 DBB2FA51 4B7E9F79
A1095115 759D6BC3 5DFB5D7F BCF655BF 6317DB12 A8287795 7D8DC6A3 D31B2486
C9C96D2C 2F70B50D 3B4CDDAE F661041A 445AE11D 002EEF08 F2A627A0 5B020301 0001
% Key pair was generated at:18:17:25 GMT Jun 6 2003
Key name:mycs2
Usage:General Purpose Key
Key is not exportable.
Key Data:
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E65253
9C30C12E 295AB73F B1DF9FAD 86F88192 7D4FA4D2 8BA7FB49 9045BAB9 373A31CB
A6B1B8F4 329F2E7E 8A50997E AADBCFAA 23C29E19 C45F4F05 DBB2FA51 4B7E9F79
A1095115 759D6BC3 5DFB5D7F BCF655BF 6317DB12 A8287795 7D8DC6A3 D31B2486
C9C96D2C 2F70B50D 3B4CDDAE F661041A 445AE11D 002EEF08 F2A627A0 5B020301 0001

```

## Exporting Router RSA Key Pairs and Certificates from PEM Files: Example

The following example shows how to generate and export the RSA key pair “aaa” and certificates of the router in PEM files that are associated with the trustpoint “mycs.” This example also shows PEM-formatted files, which include PEM boundaries before and after the base64-encoded data, that are used by other SSL and SSH applications.

```

Router(config)# crypto key generate rsa general-keys label aaa exportable

The name for the keys will be:aaa

```



Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

```

!
How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]
!
Router(config)# crypto pki trustpoint mycs
Router(ca-trustpoint)# enrollment url http://mycs
Router(ca-trustpoint)# rsakeypair aaa
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate mycs
Certificate has the following attributes:
Fingerprint:C21514AC 12815946 09F635ED FBB6CF31
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
!
Router(config)# crypto pki enroll mycs
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this password to the CA
Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.

Password:
Re-enter password:

% The fully-qualified domain name in the certificate will be: Router
% The subject name in the certificate will be:host.company.com
% Include the router serial number in the subject name? [yes/no]: n
% Include an IP address in the subject name? [no]: n
Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

Router(config)# Fingerprint:8DA777BC 08477073 A5BE2403 812DD157

00:29:11:%CRYPTO-6-CERTRET:Certificate received from Certificate Authority

Router(config)# crypto ca export aaa pem terminal 3des password
% CA certificate:
-----BEGIN CERTIFICATE-----
MIICAZCCAa2gAwIBAgIBATANBgkqhkiG9w0BAQUFADBOMQswCQYDVQQGEwJVUzES
<snip>
waDeNOSI3WlDa0AWq5DkVBkxwgn0TqIJXJOcTtjHnWHK1LMcMVGn
-----END CERTIFICATE-----

% Key name:aaa
Usage:General Purpose Key
-----BEGIN RSA PRIVATE KEY-----
Proc-Type:4,ENCRYPTED
DEK-Info:DES-EDE3-CBC,ED6B210B626BC81A

Urguv0jnJwOgowWVUQ2XR5nbzzYHI2vGLunPH/IxIsJuNjRVjbAAUpGk7VnPCT87
<snip>
kLC0txzEv7JHc72gMku9uUlrLSnFH5slzAtoC0czfU4=
-----END RSA PRIVATE KEY-----

% Certificate:
-----BEGIN CERTIFICATE-----
MIICTjCCAFigAwIBAgICIQUwDQYJKoZIhvcNAQEFBQAwTjELMAkGA1UEBhMCVVMx
<snip>
6x1BaIsuMxnHmr89KkKkYlU6

```

```
-----END CERTIFICATE-----
```

## Importing Router RSA Key Pairs and Certificate from PEM Files: Example

The following example shows how to import the RSA key pairs and certificate to the trustpoint “ggg” from PEM files via TFTP:

```
Router(config)# crypto pki import ggg pem url tftp://10.1.1.2/username/msca password
% Importing CA certificate...
Address or name of remote host [10.1.1.2]?
Destination filename [username/msca.ca]?
Reading file from tftp://10.1.1.2/username/msca.ca
Loading username/msca.ca from 10.1.1.2 (via Ethernet0):!
[OK - 1082 bytes]

% Importing private key PEM file...
Address or name of remote host [10.1.1.2]?
Destination filename [username/msca.prv]?
Reading file from tftp://10.1.1.2/username/msca.prv
Loading username/msca.prv from 10.1.1.2 (via Ethernet0):!
[OK - 573 bytes]

% Importing certificate PEM file...
Address or name of remote host [10.1.1.2]?
Destination filename [username/msca.crt]?
Reading file from tftp://10.1.1.2/username/msca.crt
Loading username/msca.crt from 10.1.1.2 (via Ethernet0):!
[OK - 1289 bytes]
% PEM files import succeeded.
Router(config)#
```

## Encrypting and Locking Private Keys on a Router: Examples

This section contains the following configuration examples:

- [Configuring and Verifying an Encrypted Key: Example, page 18](#)
- [Configuring and Verifying a Locked Key: Example, page 19](#)

### Configuring and Verifying an Encrypted Key: Example

The following example shows how to encrypt the RSA key “pki-123.company.com.” Thereafter, the **show crypto key mypubkey rsa** command is issued to verify that the RSA key is encrypted (protected) and unlocked.

```
Router(config)# crypto key encrypt rsa name pki-123.company.com passphrase password
Router(config)# exit
Router# show crypto key mypubkey rsa

% Key pair was generated at:00:15:32 GMT Jun 25 2003
Key name:pki-123.company.com
Usage:General Purpose Key
*** The key is protected and UNLOCKED. ***
Key is not exportable.
Key Data:
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E0CC9A 1D23B52C
CD00910C ABD392AE BA6D0E3F FC47A0EF 8AFEE340 0EC1E62B D40E7DCC
23C4D09E
03018B98 E0C07B42 3CFD1A32 2A3A13C0 1FF919C5 8DE9565F 1F020301 0001
```

```
% Key pair was generated at:00:15:33 GMT Jun 25 2003
Key name:pki-123.company.com.server
Usage:Encryption Key
Key is exportable.
Key Data:
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00D3491E 2A21D383
854D7DA8 58AFBDAC 4E11A7DD E6C40AC6 66473A9F 0C845120 7C0C6EC8 1FFF5757
3A41CE04 FDCB40A4 B9C68B4F BC7D624B 470339A3 DE739D3E F7DDB549 91CD4DA4
DF190D26 7033958C 8A61787B D40D28B8 29BCD0ED 4E6275C0 6D020301 0001
Router#
```

## Configuring and Verifying a Locked Key: Example

The following example shows how to lock the key “pki-123.company.com.” Thereafter, the **show crypto key mypubkey rsa** command is issued to verify that the key is protected (encrypted) and locked.

```
Router# crypto key lock rsa name pki-123.company.com passphrase password
!
Router# show crypto key mypubkey rsa

% Key pair was generated at:20:29:41 GMT Jun 20 2003
Key name:pki-123.company.com
Usage:General Purpose Key
*** The key is protected and LOCKED. ***
Key is exportable.
Key Data:
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00D7808D C5FF14AC
0D2B55AC 5D199F2F 7CB4B355 C555E07B 6D0DECBE 4519B1F0 75B12D6F 902D6E9F
B6FDAD8D 654EF851 5701D5D7 EDA047ED 9A2A619D 5639DF18 EB020301 0001
```

## Where to Go Next

After you have generated an RSA key pair, you should set up the trustpoint. If you have already set up the trustpoint, you should authenticate and enroll the routers in a PKI. For information on enrollment, see the module “Configuring Certificate Enrollment for a PKI.”

## Additional References

The following sections provide references related to configuring RSA keys for a PKI.

## Related Documents

| Related Topic                                                                                 | Document Title                                                                    |
|-----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Overview of PKI, including RSA keys, certificate enrollment, and CAs                          | <a href="#">“Cisco IOS PKI Overview: Understanding and Planning a PKI” module</a> |
| PKI commands: complete command syntax, command mode, defaults, usage guidelines, and examples | <a href="#">Cisco IOS Security Command Reference</a>                              |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                  | Link                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and technical documentation. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Feature Information for RSA Keys Within a PKI

Table 57 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the *“Implementing and Managing PKI Features Roadmap”*.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



### Note

Table 57 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 57**      **Feature Information for RSA Keys Within a PKI**

| Feature Name                                          | Software Releases                     | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco IOS 4096-Bit Public Key Support                 | 12.4(12)T                             | <p>This feature introduces Cisco IOS 4096-bit public key support.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">RSA Keys Overview</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Exporting and Importing RSA Keys                      | 12.2(15)T<br>Cisco IOS XE Release 2.1 | <p>This feature allows you to transfer security credentials between devices by exporting and importing RSA keys. The key pair that is shared between two devices will allow one device to immediately and transparently take over the functionality of the other router.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Benefits of Exportable RSA Keys</a></li> <li>• <a href="#">Exporting and Importing RSA Keys in PKCS12 Files</a></li> </ul> <p>The following commands were introduced or modified by this feature: <b>crypto ca export pkcs12</b>, <b>crypto ca import pkcs12</b>, <b>crypto key generate rsa (IKE)</b></p> |
| Import of RSA Key Pair and Certificates in PEM Format | 12.3(4)T<br>Cisco IOS XE Release 2.1  | <p>This feature allows customers to use PEM-formatted files to import or export RSA key pairs. PEM-formatted files allow customers to directly use existing RSA key pairs on their Cisco IOS routers instead of generating new keys.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Benefits of Exportable RSA Keys</a></li> <li>• <a href="#">Exporting and Importing RSA Keys in PEM-Formatted Files</a></li> </ul> <p>The following commands were introduced by this feature: <b>crypto ca export pem</b>, <b>crypto ca import pem</b>, <b>crypto key export pem</b>, <b>crypto key import pem</b></p>                          |

**Table 57**      **Feature Information for RSA Keys Within a PKI (continued)**

| Feature Name                  | Software Releases                       | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Multiple RSA Key Pair Support | 12.2(8)T<br>Cisco IOS XE<br>Release 2.1 | <p>This feature allows a user to configure a router to have multiple RSA key pairs. Thus, the Cisco IOS software can maintain a different key pair for each identity certificate.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Reasons to Store Multiple RSA Keys on a Router</a></li> <li>• <a href="#">Generating and Storing Multiple RSA Key Pairs</a></li> </ul> <p>The following commands were introduced or modified by this feature: <b>crypto key generate rsa</b>, <b>crypto key zeroize rsa</b>, <b>rsa keypair</b></p> |
| Protected Private Key Storage | 12.3(7)T<br>Cisco IOS XE<br>Release 2.1 | <p>This feature allows a user to encrypt and lock the RSA private keys that are used on a Cisco IOS router, thereby, preventing unauthorized use of the private keys.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Encrypting and Locking Private Keys on a Router</a></li> </ul> <p>The following commands were introduced or modified by this feature: <b>crypto key decrypt rsa</b>, <b>crypto key encrypt rsa</b>, <b>crypto key lock rsa</b>, <b>crypto key unlock rsa</b>, <b>show crypto key mypubkey rsa</b></p>           |

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



# Configuring Authorization and Revocation of Certificates in a PKI

---

**First Published: May 2, 2005**

Last Updated: June 19, 2006

This module describes how to configure authorization and revocation of certificates in a public key infrastructure (PKI).

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Certificate Authorization and Revocation](#)” section on page 40.*

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for Authorization and Revocation of Certificates](#), page 2
- [Information About Authorization and Revocation of Certificates](#), page 2
- [How to Configure Authorization and Revocation of Certificates for Your PKI](#), page 9
- [Configuration Examples for Setting Up Authorization and Revocation of Certificates](#), page 26
- [Additional References](#), page 39
- [Feature Information for Certificate Authorization and Revocation](#), page 40



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

# Prerequisites for Authorization and Revocation of Certificates

## Plan Your PKI Strategy



### Tip

It is strongly recommended that you plan your entire PKI strategy before you begin to deploy actual certificates.

Authorization and revocation can occur only after you or a network administrator have completed the following tasks:

- Configured the CA.
- Enrolled peer devices with the CA.
- Identified and configured the protocol (such as IP Security [IPsec] or secure socket layer [SSL]) that is to be used for peer-to-peer communication.

You should decide which authorization and revocation strategy you are going to configure before enrolling peer devices because the peer device certificates might have to contain authorization and revocation-specific information.

### “crypto ca” to “crypto pki” CLI Change

As of Cisco IOS Release 12.3(7)T, all commands that begin as “crypto ca” have been changed to begin as “crypto pki.” Although the router will still accept crypto ca commands, all output will be read back as crypto pki.

## Information About Authorization and Revocation of Certificates

Before configuring certificate authorization and revocation, you should understand the following concepts:

- [PKI Authorization, page 2](#)
- [PKI and AAA Server Integration for Certificate Status, page 3](#)
- [CRLs or OCSP Server: Choosing a Certificate Revocation Mechanism, page 4](#)
- [When to Use Certificate-Based ACLs for Authorization or Revocation, page 7](#)
- [PKI Certificate Chain Validation, page 8](#)

## PKI Authorization

PKI authentication does not provide authorization. Current solutions for authorization are specific to the router that is being configured, although a centrally managed solution is often required.

There is not a standard mechanism by which certificates are defined as authorized for some tasks and not for others. This authorization information can be captured in the certificate itself if the application is aware of the certificate-based authorization information. But this solution does not provide a simple mechanism for real-time updates to the authorization information and forces each application to be aware of the specific authorization information embedded in the certificate.



When the certificate-based ACL mechanism is configured as part of the trustpoint authentication, the application is no longer responsible for determining this authorization information, and it is no longer possible to specify for which application the certificate is authorized. In some cases, the certificate-based ACL on the router gets so large that it cannot be managed. Additionally, it is beneficial to retrieve certificate-based ACL indications from an external server. (For more information on using certificate-based ACLs for authentication, see the section [“When to Use Certificate-Based ACLs for Authorization or Revocation.”](#))

Current solutions to the real-time authorization problem involve specifying a new protocol and building a new server (with associated tasks, such as management and data distribution).

## PKI and AAA Server Integration for Certificate Status

Integrating your PKI with an authentication, authorization, and accounting (AAA) server provides an alternative online certificate status solution that leverages the existing AAA infrastructure. Certificates can be listed in the AAA database with appropriate levels of authorization. For components that do not explicitly support PKI-AAA, a default label of “all” from the AAA server provides authorization. Likewise, a label of “none” from the AAA database indicates that the specified certificate is not valid. (The absence of any application label is equivalent, but “none” is included for completeness and clarity). If the application component does support PKI-AAA, the component may be specified directly; for example, the application component could be “ipsec,” “ssl,” or “osp.” (ipsec=IP Security, ssl=Secure Sockets Layer, and osp=Open Settlement Protocol.)



### Note

- Currently, no application component supports specification of the application label.
- There may be a time delay when accessing the AAA server. If the AAA server is not available, the authorization fails.

## RADIUS or TACACS+: Choosing a AAA Server Protocol

The AAA server can be configured to work with either the RADIUS or TACACS+ protocol. When you are configuring the AAA server for the PKI integration, you must set the RADIUS or TACACS attributes that are required for authorization.

If the RADIUS protocol is used, the password that is configured for the username in the AAA server should be set to “cisco,” which is acceptable because the certificate validation provides authentication and the AAA database is only being used for authorization. When the TACACS protocol is used, the password that is configured for the username in the AAA server is irrelevant because TACACS supports authorization without requiring authentication (the password is used for authentication).

In addition, if you are using TACACS, you must add a PKI service to the AAA server. The custom attribute “cert-application=all” is added under the PKI service for the particular user or usergroup to authorize the specific username.

## Attribute-Value Pairs for PKI and AAA Server Integration

[Table 1](#) lists the attribute-value (AV) pairs that are to be used when setting up PKI integration with a AAA server. (Note the values shown in the table are possible values.) The AV pairs must match the client configuration. If they do not match, the peer certificate is not authorized.

**Note**

Users can sometimes have AV pairs that are different from those of every other user. As a result, a unique username is required for each user. The **all** parameter (within the **authorization username** command) specifies that the entire subject name of the certificate will be used as the authorization username.

**Table 1** *AV Pairs That Must Match*

| AV Pair                                             | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cisco-avpair=pki:cert-application=all               | Valid values are “all” and “none.”                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| cisco-avpair=pki:cert-trustpoint=msca               | <p>The value is a Cisco IOS command-line interface (CLI) configuration trustpoint label.</p> <p><b>Note</b> The cert-trustpoint AV pair is normally optional. If it is specified, the Cisco IOS router query must be coming from a certificate trustpoint that has a matching label, and the certificate that is authenticated must have the specified certificate serial number.</p>                                                                                                                                                                                                                               |
| cisco-avpair=pki:cert-serial=16318DB7000100001671   | <p>The value is a certificate serial number.</p> <p><b>Note</b> The cert-serial AV pair is normally optional. If it is specified, the Cisco IOS router query must be coming from a certificate trustpoint that has a matching label, and the certificate that is authenticated must have the specified certificate serial number.</p>                                                                                                                                                                                                                                                                               |
| cisco-avpair=pki:cert-lifetime-end=1:00 jan 1, 2003 | <p>The cert-lifetime-end AV pair is available to artificially extend a certificate lifetime beyond the time period that is indicated in the certificate itself. If the cert-lifetime-end AV pair is used, the cert-trustpoint and cert-serial AV pairs must also be specified. The value must match the following form: hours:minutes month day, year.</p> <p><b>Note</b> Only the first three characters of a month are used: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. If more than three characters are entered for the month, the remaining characters are ignored (for example Janxxxx).</p> |

## CRLs or OCSP Server: Choosing a Certificate Revocation Mechanism

After a certificate is validated as a properly signed certificate, a certificate revocation method is performed to ensure that the certificate has not been revoked by the issuing CA. Cisco IOS software supports two revocation mechanisms—certificate revocation lists (CRLs) and Online Certificate Status Protocol (OCSP). (Cisco IOS software also supports AAA integration for certificate checking; however, additional authorization functionality is included. For more information on PKI and AAA certificate authorization and status check, see the section “[PKI and AAA Server Integration for Certificate Status](#).”)

The following sections explain how each revocation mechanism works:

- [What Is a CRL?, page 5](#)
- [What Is OCSP?, page 6](#)

## What Is a CRL?

A certificate revocation list (CRL) contains a list of revoked certificates. The CRL is created and digitally signed by the CA that originally issued the certificates. The CRL contains dates for when each certificate was issued and when it expires.

CAs publish new CRLs periodically or when a certificate for which the CA is responsible has been revoked. By default, a new CRL will be downloaded after the currently cached CRL expires. An administrator may also configure the duration for which CRLs are cached in router memory or disable CRL caching completely. The CRL caching configuration will apply to all CRLs associated with a trustpoint.

When the CRL expires, the router deletes it from its cache. A new CRL is downloaded when a certificate is presented for verification; however, if a newer version of the CRL that lists the certificate under examination is on the server but the router is still using the CRL in its cache, the router will not know that the certificate has been revoked. The certificate will pass the revocation check even though it should have been denied.

When a CA issues a certificate, the CA can include in the certificate the CRL distribution point (CDP) for that certificate. Cisco IOS client devices use CDPs to locate and load the correct CRL. The Cisco IOS client supports multiple CDPs, but the Cisco IOS CA currently supports only one CDP; however, third-party vendor CAs may support multiple CDPs or different CDPs per certificate. If a CDP is not specified in the certificate, the client device will use the default Simple Certificate Enrollment Protocol (SCEP) method to retrieve the CRL. (The CDP location can be specified via the **cdp-url** command.)

When implementing CRLs, you should consider the following design considerations:

- CRL lifetimes and the security association (SA) and Internet Key Exchange (IKE) lifetimes  
The CRL lifetime determines the length of time between CA-issued updates to the CRL. (The default CRL lifetime value, which is 168 hours [1 week], can be changed via the **lifetime crl** command.)
- The method and location of the CDP
  - The method determines how the CRL is retrieved; some possible choices include HTTP, Lightweight Directory Access Protocol (LDAP), SCEP, or TFTP.  
HTTP, TFTP, and LDAP are the most commonly used methods. Although Cisco IOS software defaults to SCEP, an HTTP CDP is recommended for large installations using CRLs because HTTP can be made highly scalable.
  - The location determines from where the CRL is retrieved; for example, you can specify the server and file path from which to retrieve the CRL.

## Querying All CDPs During Revocation Check

When a CDP server does not respond to a request, the Cisco IOS software reports an error, which may result in the peer's certificate being rejected. To prevent a possible certificate rejection and if there are multiple CDPs in a certificate, the Cisco IOS software will attempt to use the CDPs in the order in which they appear in the certificate. The router will attempt to retrieve a CRL using each CDP URL or directory specification. If an error occurs using a CDP, an attempt will be made using the next CDP.

**Note**

Prior to Cisco IOS Release 12.3(7)T, the Cisco IOS software makes only one attempt to retrieve the CRL, even when the certificate contains more than one CDP.

**Tip**

Although the Cisco IOS software will make every attempt to obtain the CRL from one of the indicated CDPs, it is recommended that you use an HTTP CDP server with high-speed redundant HTTP servers to avoid application timeouts because of slow CDP responses.

## What Is OCSP?

OCSP is an online mechanism that is used to determine certificate validity and provides the following flexibility as a revocation mechanism:

- OCSP can provide real-time certificate status checking.
- OCSP allows the network administrator to specify a central OCSP server, which can service all devices within a network.
- OCSP also allows the network administrator the flexibility to specify multiple OCSP servers, either per client certificate or per group of client certificates.
- OCSP server validation is usually based on the root CA certificate or a valid subordinate CA certificate, but may also be configured so that external CA certificates or self-signed certificates may be used. Using external CA certificates or self-signed certificates allows the OCSP servers certificate to be issued and validated from an alternative PKI hierarchy.

A network administrator can configure an OCSP server to collect and update CRLs from different CA servers. The devices within the network can rely on the OCSP server to check the certificate status without retrieving and caching each CRL for every peer. When peers have to check the revocation status of a certificate, they send a query to the OCSP server that includes the serial number of the certificate in question and an optional unique identifier for the OCSP request, or a nonce. The OCSP server holds a copy of the CRL to determine if the CA has listed the certificate as being revoked; the server then responds to the peer including the nonce. If the nonce in the response from the OCSP server does not match the original nonce sent by the peer, the response is considered invalid and certificate verification fails. The dialog between the OCSP server and the peer consumes less bandwidth than most CRL downloads.

If the OCSP server is using a CRL, CRL time limitations will be applicable; that is, a CRL that is still valid might be used by the OCSP server although a new CRL has been issued by the CRL containing additional certificate revocation information. Because fewer devices are downloading the CRL information on a regular basis, you can decrease the CRL lifetime value or configure the OCSP server not to cache the CRL. For more information, check your OCSP server documentation.

## When to Use an OCSP Server

OCSP may be more appropriate than CRLs if your PKI has any of the following characteristics:

- Real-time certificate revocation status is necessary. CRLs are updated only periodically and the latest CRL may not always be cached by the client device. For example, if a client does not yet have the latest CRL cached and a newly revoked certificate is being checked, that revoked certificate will successfully pass the revocation check.

- There are a large number of revoked certificates or multiple CRLs. Caching a large CRL consumes large portions of Cisco IOS memory and may reduce resources available to other processes.
- CRLs expire frequently, causing the CDP to handle a larger load of CRLs.

**Note**

As of Cisco IOS Release 12.4(9)T or later, an administrator may configure CRL caching, either by disabling CRL caching completely or setting a maximum lifetime for a cached CRL per trustpoint.

## When to Use Certificate-Based ACLs for Authorization or Revocation

Certificates contain several fields that are used to determine whether a device or user is authorized to perform a specified action.

Because certificate-based ACLs are configured on the device, they do not scale well for large numbers of ACLs; however, certificate-based ACLs do provide very granular control of specific device behavior. Certificate-based ACLs are also leveraged by additional features to help determine when PKI components such as revocation, authorization, or a trustpoint should be used. They provide a general mechanism allowing users to select a specific certificate or a group of certificates that are being validated for either authorization or additional processing.

Certificate-based ACLs specify one or more fields within the certificate and an acceptable value for each specified field. You can specify which fields within a certificate should be checked and which values those fields may or may not have.

There are six logical tests for comparing the field with the value—equal, not equal, contains, does not contain, less than, and greater than or equal. If more than one field is specified within a single certificate-based ACL, the tests of all of the fields within the ACL must succeed to match the ACL. The same field may be specified multiple times within the same ACL. More than one ACL may be specified, and ACL will be processed in turn until a match is found or all of the ACLs have been processed.

## Ignore Revocation Checks Using a Certificate-Based ACL

Certificate-based ACLs can be configured to instruct your router to ignore the revocation check and expired certificates of a valid peer. Thus, a certificate that meets the specified criteria can be accepted regardless of the validity period of the certificate, or if the certificate meets the specified criteria, revocation checking does not have to be performed. You can also use a certificate-based ACL to ignore the revocation check when the communication with a AAA server is protected with a certificate.

### Ignoring Revocation Lists

To allow a trustpoint to enforce CRLs except for specific certificates, enter the **match certificate** command with the **skip revocation-check** keyword. This type of enforcement is most useful in a hub-and-spoke configuration in which you also want to allow direct spoke-to-spoke connections. In pure hub-and-spoke configurations, all spokes connect only to the hub, so CRL checking is necessary only on the hub. For one spoke to communicate directly with another spoke, the **match certificate** command with the **skip revocation-check** keyword can be used for neighboring peer certificates instead of requiring a CRL on each spoke.

### Ignoring Expired Certificates

To configure your router to ignore expired certificates, enter the **match certificate** command with the **allow expired-certificate** keyword. This command has the following purposes:

- If the certificate of a peer has expired, this command may be used to “allow” the expired certificate until the peer can obtain a new certificate.
- If your router clock has not yet been set to the correct time, the certificate of a peer will appear to be not yet valid until the clock is set. This command may be used to allow the certificate of the peer even though your router clock is not set.

**Note**

- If Network Time Protocol (NTP) is available only via the IPsec connection (usually via the hub in a hub-and-spoke configuration), the router clock can never be set. The tunnel to the hub cannot be “brought up” because the certificate of the hub is not yet valid.
- “Expired” is a generic term for a certificate that is expired or that is not yet valid. The certificate has a start and end time. An expired certificate, for purposes of the ACL, is one for which the current time of the router is outside the start and end times specified in the certificate.

**Skipping the AAA Check of the Certificate**

If the communication with an AAA server is protected with a certificate, and you want to skip the AAA check of the certificate, use the **match certificate** command with the **skip authorization-check** keyword. For example, if a virtual private network (VPN) tunnel is configured so that all AAA traffic goes over that tunnel, and the tunnel is protected with a certificate, you can use the **match certificate** command with the **skip authorization-check** keyword to skip the certificate check so that the tunnel can be established.

The **match certificate** command and the **skip authorization-check** keyword should be configured after PKI integration with an AAA server is configured.

**Note**

If the AAA server is available only via an IPsec connection, the AAA server cannot be contacted until after the IPsec connection is established. The IPsec connection cannot be “brought up” because the certificate of the AAA server is not yet valid.

## PKI Certificate Chain Validation

A certificate chain establishes a sequence of trusted certificates—from a peer certificate to the root CA certificate. Within a PKI hierarchy, all enrolled peers can validate the certificate of one another if the peers share a trusted root CA certificate or a common subordinate CA. Each CA corresponds to a trustpoint.

When a certificate chain is received from a peer, the default processing of a certificate chain path continues until the first trusted certificate, or trustpoint, is reached. In Cisco IOS Release 12.4(6)T and later releases, an administrator may configure the level to which a certificate chain is processed on all certificates including subordinate CA certificates.

Configuring the level to which a certificate chain is processed allows for the reauthentication of trusted certificates, the extension of a trusted certificate chain, and the completion of a certificate chain that contains a gap.

**Reauthentication of Trusted Certificates**

The default behavior is for the router to remove any trusted certificates from the certificate chain sent by the peer before the chain is validated. An administrator may configure certificate chain path processing so that the router does not remove CA certificates that are already trusted before chain validation, so that all certificates in the chain are re-authenticated for the current session.

### Extending the Trusted Certificate Chain

The default behavior is for the router to use its trusted certificates to extend the certificate chain if there are any missing certificates in the certificate chain sent by the peer. The router will validate only certificates in the chain sent by the peer. An administrator may configure certificate chain path processing so that the certificates in the peer's certificate chain and the router's trusted certificates are validated to a specified point.

### Completing Gaps in a Certificate Chain

An administrator may configure certificate chain processing so that if there is a gap in the configured Cisco IOS trustpoint hierarchy, certificates sent by the peer can be used to complete the set of certificates to be validated.

**Note**

If the trustpoint is configured to require parent validation and the peer does not provide the full certificate chain, the gap cannot be completed and the certificate chain is rejected and invalid.

**Note**

It is a configuration error if the trustpoint is configured to require parent validation and there is no parent trustpoint configured. The resulting certificate chain gap cannot be completed and the subordinate CA certificate cannot be validated. The certificate chain is invalid.

## How to Configure Authorization and Revocation of Certificates for Your PKI

This section contains the following procedures:

- [Configuring PKI Integration with a AAA Server, page 9](#)
- [Configuring a Revocation Mechanism for PKI Certificate Status Checking, page 13](#)
- [Configuring Certificate Authorization and Revocation Settings, page 16](#)
- [Configuring Certificate Chain Validation, page 25](#)

## Configuring PKI Integration with a AAA Server

Perform this task to generate a AAA username from the certificate presented by the peer and specify which fields within a certificate should be used to build the AAA database username.

### Restrictions When Using the Entire Subject Name for PKI Authorization

The following restrictions should be considered when using the **all** keyword as the subject name for the **authorization username** command:

- Some AAA servers limit the length of the username (for example, to 64 characters). As a result, the entire certificate subject name cannot be longer than the limitation of the server.
- Some AAA servers limit the available character set that may be used for the username (for example, a space [ ] and an equal sign [=] may not be acceptable). You cannot use the **all** keyword for a AAA server having such a character-set limitation.

- The **subject-name** command in the trustpoint configuration may not always be the final AAA subject name. If the fully qualified domain name (FQDN), serial number, or IP address of the router are included in a certificate request, the subject name field of the issued certificate will also have these components. To turn off the components, use the **fqdn**, **serial-number**, and **ip-address** commands with the **none** keyword.
- CA servers sometimes change the requested subject name field when they issue a certificate. For example, CA servers of some vendors switch the relative distinguished names (RDNs) in the requested subject names to the following order: CN, OU, O, L, ST, and C. However, another CA server might append the configured LDAP directory root (for example, O=cisco.com) to the end of the requested subject name.
- Depending on the tools you choose for displaying a certificate, the printed order of the RDNs in the subject name could be different. Cisco IOS software always displays the least significant RDN first, but other software, such as Open Source Secure Socket Layer (OpenSSL), does the opposite. Therefore, if you are configuring a AAA server with a full distinguished name (DN) (subject name) as the corresponding username, ensure that the Cisco IOS software style (that is, with the least significant RDN first) is used.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authorization network** *listname* [*method*]
5. **crypto pki trustpoint** *name*
6. **enrollment url** *url*
7. **revocation-check** *method*
8. **exit**
9. **authorization username** {*subjectname* *subjectname*}
10. **authorization list** *listname*
11. **tacacs-server host** *hostname* [**key** *string*]  
or  
**radius-server host** *hostname* [**key** *string*]

## DETAILED STEPS

|        | Command or Action                             | Purpose                                                                                                            |
|--------|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
|        | <b>Example:</b><br>Router> enable             |                                                                                                                    |
| Step 2 | <b>configure terminal</b>                     | Enters global configuration mode.                                                                                  |
|        | <b>Example:</b><br>Router# configure terminal |                                                                                                                    |



|        | Command or Action                                                                                                                               | Purpose                                                                                                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>aaa new-model</b><br><br><b>Example:</b><br>Router(config)# aaa new-model                                                                    | Enables the AAA access control model.                                                                                                                                                                     |
| Step 4 | <b>aaa authorization network listname [method]</b><br><br><b>Example:</b><br>Router (config)# aaa authorization network<br>maxaaa group tacacs+ | Sets the parameters that restrict user access to a network. <ul style="list-style-type: none"> <li><i>method</i>—Can be <b>group radius</b>, <b>group tacacs+</b>, or <b>group group-name</b>.</li> </ul> |
| Step 5 | <b>crypto pki trustpoint name</b><br><br><b>Example:</b><br>Route (config)# crypto pki trustpoint msca                                          | Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.                                                                                                                     |
| Step 6 | <b>enrollment url url</b><br><br><b>Example:</b><br>Router (ca-trustpoint)# enrollment url<br>http://caserver.mycompany.com                     | Specifies the enrollment parameters of your CA. <ul style="list-style-type: none"> <li>The <i>url</i> argument is the URL of the CA to which your router should send certificate requests.</li> </ul>     |
| Step 7 | <b>revocation-check method</b><br><br><b>Example:</b><br>Router (ca-trustpoint)# revocation-check crl                                           | (Optional) Checks the revocation status of a certificate.                                                                                                                                                 |
| Step 8 | <b>exit</b><br><br><b>Example:</b><br>Router (ca-trustpoint)# exit                                                                              | Exits ca-trustpoint configuration mode and returns to global configuration mode.                                                                                                                          |

|         | Command or Action                                                                                                                                                                                                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 9  | <p><b>authorization username</b> {<b>subjectname</b> <i>subjectname</i>}</p> <p><b>Example:</b><br/>Router (config)# authorization username <i>subjectname</i> <i>serialnumber</i></p>                                                                                                                                                                            | <p>Sets parameters for the different certificate fields that are used to build the AAA username.</p> <p>The <i>subjectname</i> argument can be any of the following:</p> <ul style="list-style-type: none"> <li>• <b>all</b>—Entire distinguished name (subject name) of the certificate.</li> <li>• <b>commonname</b>—Certification common name.</li> <li>• <b>country</b>—Certificate country.</li> <li>• <b>email</b>—Certificate e-mail.</li> <li>• <b>ipaddress</b>—Certificate IP address.</li> <li>• <b>locality</b>—Certificate locality.</li> <li>• <b>organization</b>—Certificate organization.</li> <li>• <b>organizationalunit</b>—Certificate organizational unit.</li> <li>• <b>postalcode</b>—Certificate postal code.</li> <li>• <b>serialnumber</b>—Certificate serial number.</li> <li>• <b>state</b>—Certificate state field.</li> <li>• <b>streetaddress</b>—Certificate street address.</li> <li>• <b>title</b>—Certificate title.</li> <li>• <b>unstructuredname</b>—Certificate unstructured name.</li> </ul> |
| Step 10 | <p><b>authorization list</b> <i>listname</i></p> <p><b>Example:</b><br/>Route (config)# authorization list maxaaa</p>                                                                                                                                                                                                                                             | Specifies the AAA authorization list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 11 | <p><b>tacacs-server host</b> <i>hostname</i> [<b>key</b> <i>string</i>]</p> <p><b>Example:</b><br/>Router(config)# tacacs-server host 192.0.2.2<br/>key a_secret_key</p> <p>or</p> <p><b>radius-server host</b> <i>hostname</i> [<b>key</b> <i>string</i>]</p> <p><b>Example:</b><br/>Router(config)# radius-server host 192.0.2.1<br/>key another_secret_key</p> | <p>Specifies a TACACS+ host.</p> <p>or</p> <p>Specifies a RADIUS host.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## Troubleshooting Tips

To display debug messages for the trace of interaction (message type) between the CA and the router, use the **debug crypto pki transactions** command. (See the sample output, which shows a successful PKI integration with AAA server exchange and a failed PKI integration with AAA server exchange.)

### Successful Exchange

Router# **debug crypto pki transactions**

```
Apr 22 23:15:03.695: CRYPTO_PKI: Found a issuer match
Apr 22 23:15:03.955: CRYPTO_PKI: cert revocation status unknown.
Apr 22 23:15:03.955: CRYPTO_PKI: Certificate validated without revocation check
```

Each line that shows “CRYPTO\_PKI\_AAA” indicates the state of the AAA authorization checks. Each of the AAA AV pairs is indicated, and then the results of the authorization check are shown.

```
Apr 22 23:15:04.019: CRYPTO_PKI_AAA: checking AAA authorization (ipsecca_script_aaalist,
PKIAAA-L, <all>)
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-trustpoint" = "CA1")
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-serial" = "15DE")
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: authorization passed
Apr 22 23:12:30.327: CRYPTO_PKI: Found a issuer match
```

### Failed Exchange

Router# **debug crypto pki transactions**

```
Apr 22 23:11:13.703: CRYPTO_PKI_AAA: checking AAA authorization =
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: reply attribute ("cert-trustpoint" = "CA1")
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: reply attribute ("cert-serial" = "233D")
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: parsed cert-lifetime-end as: 21:30:00
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: timezone specific extended
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: cert-lifetime-end is expired
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: cert-lifetime-end check failed.
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: authorization failed
```

In the above failed exchange, the certificate has expired.

## Configuring a Revocation Mechanism for PKI Certificate Status Checking

Perform this task to set up a CRL as the certificate revocation mechanism—CRLs or OCSP—that is used to check the status of certificates in a PKI.

### The revocation-check Command

Use the **revocation-check** command to specify at least one method (OCSP, CRL, or skip the revocation check) that is to be used to ensure that the certificate of a peer has not been revoked. For multiple methods, the order in which the methods are applied is determined by the order specified via this command.

If your router does not have the applicable CRL and is unable to obtain one or if the OCSP server returns an error, your router will reject the peer’s certificate—unless you include the **none** keyword in your configuration. If the **none** keyword is configured, a revocation check will not be performed and the certificate will always be accepted.

### Nonces and Peer Communications with OCSP Servers

When using OCSP, nonces, unique identifiers for OCSP requests, are sent by default during peer communications with your OCSP server. The use of nonces offers a more secure and reliable communication channel between the peer and OCSP server.

If your OCSP server does not support nonces, you may disable the sending of nonces. For more information, check your OCSP server documentation.

## Prerequisites

- Before issuing any client certificates, the appropriate settings on the server (such as setting the CDP) should be configured.
- When configuring an OCSP server to return the revocation status for a CA server, the OCSP server must be configured with an OCSP response signing certificate that is issued by that CA server. Ensure that the signing certificate is in the correct format, or the router will not accept the OCSP response. See your OCSP manual for additional information.

## Restrictions

- OCSP transports messages over HTTP, so there may be a time delay when you access the OCSP server.
- If the OCSP server depends on normal CRL processing to check revocation status, the same time delay that affects CRLs will also apply to OCSP.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint *name***
4. **ocsp url *url***
5. **revocation-check *method1* [*method2* [*method3*]]**
6. **ocsp disable-nonce**
7. **exit**
8. **exit**
9. **show crypto pki certificates**
10. **show crypto pki trustpoints [*status* | *label* [*status*]]**

## DETAILED STEPS

|        | Command or Action                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                             | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                    |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                     | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 3 | <b>crypto pki trustpoint name</b><br><br><b>Example:</b><br>Router(config)# crypto pki trustpoint hazel                            | Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.                                                                                                                                                                                                                                                                                                                                                                               |
| Step 4 | <b>ocsp url url</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# ocsp url<br>http://ocsp-server                                | (Optional) Specifies the URL of an OCSP server so that the trustpoint can check the certificate status. This URL will override the URL of the OCSP server (if one exists) in the Authority Info Access (AIA) extension of the certificate.                                                                                                                                                                                                                          |
| Step 5 | <b>revocation-check method1 [method2 [method3]]</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# revocation-check ocsp<br>none | Checks the revocation status of a certificate. <ul style="list-style-type: none"> <li><b>crl</b>—Certificate checking is performed by a CRL. This is the default option.</li> <li><b>none</b>—Certificate checking is ignored.</li> <li><b>ocsp</b>—Certificate checking is performed by an OCSP server.</li> </ul> If a second and third method are specified, each method will be used only if the previous method returns an error, such as a server being down. |
| Step 6 | <b>ocsp disable-nonce</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# ocsp disable-nonce                                      | (Optional) Specifies that a nonce, or an OCSP request unique identifier, will not be sent during peer communications with the OCSP server.                                                                                                                                                                                                                                                                                                                          |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# exit                                                                  | Returns to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 8 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                         | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|         | Command or Action                                                                                                          | Purpose                                                         |
|---------|----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| Step 9  | <b>show crypto pki certificates</b><br><br><b>Example:</b><br>Router# show crypto pki certificates                         | (Optional) Displays information about your certificates.        |
| Step 10 | <b>show crypto pki trustpoints [status   label [status]]</b><br><br><b>Example:</b><br>Router# show crypto pki trustpoints | Displays information about the trustpoint configured in router. |

## Configuring Certificate Authorization and Revocation Settings

Perform this task to specify a certificate-based ACL, to ignore revocation checks or expired certificates, to manually override the default CDP location, to manually override the OCSP server setting, to configure CRL caching, or to set session acceptance or rejection based on a certificate serial number, as appropriate.

### Configuring Certificate-Based ACLs to Ignore Revocation Checks

To configure your router to use certificate-based ACLs to ignore revocation checks and expired certificates, perform the following steps:

- Identify an existing trustpoint or create a new trustpoint to be used when verifying the certificate of the peer. Authenticate the trustpoint if it has not already been authenticated. The router may enroll with this trustpoint if you want. Do not set optional CRLs for the trustpoint if you plan to use the **match certificate** command and **skip revocation-check** keyword.
- Determine the unique characteristics of the certificates that should not have their CRL checked and of the expired certificates that should be allowed.
- Define a certificate map to match the characteristics identified in the prior step.
- You can add the **match certificate** command and **skip revocation-check** keyword and the **match certificate command** and **allow expired-certificate** keyword to the trustpoint that was created or identified in the first step.

### Manually Overriding CDPs in a Certificate

Users can override the CDPs in a certificate with a manually configured CDP. Manually overriding the CDPs in a certificate can be advantageous when a particular server is unavailable for an extended period of time. The certificate's CDPs can be replaced with a URL or directory specification without reissuing all of the certificates that contain the original CDP.

### Manually Overriding the OCSP Server Setting in a Certificate

Administrators can override the OCSP server setting specified in the Authority Information Access (AIA) field of the client certificate or set by the issuing the **ocsp url** command. One or more OCSP servers may be manually specified, either per client certificate or per group of client certificates by the

**match certificate override ocs**p command. The **match certificate override ocs**p command overrides the client certificate AIA field or the **ocsp url** command setting if a client certificate is successfully matched to a certificate map during the revocation check.

**Note**

Only one OCSF server can be specified per client certificate.

## Configuring CRL Cache Control

By default, a new CRL will be downloaded after the currently cached CRL expires. Administrators can either configure the maximum amount of time in minutes a CRL remains in the cache by issuing the **crl cache delete-after** command or disable CRL caching by issuing the **crl cache none** command. Only the **crl-cache delete-after** command or the **crl-cache none** command may be specified. If both commands are entered for a trustpoint, the last command executed will take effect and a message will be displayed.

Neither the **crl-cache none** command nor the **crl-cache delete-after** command affects the currently cached CRL. If you configure the **crl-cache none** command, all CRLs downloaded after this command is issued will not be cached. If you configure the **crl-cache delete-after** command, the configured lifetime will only affect CRLs downloaded after this command is issued.

This functionality is useful is when a CA issues CRLs with no expiration date or with expiration dates days or weeks ahead.

## Configuring Certificate Serial Number Session Control

A certificate serial number can be specified to allow a certificate validation request to be accepted or rejected by the trustpoint for a session. A session may be rejected, depending on certificate serial number session control, even if a certificate is still valid. Certificate serial number session control may be configured by using either a certificate map with the **serial-number** field or an AAA attribute, with the **cert-serial-not** command.

Using certificate maps for session control allows an administrator to specify a single certificate serial number. Using the AAA attribute allows an administrator to specify one or more certificate serial numbers for session control.

## Prerequisites

- The trustpoint should be defined and authenticated before attaching certificate maps to the trustpoint.
- The certificate map must be configured before the CDP override feature can be enabled or the **serial-number** command is issued.
- The PKI and AAA server integration must be successfully completed to use AAA attributes as described in [“PKI and AAA Server Integration for Certificate Status.”](#)

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki certificate map** *label sequence-number*
4. *field-name match-criteria match-value*

5. **exit**
6. **crypto pki trustpoint** *name*
7. **crl-cache none**
8. **crl-cache delete-after** *time*
9. **match certificate** *certificate-map-label* [**allow expired-certificate** | **skip revocation-check** | **skip authorization-check**]
10. **match certificate** *certificate-map-label* **override cdp** {**url** | **directory**} *string*
11. **match certificate** *certificate-map-label* **override ocsp** [**trustpoint** *trustpoint-label*] *sequence-number* **url** *ocsp-url*
12. **exit**
13. **aaa new-model**
14. **aaa attribute list** *list-name*
15. **attribute type** {*name*} {*label*}
16. **exit**
17. **exit**
18. **show crypto pki certificates**



## DETAILED STEPS

|        | Command or Action                                                                                                                                      | Purpose                                                                                                                 |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                         | Enters global configuration mode.                                                                                       |
| Step 3 | <b>crypto pki certificate map</b> <i>label</i> <i>sequence-number</i><br><br><b>Example:</b><br>Router(config)# crypto pki certificate map<br>Group 10 | Defines values in a certificate that should be matched or not matched and enters ca-certificate-map configuration mode. |

|        | Command or Action                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <p><i>field-name match-criteria match-value</i></p> <p><b>Example:</b><br/>Router(ca-certificate-map)# subject-name co MyCompany</p> | <p>Specifies one or more certificate fields together with their matching criteria and the value to match.</p> <p>The <i>field-name</i> is one of the following case-insensitive name strings or a date:</p> <ul style="list-style-type: none"> <li>• <b>alt-subject-name</b></li> <li>• <b>expires-on</b></li> <li>• <b>issuer-name</b></li> <li>• <b>name</b></li> <li>• <b>serial-number</b></li> <li>• <b>subject-name</b></li> <li>• <b>unstructured-subject-name</b></li> <li>• <b>valid-start</b></li> </ul> <p><b>Note</b> Date field format is dd mm yyyy hh:mm:ss or mmm dd yyyy hh:mm:ss.</p> <p>The <i>match-criteria</i> is one of the following logical operators:</p> <ul style="list-style-type: none"> <li>• <b>co</b> —contains (valid only for name fields and serial number field)</li> <li>• <b>eq</b> —equal (valid for name, serial number, and date fields)</li> <li>• <b>ge</b> —greater than or equal (valid only for date fields)</li> <li>• <b>lt</b> —less than (valid only for date fields)</li> <li>• <b>nc</b> —does not contain (valid only for name fields and serial number field)</li> <li>• <b>ne</b> —not equal (valid for name, serial number, and date fields)</li> </ul> <p>The <i>match-value</i> is the name or date to test with the logical operator assigned by match-criteria.</p> <p><b>Note</b> Use this command only when setting up a certificate-based ACL—not when setting up a certificate-based ACL to ignore revocation checks or expired certificates.</p> |
| Step 5 | <p><b>exit</b></p> <p><b>Example:</b><br/>Router(ca-certificate-map)# exit</p>                                                       | Returns to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 6 | <p><b>crypto pki trustpoint name</b></p> <p><b>Example:</b><br/>Router(config)# crypto pki trustpoint Access2</p>                    | Declares the trustpoint, given name and enters ca-trustpoint configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

|         | Command or Action                                                                                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7  | <b>crl-cache none</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# <b>crl-cache none</b>                                                                                                                                         | (Optional) Disables CRL caching completely for all CRLs associated with the trustpoint.<br><br>The <b>crl-cache none</b> command does not affect any currently cached CRLs. All CRLs downloaded after this command is configured will not be cached.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 8  | <b>crl-cache delete-after time</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# <b>crl-cache delete-after 2</b>                                                                                                                  | (Optional) Specifies the maximum time CRLs will remain in the cache for all CRLs associated with the trustpoint. <ul style="list-style-type: none"> <li><i>time</i>—The amount of time in minutes before the CRL is deleted.</li> </ul> The <b>crl-cache delete-after</b> command does not affect any currently cached CRLs. The configured lifetime will only affect CRLs downloaded after this command is configured.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 9  | <b>match certificate certificate-map-label [allow expired-certificate   skip revocation-check   skip authorization-check]</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# <b>match certificate Group1 skip revocation-check</b> | (Optional) Associates the certificate-based ACL (that was defined via the <b>crypto pki certificate map</b> command) to a trustpoint. <ul style="list-style-type: none"> <li><i>certificate-map-label</i>—Must match the <i>label</i> argument specified via the <b>crypto pki certificate map</b> command.</li> <li><b>allow expired-certificate</b>—Ignores expired certificates.</li> <li><b>skip revocation-check</b>—Allows a trustpoint to enforce CRLs except for specific certificates.</li> <li><b>skip authorization-check</b>—Skips the AAA check of a certificate when PKI integration with an AAA server is configured.</li> </ul>                                                                                                                                                                                                                                                                 |
| Step 10 | <b>match certificate certificate-map-label override cdp {url   directory} string</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# <b>match certificate Group1 override cdp url http://server.cisco.com</b>                       | (Optional) Manually overrides the existing CDP entries for a certificate with a URL or directory specification. <ul style="list-style-type: none"> <li><i>certificate-map-label</i>—A user-specified label that must match the <i>label</i> argument specified in a previously defined <b>crypto pki certificate map</b> command.</li> <li><b>url</b>—Specifies that the certificate's CDPs will be overridden with an HTTP or LDAP URL.</li> <li><b>directory</b>—Specifies that the certificate's CDPs will be overridden with an LDAP directory specification.</li> <li><i>string</i>—The URL or directory specification.</li> </ul> <p><b>Note</b> Some applications may time out before all CDPs have been tried and will report an error message. The error message will not affect the router, and the Cisco IOS software will continue attempting to retrieve a CRL until all CDPs have been tried.</p> |

|         | Command or Action                                                                                                                                                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 11 | <p><b>match certificate</b> <i>certificate-map-label</i><br/> <b>override ocs</b> [<i>trustpoint</i> <i>trustpoint-label</i>]<br/> <i>sequence-number</i> <b>url</b> <i>ocsp-url</i></p> <p><b>Example:</b><br/> Router(ca-trustpoint)# match certificate<br/> mycertmapname override ocs trustpoint mytp 15<br/> url http://192.0.2.2</p> | <p>(Optional) Specifies an OCSP server, either per client certificate or per group of client certificates, and may be issued more than once to specify additional OCSP servers and client certificate settings including alternative PKI hierarchies.</p> <ul style="list-style-type: none"> <li>• <i>certificate-map-label</i>—The name of an existing certificate map.</li> <li>• <b>trustpoint</b>—The trustpoint to be used when validating the OCSP server certificate.</li> <li>• <i>sequence-number</i>—The order the <b>match certificate override ocs</b> command statements apply to the certificate being verified. Matches are performed from the lowest sequence number to the highest sequence number. If more than one command is issued with the same sequence number, it overwrites the previous OCSP server override setting.</li> <li>• <b>url</b>—The URL of the OCSP server.</li> </ul> <p>When the certificate matches a configured certificate map, the AIA field of the client certificate and any previously issued <b>ocsp url</b> command settings are overwritten with the specified OCSP server.</p> <p>If no map-based match occurs, one of the following two cases will continue to apply to the client certificate.</p> <ul style="list-style-type: none"> <li>• If OCSP is specified as the revocation method, the AIA field value will continue to apply to the client certificate.</li> <li>• If the <b>ocsp url</b> configuration exists, the <b>ocsp url</b> configuration settings will continue to apply to the client certificates.</li> </ul> |
| Step 12 | <p><b>exit</b></p> <p><b>Example:</b><br/> Router(ca-trustpoint)# exit</p>                                                                                                                                                                                                                                                                 | Returns to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 13 | <p><b>aaa new-model</b></p> <p><b>Example:</b><br/> Router(config)# aaa new-model</p>                                                                                                                                                                                                                                                      | (Optional) Enables the AAA access control model.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 14 | <p><b>aaa attribute list</b> <i>list-name</i></p> <p><b>Example:</b><br/> Router(config)# aaa attribute list crl</p>                                                                                                                                                                                                                       | (Optional) Defines an AAA attribute list locally on a router and enters config-attr-list configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

|         | Command or Action                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------|-----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 15 | <b>attribute type</b> {name}{value}<br><br><b>Example:</b><br>Router(config-attr-list)# attribute type cert-serial-not 6C4A | (Optional) Defines an AAA attribute type that is to be added to an AAA attribute list locally on a router.<br><br>To configure certificate serial number session control, an administrator may specify a specific certificate in the <i>value</i> field to be accepted or rejected based on its serial number where <i>name</i> is set to <b>cert-serial-not</b> . If the serial number of the certificate matches the serial number specified by the attribute type setting, the certificate will be rejected.<br><br>For a full list of available AAA attribute types, execute the <b>show aaa attributes</b> command. |
| Step 16 | <b>exit</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# exit<br><br><b>Example:</b><br>Router(config-attr-list)# exit  | Returns to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Step 17 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                  | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 18 | <b>show crypto pki certificates</b><br><br><b>Example:</b><br>Router# show crypto pki certificates                          | (Optional) Displays the components of the certificates installed on the router if the CA certificate has been authenticated.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## Examples

The following is a sample OCSP response when signing a certificate. The OCSP-related extensions are in bold.

```
Certificate:
 Data:
 Version: v3
 Serial Number:0x14
 Signature Algorithm:MD5withRSA - 1.2.840.113549.1.1.4
 Issuer:CN=CA server,OU=PKI,O=Cisco Systems
 Validity:
 Not Before:Thursday, August 8, 2002 4:38:05 PM PST
 Not After:Tuesday, August 7, 2003 4:38:05 PM PST
 Subject:CN=OCSP server,OU=PKI,O=Cisco Systems
 Subject Public Key Info:
 Algorithm:RSA - 1.2.840.113549.1.1.1
 Public Key:
 Exponent:65537
 Public Key Modulus:(1024 bits) :
 <snip>

 Extensions:
 Identifier:Subject Key Identifier - 2.5.29.14
 Critical:no
```

```

Key Identifier:
 <snip>
Identifier:Authority Key Identifier - 2.5.29.35
Critical:no
Key Identifier:
 <snip>

Identifier:OCSP NoCheck:- 1.3.6.1.5.5.7.48.1.5
Critical:no
Identifier:Extended Key Usage:- 2.5.29.37
Critical:no
Extended Key Usage:
 OCSPSigning
Identifier:CRL Distribution Points - 2.5.29.31
Critical:no
Number of Points:1
Point 0
 Distribution Point:
[URIName:ldap://CA-server/CN=CA server,OU=PKI,O=Cisco Systems]
Signature:
 Algorithm:MD5withRSA - 1.2.840.113549.1.1.4
Signature:
 <snip>

```

The following example shows an excerpt of the running configuration output when adding a **match certificate override ocs** command to the beginning of an existing sequence:

```

match certificate map3 override ocs 5 url http://192.0.2.3/
show running-configuration
.
.
.
 match certificate map3 override ocs 5 url http://192.0.2.3/
 match certificate map1 override ocs 10 url http://192.0.2.1/
 match certificate map2 override ocs 15 url http://192.0.2.2/

```

The following example shows an excerpt of the running configuration output when an existing **match certificate override ocs** command is replaced and a trustpoint is specified to use an alternative PKI hierarchy:

```

match certificate map4 override ocs trustpoint tp4 10 url http://192.0.2.4/newvalue
show running-configuration
.
.
.
 match certificate map3 override ocs trustpoint tp3 5 url http://192.0.2.3/
 match certificate map1 override ocs trustpoint tp1 10 url http://192.0.2.1/
 match certificate map4 override ocs trustpoint tp4 10 url
 http://192.0.2.4/newvalue
 match certificate map2 override ocs trustpoint tp2 15 url http://192.0.2.2/

```

## Troubleshooting Tips

If you ignored revocation check or expired certificates, you should carefully check your configuration. Verify that the certificate map properly matches either the certificate or certificates that should be allowed or the AAA checks that should be skipped. In a controlled environment, try modifying the certificate map and determine what is not working as expected.

## Configuring Certificate Chain Validation

Perform this task to configure the processing level for the certificate chain path of your peer certificates.

### Prerequisites

- The device must be enrolled in your PKI hierarchy.
- The appropriate key pair must be associated with the certificate.

### Restrictions

- A trustpoint associated with the root CA cannot be configured to be validated to the next level.

The **chain-validation** command is configured with the **continue** keyword for the trustpoint associated with the root CA, an error message will be displayed and the chain validation will revert to the default **chain-validation** command setting.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **chain-validation** [{**stop** | **continue**} [*parent-trustpoint*]]
5. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                    | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Step 3 | <b>crypto pki trustpoint name</b><br><br><b>Example:</b><br>Router(config)# crypto pki trustpoint ca-sub1                                                                         | Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 4 | <b>chain-validation</b> [{ <b>stop</b>   <b>continue</b> }<br>[ <i>parent-trustpoint</i> ]]<br><br><b>Example:</b><br>Router(ca-trustpoint)# chain-validation<br>continue ca-sub1 | Configures the level to which a certificate chain is processed on all certificates including subordinate CA certificates. <ul style="list-style-type: none"><li>Use the <b>stop</b> keyword to specify that the certificate is already trusted. This is the default setting.</li><li>Use the <b>continue</b> keyword to specify that the subordinate CA certificate associated with the trustpoint must be validated.</li><li>The <i>parent-trustpoint</i> argument specifies the name of the parent trustpoint the certificate must be validated against.</li></ul> |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# exit                                                                                                                 | Returns to global configuration mode                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## Configuration Examples for Setting Up Authorization and Revocation of Certificates

This section contains the following configuration examples:

- [Configuring and Verifying PKI AAA Authorization: Examples, page 27](#)
- [Configuring a Revocation Mechanism: Examples, page 31](#)
- [Configuring a Hub Router at a Central Site for Certificate Revocation Checks: Example, page 32](#)
- [Configuring Certificate Authorization and Revocation Settings: Examples, page 36](#)
- [Configuring Certificate Chain Validation: Examples, page 38](#)



## Configuring and Verifying PKI AAA Authorization: Examples

This section provides configuration examples of PKI AAA authorizations:

- [Router Configuration: Example, page 27](#)
- [Debug of a Successful PKI AAA Authorization: Example, page 29](#)
- [Debugs of a Failed PKI AAA Authorization: Example, page 30](#)

### Router Configuration: Example

The following **show running-config** command output shows the working configuration of a router that is set up to authorize VPN connections using the PKI Integration with AAA Server feature:

```
Router# show running-config

Building configuration...
!
version 12.3
!
hostname router7200router7200
!
aaa new-model
!
!
aaa authentication login default group tacacs+
aaa authentication login no_tacacs enable
aaa authentication ppp default group tacacs+
aaa authorization exec ACSLab group tacacs+
aaa authorization network ACSLab group tacacs+
aaa accounting exec ACSLab start-stop group tacacs+
aaa accounting network default start-stop group ACSLab
aaa session-id common
!
ip domain name company.com
!
crypto pki trustpoint EM-CERT-SERV
 enrollment url http://192.0.2.33:80
 serial-number
 crl optional
 rsa-keypair STOREVPN 1024
 auto-enroll
 authorization list ACSLab
!
crypto pki certificate chain EM-CERT-SERV
certificate 04
 30820214 3082017D A0030201 02020104 300D0609 2A864886 F70D0101 04050030
 17311530 13060355 0403130C 454D2D43 4552542D 53455256 301E170D 30343031
 31393232 30323535 5A170D30 35303131 38323230 3235355A 3030312E 300E0603
 55040513 07314437 45424434 301C0609 2A864886 F70D0109 02160F37 3230302D
 312E6772 696C2E63 6F6D3081 9F300D06 092A8648 86F70D01 01010500 03818D00
 30818902 818100BD F3B837AA D925F391 2B64DA14 9C2EA031 5A7203C4 92F8D6A8
 7D2357A6 BCC8596F A38A9B10 47435626 D59A8F2A 123195BB BE5A1E74 B1AA5AE0
 5CA162FF 8C3ACA4F B3EE9F27 8B031642 B618AE1B 40F2E3B4 F996BEFE 382C7283
 3792A369 236F8561 8748AA3F BC41F012 B859BD9C DB4F75EE 3CEE2829 704BD68F
 FD904043 0F555702 03010001 A3573055 30250603 551D1F04 1E301C30 1AA018A0
 16861468 7474703A 2F2F3633 2E323437 2E313037 2E393330 0B060355 1D0F0404
 030205A0 301F0603 551D2304 18301680 1420FC4B CF0B1C56 F5BD4C06 0AFD4E67
 341AE612 D1300D06 092A8648 86F70D01 01040500 03818100 79E97018 FB955108
 12F42A56 2A6384BC AC8E22FE F1D6187F DA5D6737 C0E241AC AAAEC75D 3C743F59
 08DEEFF2 0E813A73 D79E0FA9 D62DC20D 8E2798CD 2C1DC3EC 3B2505A1 3897330C
```

```

15A60D5A 8A13F06D 51043D37 E56E45DF A65F43D7 4E836093 9689784D C45FD61D
EC1F160C 1ABC8D03 49FB11B1 DA0BED6C 463E1090 F34C59E4
quit
certificate ca 01
30820207 30820170 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
17311530 13060355 0403130C 454D2D43 4552542D 53455256 301E170D 30333132
31363231 34373432 5A170D30 36313231 35323134 3734325A 30173115 30130603
55040313 0C454D2D 43455254 2D534552 5630819F 300D0609 2A864886 F70D0101
01050003 818D0030 81890281 8100C14D 833641CF D784F516 DA6B50C0 7B3CB3C9
589223AB 99A7DC14 04F74EF2 AAEEE8F5 E3BFAE97 F2F980F7 D889E6A1 2C726C69
54A29870 7E7363FF 3CD1F991 F5A37CFF 3FFDD3D0 9E486C44 A2E34595 C2D078BB
E9DE981E B733B868 AA8916C0 A8048607 D34B83C0 64BDC101 161FC103 13C06500
22D6EE75 7D6CF133 7F1B515F 32830203 010001A3 63306130 0F060355 1D130101
FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186 301D0603 551D0E04
16041420 FC4BCF0B 1C56F5BD 4C060AFD 4E67341A E612D130 1F060355 1D230418
30168014 20FC4BCF 0B1C56F5 BD4C060A FD4E6734 1AE612D1 300D0609 2A864886
F70D0101 04050003 81810085 D2E386F5 4107116B AD3AC990 CBE84063 5FB2A6B5
BD572026 528E92ED 02F3A0AE 1803F2AE AA4C0ED2 0F59F18D 7B50264F 30442C41
0AF19C4E 70BD3CB5 0ADD8DE8 8EF636BD 24410DF4 DB62DAFC 67DA6E58 3879AA3E
12AFB1C3 2E27CB27 EC74E1FC AEE2F5CF AA80B439 615AA8D5 6D6DEDC3 7F9C2C79
3963E363 F2989FB9 795BA8
quit
!
!
crypto isakmp policy 10
 encr 3des
 group 2
!
!
crypto ipsec transform-set ISC_TS_1 esp-3des esp-sha-hmac
!
crypto ipsec profile ISC_IPSEC_PROFILE_2
 set security-association lifetime kilobytes 530000000
 set security-association lifetime seconds 14400
 set transform-set ISC_TS_1
!
!
controller ISA 1/1
!
!
interface Tunnel0
 description MGRE Interface provisioned by ISC
 bandwidth 10000
 ip address 192.0.2.172 255.255.255.0
 no ip redirects
 ip mtu 1408
 ip nhrp map multicast dynamic
 ip nhrp network-id 101
 ip nhrp holdtime 500
 ip nhrp server-only
 no ip split-horizon eigrp 101
 tunnel source FastEthernet2/1
 tunnel mode gre multipoint
 tunnel key 101
 tunnel protection ipsec profile ISC_IPSEC_PROFILE_2
!
interface FastEthernet2/0
 ip address 192.0.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet2/1
 ip address 192.0.2.2 255.255.255.0
 duplex auto

```

```

speed auto
!
!
tacacs-server host 192.0.2.55 single-connection
tacacs-server directed-request
tacacs-server key company lab
!
ntp master 1
!
end

```

## Debug of a Successful PKI AAA Authorization: Example

The following **show debugging** command output shows a successful authorization using the PKI Integration with AAA Server feature:

Router# **show debugging**

General OS:

```

TACACS access control debugging is on
AAA Authentication debugging is on
AAA Authorization debugging is on

```

Cryptographic Subsystem:

Crypto PKI Trans debugging is on

Router#

```

May 28 19:36:11.117: CRYPTO_PKI: Trust-Point EM-CERT-SERV picked up
May 28 19:36:12.789: CRYPTO_PKI: Found a issuer match
May 28 19:36:12.805: CRYPTO_PKI: cert revocation status unknown.
May 28 19:36:12.805: CRYPTO_PKI: Certificate validated without revocation check
May 28 19:36:12.813: CRYPTO_PKI_AAA: checking AAA authorization (ACSLab, POD5.company.com,
<all>)
May 28 19:36:12.813: AAA/BIND(00000042): Bind i/f
May 28 19:36:12.813: AAA/AUTHOR (0x42): Pick method list 'ACSLab'
May 28 19:36:12.813: TPLUS: Queuing AAA Authorization request 66 for processing
May 28 19:36:12.813: TPLUS: processing authorization request id 66
May 28 19:36:12.813: TPLUS: Protocol set to NoneSkipping
May 28 19:36:12.813: TPLUS: Sending AV service=pki
May 28 19:36:12.813: TPLUS: Authorization request created for 66(POD5.company.com)
May 28 19:36:12.813: TPLUS: Using server 192.0.2.55
May 28 19:36:12.813: TPLUS(00000042)/0/NB_WAIT/203A4628: Started 5 sec timeout
May 28 19:36:12.813: TPLUS(00000042)/0/NB_WAIT: wrote entire 46 bytes request
May 28 19:36:12.813: TPLUS: Would block while reading pak header
May 28 19:36:12.817: TPLUS(00000042)/0/READ: read entire 12 header bytes (expect 27 bytes)
May 28 19:36:12.817: TPLUS(00000042)/0/READ: read entire 39 bytes response
May 28 19:36:12.817: TPLUS(00000042)/0/203A4628: Processing the reply packet
May 28 19:36:12.817: TPLUS: Processed AV cert-application=all
May 28 19:36:12.817: TPLUS: received authorization response for 66: PASS
May 28 19:36:12.817: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
May 28 19:36:12.817: CRYPTO_PKI_AAA: authorization passed

```

Router#

Router#

```

May 28 19:36:18.681: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 101: Neighbor 192.0.2.171 (Tunnel0) is
up: new adjacency

```

Router#

Router# **show crypto isakmp sa**

| dst        | src         | state   | conn-id | slot |
|------------|-------------|---------|---------|------|
| 192.0.2.22 | 192.0.2.102 | QM_IDLE | 84      | 0    |

## Debugs of a Failed PKI AAA Authorization: Example

The following **show debugging** command output shows that the router is not authorized to connect using VPN. The messages are typical of those that you might see in such a situation.

In this example, the peer username was configured as not authorized, by moving the username to a Cisco Secure ACS group called VPN\_Router\_Disabled in Cisco Secure ACS. The router, router7200.company.com, has been configured to check with a Cisco Secure ACS AAA server prior to establishing a VPN connection to any peer.

Router# **show debugging**

General OS:

TACACS access control debugging is on  
AAA Authentication debugging is on  
AAA Authorization debugging is on

Cryptographic Subsystem:

Crypto PKI Trans debugging is on

Router#

```
May 28 19:48:29.837: CRYPTO_PKI: Trust-Point EM-CERT-SERV picked up
May 28 19:48:31.509: CRYPTO_PKI: Found a issuer match
May 28 19:48:31.525: CRYPTO_PKI: cert revocation status unknown.
May 28 19:48:31.525: CRYPTO_PKI: Certificate validated without revocation check
May 28 19:48:31.533: CRYPTO_PKI_AAA: checking AAA authorization (ACSLab, POD5.company.com,
<all>)
May 28 19:48:31.533: AAA/BIND(00000044): Bind i/f
May 28 19:48:31.533: AAA/AUTHOR (0x44): Pick method list 'ACSLab'
May 28 19:48:31.533: TPLUS: Queuing AAA Authorization request 68 for processing
May 28 19:48:31.533: TPLUS: processing authorization request id 68
May 28 19:48:31.533: TPLUS: Protocol set to NoneSkipping
May 28 19:48:31.533: TPLUS: Sending AV service=pki
May 28 19:48:31.533: TPLUS: Authorization request created for 68(POD5.company.com)
May 28 19:48:31.533: TPLUS: Using server 192.0.2.55
May 28 19:48:31.533: TPLUS(00000044)/0/NB_WAIT/203A4C50: Started 5 sec timeout
May 28 19:48:31.533: TPLUS(00000044)/0/NB_WAIT: wrote entire 46 bytes request
May 28 19:48:31.533: TPLUS: Would block while reading pak header
May 28 19:48:31.537: TPLUS(00000044)/0/READ: read entire 12 header bytes (expect 6 bytes)
May 28 19:48:31.537: TPLUS(00000044)/0/READ: read entire 18 bytes response
May 28 19:48:31.537: TPLUS(00000044)/0/203A4C50: Processing the reply packet
May 28 19:48:31.537: TPLUS: received authorization response for 68: FAIL
May 28 19:48:31.537: CRYPTO_PKI_AAA: authorization declined by AAA, or AAA server not
found.
May 28 19:48:31.537: CRYPTO_PKI_AAA: No cert-application attribute found. Failing.
May 28 19:48:31.537: CRYPTO_PKI_AAA: authorization failed
May 28 19:48:31.537: CRYPTO_PKI: AAA authorization for list 'ACSLab', and user
'POD5.company.com' failed.
May 28 19:48:31.537: %CRYPTO-5-IKMP_INVALID_CERT: Certificate received from 192.0.2.162 is
bad: certificate invalid
May 28 19:48:39.821: CRYPTO_PKI: Trust-Point EM-CERT-SERV picked up
May 28 19:48:41.481: CRYPTO_PKI: Found a issuer match
May 28 19:48:41.501: CRYPTO_PKI: cert revocation status unknown.
May 28 19:48:41.501: CRYPTO_PKI: Certificate validated without revocation check
May 28 19:48:41.505: CRYPTO_PKI_AAA: checking AAA authorization (ACSLab, POD5.company.com,
<all>)
May 28 19:48:41.505: AAA/BIND(00000045): Bind i/f
May 28 19:48:41.505: AAA/AUTHOR (0x45): Pick method list 'ACSLab'
May 28 19:48:41.505: TPLUS: Queuing AAA Authorization request 69 for processing
May 28 19:48:41.505: TPLUS: processing authorization request id 69
May 28 19:48:41.505: TPLUS: Protocol set to NoneSkipping
May 28 19:48:41.505: TPLUS: Sending AV service=pki
May 28 19:48:41.505: TPLUS: Authorization request created for 69(POD5.company.com)
May 28 19:48:41.505: TPLUS: Using server 198.168.244.55
```

```

May 28 19:48:41.509: TPLUS(00000045)/0/IDLE/63B22834: got immediate connect on new 0
May 28 19:48:41.509: TPLUS(00000045)/0/WRITE/63B22834: Started 5 sec timeout
May 28 19:48:41.509: TPLUS(00000045)/0/WRITE: wrote entire 46 bytes request
May 28 19:48:41.509: TPLUS(00000045)/0/READ: read entire 12 header bytes (expect 6 bytes)
May 28 19:48:41.509: TPLUS(00000045)/0/READ: read entire 18 bytes response
May 28 19:48:41.509: TPLUS(00000045)/0/63B22834: Processing the reply packet
May 28 19:48:41.509: TPLUS: received authorization response for 69: FAIL
May 28 19:48:41.509: CRYPTO_PKI_AAA: authorization declined by AAA, or AAA server not
found.
May 28 19:48:41.509: CRYPTO_PKI_AAA: No cert-application attribute found. Failing.
May 28 19:48:41.509: CRYPTO_PKI_AAA: authorization failed
May 28 19:48:41.509: CRYPTO_PKI: AAA authorization for list 'ACSLab', and user
'POD5.company.com' failed.
May 28 19:48:41.509: %CRYPTO-5-IKMP_INVALID_CERT: Certificate received from 192.0.2.162 is
bad: certificate invalid
Router#

Router# show crypto iskmp sa

```

| dst       | src         | state       | conn-id | slot |
|-----------|-------------|-------------|---------|------|
| 192.0.2.2 | 192.0.2.102 | MM_KEY_EXCH | 95      | 0    |

## Configuring a Revocation Mechanism: Examples

This section contains the following configuration examples that can be used when specifying a revocation mechanism for your PKI:

- [Configuring an OCSP Server: Example, page 31](#)
- [Specifying a CRL and Then an OCSP Server: Example, page 31](#)
- [Specifying an OCSP Server: Example, page 31](#)
- [Disabling Nonces in Communications with the OCSP Server: Example, page 32](#)

### Configuring an OCSP Server: Example

The following example shows how to configure the router to use the OCSP server that is specified in the AIA extension of the certificate:

```

Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check ocsp

```

### Specifying a CRL and Then an OCSP Server: Example

The following example shows how to configure the router to download the CRL from the CDP. If the CRL is unavailable, the OCSP server that is specified in the AIA extension of the certificate will be used. If both options fail, certificate verification will also fail.

```

Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check crl ocsp

```

### Specifying an OCSP Server: Example

The following example shows how to configure your router to use the OCSP server at the HTTP URL “http://myocspserver:81.” If the server is down, the revocation check will be ignored.

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# ocsf url http://myocspserver:81
Router(ca-trustpoint)# revocation-check ocsf none
```

## Disabling Nonces in Communications with the OCSP Server: Example

The following example shows communications when a nonce, or a unique identifier for the OCSP request, is disabled for communications with the OCSP server:

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# ocsf url http://myocspserver:81
Router(ca-trustpoint)# revocation-check ocsf none
Router(ca-trustpoint)# ocsf disable-nonce
```

## Configuring a Hub Router at a Central Site for Certificate Revocation Checks: Example

The following example shows a hub router at a central site that is providing connectivity for several branch offices to the central site.

The branch offices are also able to communicate directly with each other using additional IPSec tunnels between the branch offices.

The CA publishes CRLs on an HTTP server at the central site. The central site checks CRLs for each peer when setting up an IPSec tunnel with that peer.

The example does not show the IPSec configuration—only the PKI-related configuration is shown.

### Home Office Hub Configuration

```
crypto pki trustpoint VPN-GW
enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
serial-number none
fqdn none
ip-address none
subject-name o=Home Office Inc,cn=Central VPN Gateway
revocation-check crl
```

### Central Site Hub Router

```
Router# show crypto ca certificate
```

```
Certificate
 Status: Available
 Certificate Serial Number: 2F62BE1400000000CA0
 Certificate Usage: General Purpose
 Issuer:
 cn=Central Certificate Authority
 o=Home Office Inc
 Subject:
 Name: Central VPN Gateway
 cn=Central VPN Gateway
 o=Home Office Inc
 CRL Distribution Points:
 http://ca.home-office.com/CertEnroll/home-office.crl
 Validity Date:
 start date: 00:43:26 GMT Sep 26 2003
 end date: 00:53:26 GMT Sep 26 2004
 renew date: 00:00:00 GMT Jan 1 1970
 Associated Trustpoints: VPN-GW
```

```

CA Certificate
 Status: Available
 Certificate Serial Number: 1244325DE0369880465F977A18F61CA8
 Certificate Usage: Signature
 Issuer:
 cn=Central Certificate Authority
 o=Home Office Inc
 Subject:
 cn=Central Certificate Authority
 o=Home Office Inc
 CRL Distribution Points:
 http://ca.home-office.com/CertEnroll/home-office.crl
 Validity Date:
 start date: 22:19:29 GMT Oct 31 2002
 end date: 22:27:27 GMT Oct 31 2017
 Associated Trustpoints: VPN-GW

```

### Trustpoint on the Branch Office Router

```

crypto pki trustpoint home-office
 enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
 serial-number none
 fqdn none

ip-address none
subject-name o=Home Office Inc,cn=Branch 1
revocation-check crl

```

A certificate map is entered on the branch office router.

#### Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

```

branch1(config)# crypto pki certificate map central-site 10
branch1(ca-certificate-map)#

```

The output from the **show certificate** command on the central site hub router shows that the certificate was issued by the following:

cn=Central Certificate Authority

o=Home Office Inc

These two lines are combined into one line using a comma (,) to separate them, and the original lines are added as the first criteria for a match.

```

Router (ca-certificate-map)# issuer-name co cn=Central Certificate Authority, ou=Home
Office Inc

```

!The above line wrapped but should be shown on one line with the line above it.

The same combination is done for the subject name from the certificate on the central site router (note that the line that begins with “Name:” is not part of the subject name and must be ignored when creating the certificate map criteria). This is the subject name to be used in the certificate map.

cn=Central VPN Gateway

o=Home Office Inc

```

Router (ca-certificate-map)# subject-name eq cn=central vpn gateway, o=home office inc

```

Now the certificate map is added to the trustpoint that was configured earlier.

```

Router (ca-certificate-map)# crypto pki trustpoint home-office
Router (ca-trustpoint)# match certificate central-site skip revocation-check
Router (ca-trustpoint)# exit
Router (config)# exit

```

The configuration is checked (most of configuration is not shown).

```
Router# write term
!Many lines left out
.
.
.
crypto pki trustpoint home-office
 enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
 serial-number none
 fqdn none
 ip-address none
 subject-name o=Home Office Inc,cn=Branch 1
 revocation-check crl
 match certificate central-site skip revocation-check
!
!
crypto pki certificate map central-site 10
 issuer-name co cn = Central Certificate Authority, ou = Home Office Inc
 subject-name eq cn = central vpn gateway, o = home office inc
!many lines left out
```

Note that the issuer-name and subject-name lines have been reformatted to make them consistent for later matching with the certificate of the peer.

If the branch office is checking the AAA, the trustpoint will have lines similar to the following:

```
crypto pki trustpoint home-office
 auth list allow_list
 auth user subj commonname
```

After the certificate map has been defined as was done above, the following command is added to the trustpoint to skip AAA checking for the central site hub.

```
match certificate central-site skip authorization-check
```

In both cases, the branch site router has to establish an IPSec tunnel to the central site to check CRLs or to contact the AAA server. However, without the **match certificate** command and **central-site skip authorization-check (argument and keyword)**, the branch office cannot establish the tunnel until it has checked the CRL or the AAA server. (The tunnel will not be established unless the **match certificate** command and **central-site skip authorization-check** argument and keyword are used.)

The **match certificate** command and **allow expired-certificate** keyword would be used at the central site if the router at a branch site had an expired certificate and it had to establish a tunnel to the central site to renew its certificate.

#### Trustpoint on the Central Site Router

```
crypto pki trustpoint VPN-GW
 enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
 serial-number none
 fqdn none
 ip-address none
 subject-name o=Home Office Inc,cn=Central VPN Gateway
 revocation-check crl
```

#### Trustpoint on the Branch 1 Site Router

```
Router# show crypto ca certificate
```

```
Certificate
 Status: Available
 Certificate Serial Number: 2F62BE1400000000CA0
```



```

Certificate Usage: General Purpose
Issuer:
 cn=Central Certificate Authority
 o=Home Office Inc
Subject:
 Name: Branch 1 Site
 cn=Branch 1 Site
 o=Home Office Inc
CRL Distribution Points:
 http://ca.home-office.com/CertEnroll/home-office.crl
Validity Date:
 start date: 00:43:26 GMT Sep 26 2003
 end date: 00:53:26 GMT Oct 3 2003
 renew date: 00:00:00 GMT Jan 1 1970
Associated Trustpoints: home-office
CA Certificate
Status: Available
Certificate Serial Number: 1244325DE0369880465F977A18F61CA8
Certificate Usage: Signature
Issuer:
 cn=Central Certificate Authority
 o=Home Office Inc
Subject:
 cn=Central Certificate Authority
 o=Home Office Inc
CRL Distribution Points:
 http://ca.home-office.com/CertEnroll/home-office.crl
Validity Date:
 start date: 22:19:29 GMT Oct 31 2002
 end date: 22:27:27 GMT Oct 31 2017
Associated Trustpoints: home-office

```

A certificate map is entered on the central site router.

```

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router (config)# crypto pki certificate map branch1 10
Router (ca-certificate-map)# issuer-name co cn=Central Certificate Authority, ou=Home Office Inc
!The above line wrapped but should be part of the line above it.
Router (ca-certificate-map)# subject-name eq cn=Branch 1 Site,o=home office inc

```

The certificate map is added to the trustpoint.

```

Router (ca-certificate-map)# crypto pki trustpoint VPN-GW
Router (ca-trustpoint)# match certificate branch1 allow expired-certificate
Router (ca-trustpoint)# exit
Router (config) #exit

```

The configuration should be checked (most of the configuration is not shown).

```

Router# write term

!many lines left out

crypto pki trustpoint VPN-GW
 enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
 serial-number none
 fqdn none
 ip-address none
 subject-name o=Home Office Inc,cn=Central VPN Gateway
 revocation-check crl
 match certificate branch1 allow expired-certificate
!
!

```

```
crypto pki certificate map central-site 10
 issuer-name co cn = Central Certificate Authority, ou = Home Office Inc
 subject-name eq cn = central vpn gateway, o = home office inc
! many lines left out
```

The **match certificate** command and **branch1 allow expired-certificate** (argument and keyword) and the certificate map should be removed as soon as the branch router has a new certificate.

## Configuring Certificate Authorization and Revocation Settings: Examples

This section contains the following configuration examples that can be used when specifying a CRL cache control setting or certificate serial number session control:

- [Configuring CRL Cache Control, page 36](#)
- [Configuring Certificate Serial Number Session Control, page 37](#)

### Configuring CRL Cache Control

The following example shows how to disable CRL caching for all CRLs associated with the CA1 trustpoint:

```
crypto pki trustpoint CA1
 enrollment url http://CA1:80
 ip-address FastEthernet0/0
 crl query ldap://ldap_CA1
 revocation-check crl
 crl-cache none
```

The current CRL is still cached immediately after executing the example configuration shown above:

```
Router# show crypto pki crls
CRL Issuer Name:
 cn=name Cert Manager,ou=pki,o=company.com,c=US
 LastUpdate: 18:57:42 GMT Nov 26 2005
 NextUpdate: 22:57:42 GMT Nov 26 2005
 Retrieved from CRL Distribution Point:
 ldap://ldap.company.com/CN=name Cert Manager,O=company.com
```

When the current CRL expires, a new CRL is then downloaded to the router at the next update. The **crl-cache none** command takes effect and all CRLs for the trustpoint are no longer cached; caching is disabled. You can verify that no CRL is cached by executing the **show crypto pki crls** command. No output will be shown because there are no CRLs cached.

The following example shows how to configure the maximum lifetime of 2 minutes for all CRLs associated with the CA1 trustpoint:

```
crypto pki trustpoint CA1
 enrollment url http://CA1:80
 ip-address FastEthernet0/0
 crl query ldap://ldap_CA1
 revocation-check crl
 crl-cache delete-after 2
```

The current CRL is still cached immediately after executing the example configuration above for setting the maximum lifetime of a CRL:

```
Router# show crypto pki crls
CRL Issuer Name:
 cn=name Cert Manager,ou=pki,o=company.com,c=US
```

```
LastUpdate: 18:57:42 GMT Nov 26 2005
NextUpdate: 22:57:42 GMT Nov 26 2005
Retrieved from CRL Distribution Point:
 ldap://ldap.company.com/CN=name Cert Manager,O=company.com
```

When the current CRL expires, a new CRL is downloaded to the router at the next update and the **crl-cache delete-after** command takes effect. This newly cached CRL and all subsequent CRLs will be deleted after a maximum lifetime of 2 minutes.

You can verify that the CRL will be cached for 2 minutes by executing the **show crypto pki crls** command. Note that the NextUpdate time is 2 minutes after the LastUpdate time.

```
Router# show crypto pki crls

CRL Issuer Name:
 cn=name Cert Manager,ou=pki,o=company.com,c=US
 LastUpdate: 22:57:42 GMT Nov 26 2005

 NextUpdate: 22:59:42 GMT Nov 26 2005
 Retrieved from CRL Distribution Point:
 ldap://ldap.company.com/CN=name Cert Manager,O=company.com
```

## Configuring Certificate Serial Number Session Control

The following example shows the configuration of certificate serial number session control using a certificate map for the CA1 trustpoint:

```
crypto pki trustpoint CA1
 enrollment url http://CA1
 chain-validation stop
 crl query ldap://ldap_server
 revocation-check crl
 match certificate crl
!
crypto pki certificate map crl 10
 serial-number co 279d
```



### Note

If the *match-criteria* value is set to **eq** (equal) instead of **co** (contains), the serial number must match the certificate map serial number *exactly*, including any spaces.

The following example shows the configuration of certificate serial number session control using AAA attributes. In this case, all valid certificates will be accepted if the certificate does not have the serial number “4ACA.”

```
crypto pki trustpoint CA1
 enrollment url http://CA1
 ip-address FastEthernet0/0
 crl query ldap://ldap_CA1
 revocation-check crl
 aaa new-model
!
aaa attribute list crl
attribute-type aaa-cert-serial-not 4ACA
```

The server log shows that the certificate with the serial number “4ACA” was rejected. The certificate rejection is shown in bold.

```
.
.
.
```

```

Dec 3 04:24:39.051: CRYPTO_PKI: Trust-Point CA1 picked up
Dec 3 04:24:39.051: CRYPTO_PKI: locked trustpoint CA1, refcount is 1
Dec 3 04:24:39.051: CRYPTO_PKI: unlocked trustpoint CA1, refcount is 0
Dec 3 04:24:39.051: CRYPTO_PKI: locked trustpoint CA1, refcount is 1
Dec 3 04:24:39.135: CRYPTO_PKI: validation path has 1 certs
Dec 3 04:24:39.135: CRYPTO_PKI: Found a issuer match
Dec 3 04:24:39.135: CRYPTO_PKI: Using CA1 to validate certificate
Dec 3 04:24:39.135: CRYPTO_PKI: Certificate validated without revocation check
Dec 3 04:24:39.135: CRYPTO_PKI: Selected AAA username: 'PKIAAA'
Dec 3 04:24:39.135: CRYPTO_PKI: Anticipate checking AAA list:'CRL'
Dec 3 04:24:39.135: CRYPTO_PKI_AAA: checking AAA authorization (CRL, PKIAAA-L1, <all>)
Dec 3 04:24:39.135: CRYPTO_PKI_AAA: pre-authorization chain validation status (0x4)
Dec 3 04:24:39.135: AAA/BIND(00000021): Bind i/f
Dec 3 04:24:39.135: AAA/AUTHOR (0x21): Pick method list 'CRL'
.
.
.

Dec 3 04:24:39.175: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: reply attribute ("cert-trustpoint" = "CA1")
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: reply attribute ("cert-serial-not" = "4ACA")
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: cert-serial doesn't match ("4ACA" != "4ACA")
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: post-authorization chain validation status (0x7)
Dec 3 04:24:39.175: CRYPTO_PKI: AAA authorization for list 'CRL', and user 'PKIAAA'
failed.
Dec 3 04:24:39.175: CRYPTO_PKI: chain cert was anchored to trustpoint CA1, and chain
validation result was: CRYPTO_PKI_CERT_NOT_AUTHORIZED
Dec 3 04:24:39.175: %CRYPTO-5-IKMP_INVALID_CERT: Certificate received from 192.0.2.43 is
bad: certificate invalid
Dec 3 04:24:39.175: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main mode failed with peer
at 192.0.2.43
.
.
.

```

## Configuring Certificate Chain Validation: Examples

This section contains the following configuration examples that can be used to specify the level of certificate chain processing for your device certificates:

- [Configuring Certificate Chain Validation from Peer to Root CA, page 38](#)
- [Configuring Certificate Chain Validation from Peer to Subordinate CA, page 39](#)
- [Configuring Certificate Chain Validation Through a Gap, page 39](#)

### Configuring Certificate Chain Validation from Peer to Root CA

In the following configuration example, all of the certificates will be validated—the peer, SubCA11, SubCA1, and RootCA certificates.

```

crypto pki trustpoint RootCA
 enrollment terminal
 chain-validation stop
 revocation-check none
 rsakeypair RootCA

crypto pki trustpoint SubCA1
 enrollment terminal
 chain-validation continue RootCA
 revocation-check none

```

```
rsa-keypair SubCA1

crypto pki trustpoint SubCA11
 enrollment terminal
 chain-validation continue SubCA1
 revocation-check none
 rsa-keypair SubCA11
```

## Configuring Certificate Chain Validation from Peer to Subordinate CA

In the following configuration example, the following certificates will be validated—the peer and SubCA1 certificates.

```
crypto pki trustpoint RootCA
 enrollment terminal
 chain-validation stop
 revocation-check none
 rsa-keypair RootCA

crypto pki trustpoint SubCA1
 enrollment terminal
 chain-validation continue RootCA
 revocation-check none
 rsa-keypair SubCA1

crypto pki trustpoint SubCA11
 enrollment terminal
 chain-validation continue SubCA1
 revocation-check none
 rsa-keypair SubCA11
```

## Configuring Certificate Chain Validation Through a Gap

In the following configuration example, SubCA1 is not in the configured Cisco IOS hierarchy but is expected to have been supplied in the certificate chain presented by the peer.

If the peer supplies the SubCA1 certificate in the presented certificate chain, the following certificates will be validated—the peer, SubCA11, and SubCA1 certificates.

If the peer does not supply the SubCA1 certificate in the presented certificate chain, the chain validation will fail.

```
crypto pki trustpoint RootCA
 enrollment terminal
 chain-validation stop
 revocation-check none
 rsa-keypair RootCA

crypto pki trustpoint SubCA11
 enrollment terminal
 chain-validation continue RootCA
 revocation-check none
 rsa-keypair SubCA11
```

## Additional References

The following sections provide references related to PKI certificate authorization and revocation.

## Related Documents

| Related Topic                                                                                 | Document Title                                                                      |
|-----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| PKI commands: complete command syntax, command mode, defaults, usage guidelines, and examples | <i>Cisco IOS Security Command Reference, Release 12.4</i>                           |
| Overview of PKI, including RSA keys, certificate enrollment, and CAs                          | “Cisco IOS PKI Overview: Understanding and Planning a PKI” module                   |
| RSA key generation and deployment                                                             | “Deploying RSA Keys Within a PKI” module                                            |
| Certificate enrollment: supported methods, enrollment profiles, configuration tasks           | “Configuring Certificate Enrollment for a PKI” module                               |
| Cisco IOS certificate server overview information and configuration tasks                     | “Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment” module |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                       | Link                                                                            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Feature Information for Certificate Authorization and Revocation

Table 2 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for a specific command was introduced, see the command reference documentation. For information on a feature in this technology that is not documented here, see the Implementing and Managing PKI Features Roadmap.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



### Note

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 2**      **Feature Information for PKI Certificate Authorization and Revocation**

| Feature Name                                                  | Software Releases | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cache Control Enhancements for Certification Revocation Lists | 12.4(9)T          | <p>This feature provides users the ability to disable CRL caching or to specify the maximum lifetime for which a CRL will be cached in router memory. It also provides functionality to configure certificate serial number session control.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">What Is a CRL?</a></li> <li>• <a href="#">Configuring Certificate Authorization and Revocation Settings</a></li> <li>• <a href="#">Configuring Certificate Authorization and Revocation Settings: Examples</a></li> </ul> <p>The following commands were introduced or modified by this feature: <b>crl-cache delete-after</b>, <b>crl-cache none</b>, <b>crypto pki certificate map</b></p> |
| Certificate-Complete Chain Validation                         | 12.4(6)T          | <p>This feature provides users the ability to configure the level to which a certificate chain is processed on all certificates including subordinate CA certificates.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">PKI Certificate Chain Validation</a></li> <li>• <a href="#">Configuring Certificate Chain Validation</a></li> <li>• <a href="#">Configuring Certificate Chain Validation: Examples</a></li> </ul> <p>The following command was introduced by this feature: <b>chain-validation</b></p>                                                                                                                                                                             |
| OCSP - Server Certification from Alternate Hierarchy          | 12.4(6)T          | <p>This feature provides users with the flexibility to specify multiple OCSP servers, either per client certificate or per group of client certificates, and provides the capability for OCSP server validation based on external CA certificates or self-signed certificates.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">What Is OCSP?</a></li> <li>• <a href="#">Configuring Certificate Authorization and Revocation Settings</a></li> </ul> <p>The following command was introduced by this feature: <b>match certificate override ocsp</b></p>                                                                                                                                  |

**Table 2** *Feature Information for PKI Certificate Authorization and Revocation (continued)*

| Feature Name                                        | Software Releases      | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Optional OCSP Nonce                                 | 12.2(33)SR<br>12.4(4)T | <p>This feature provides users with the ability to configure the sending of a nonce, or unique identifier for an OCSP request, during OCSP communications.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">What Is OCSP?</a></li> <li>• <a href="#">Configuring a Revocation Mechanism for PKI Certificate Status Checking</a></li> <li>• <a href="#">Disabling Nonces in Communications with the OCSP Server: Example</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                 |
| Certificate Security Attribute-Based Access Control | 12.2(15)T              | <p>Under the IPsec protocol, CA interoperability permits Cisco IOS devices and a CA to communicate so that the Cisco IOS device can obtain and use digital certificates from the CA. Certificates contain several fields that are used to determine whether a device or user is authorized to perform a specified action. This feature adds fields to the certificate that allow specifying an ACL, creating a certificate-based ACL.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">When to Use Certificate-Based ACLs for Authorization or Revocation</a></li> <li>• <a href="#">Configuring Certificate Authorization and Revocation Settings</a></li> </ul> <p>The following commands were introduced or modified by this feature: <b>crypto pki certificate map</b>, <b>crypto pki trustpoint</b>, <b>match certificate</b></p> |
| Online Certificate Status Protocol (OCSP)           | 12.3(2)T               | <p>This feature allows users to enable OCSP instead of CRLs to check certificate status. Unlike CRLs, which provide only periodic certificate status, OCSP can provide timely information regarding the status of a certificate.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">CRLs or OCSP Server: Choosing a Certificate Revocation Mechanism</a></li> <li>• <a href="#">Configuring a Revocation Mechanism for PKI Certificate Status Checking</a></li> </ul> <p>The following commands were introduced by this feature: <b>ocsp url</b>, <b>revocation-check</b></p>                                                                                                                                                                                                                                                            |



**Table 2**      **Feature Information for PKI Certificate Authorization and Revocation (continued)**

| Feature Name                                                    | Software Releases | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------------|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PKI AAA Authorization Using the Entire Subject Name             | 12.3(11)T         | <p>This feature provides users with the ability to query the AAA server using the entire subject name from the certificate as a unique AAA username.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Attribute-Value Pairs for PKI and AAA Server Integration</a></li> <li>• <a href="#">Configuring PKI Integration with a AAA Server</a></li> </ul> <p>The following command was modified by this feature:<br/><b>authorization username</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| PKI Integration with AAA Server                                 | 12.3(1)           | <p>This feature provides additional scalability for authorization by generating a AAA username from the certificate presented by the peer. A AAA server is queried to determine whether the certificate is authorized for use by the internal component. The authorization is indicated by a component-specified label that must be present in the AV pair for the user.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">PKI and AAA Server Integration for Certificate Status</a></li> <li>• <a href="#">Configuring PKI Integration with a AAA Server</a></li> </ul> <p>The following commands were introduced by this feature:<br/><b>authorization list, authorization username</b></p>                                                                                                                                                                                                     |
| PKI: Query Multiple Servers During Certificate Revocation Check | 12.3(7)T          | <p>This feature introduces the ability for Cisco IOS software to make multiple attempts to retrieve the CRL, allowing operations to continue when a particular server is not available. In addition, the ability to override the CDPs in a certificate with a manually configured CDP has been introduced. Manually overriding the CDPs in a certificate can be advantageous when a particular server is unavailable for an extended period of time. The certificate's CDPs can be replaced with a URL or directory specification without reissuing all of the certificates that contain the original CDP.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Querying All CDPs During Revocation Check</a></li> <li>• <a href="#">Manually Overriding CDPs in a Certificate</a></li> </ul> <p>The following command was introduced by this feature:<br/><b>match certificate override cdp</b></p> |

**Table 2** *Feature Information for PKI Certificate Authorization and Revocation (continued)*

| Feature Name                                                               | Software Releases        | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------------------------------|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PKI: Query Multiple Servers During Certificate Revocation Check            | 12.3(7)T                 | <p>This feature introduces the ability for Cisco IOS software to make multiple attempts to retrieve the CRL, allowing operations to continue when a particular server is not available. In addition, the ability to override the CDPs in a certificate with a manually configured CDP has been introduced. Manually overriding the CDPs in a certificate can be advantageous when a particular server is unavailable for an extended period of time. The certificate's CDPs can be replaced with a URL or directory specification without reissuing all of the certificates that contain the original CDP.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li><a href="#">Querying All CDPs During Revocation Check</a></li> <li><a href="#">Manually Overriding CDPs in a Certificate</a></li> </ul> <p>The following command was introduced by this feature:<br/><b>match certificate override cdp</b></p> |
| Using Certificate ACLs to Ignore Revocation Check and Expired Certificates | 12.3(4)T                 | <p>This feature allows a certificate that meets specified criteria to be accepted regardless of the validity period of the certificate, or if the certificate meets the specified criteria, revocation checking does not have to be performed. Certificate ACLs are used to specify the criteria that the certificate must meet to be accepted or to avoid revocation checking. In addition, if AAA communication is protected by a certificate, this feature provides for the AAA checking of the certificate to be ignored.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li><a href="#">Ignore Revocation Checks Using a Certificate-Based ACL</a></li> <li><a href="#">Configuring Certificate-Based ACLs to Ignore Revocation Checks</a></li> </ul> <p>The following command was modified by this feature:<br/><b>match certificate</b></p>                                                           |
| Certificate - Security Attribute-Based Access Control                      | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| OCSP (Online Certificate Status Protocol)                                  | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Optional OCSP Nonce                                                        | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

**Table 2** *Feature Information for PKI Certificate Authorization and Revocation (continued)*

| Feature Name                                               | Software Releases        | Feature Configuration Information                             |
|------------------------------------------------------------|--------------------------|---------------------------------------------------------------|
| PKI AAA Authorization Using the Entire Subject Name        | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers. |
| PKI Integration with AAA Server                            | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers. |
| Query Mode Definition Per Trustpoint                       | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers. |
| Query Multiple Servers during Certificate Revocation Check | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers. |

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





# Configuring Certificate Enrollment for a PKI

---

**First Published: May 2, 2005**

**Last Updated: August 21, 2007**

Certificate enrollment, which is the process of obtaining a certificate from a certification authority (CA), occurs between the end host that requests the certificate and the CA. Each peer that participates in the public key infrastructure (PKI) must enroll with a CA. This module describes the different methods available for certificate enrollment and how to set up each method for a participating PKI peer.

## **Finding Feature Information in This Module**

*Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for PKI Certificate Enrollment](#)” section on page 34.*

## **Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images**

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for PKI Certificate Enrollment, page 2](#)
- [Information About Certificate Enrollment for a PKI, page 2](#)
- [How to Configure Certificate Enrollment for a PKI, page 6](#)
- [Configuration Examples for PKI Certificate Enrollment Requests, page 25](#)
- [Additional References, page 32](#)
- [Feature Information for PKI Certificate Enrollment, page 34](#)



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

# Prerequisites for PKI Certificate Enrollment

Before configuring peers for certificate enrollment, you should have the following items:

- A generated Rivest, Shamir, and Adelman (RSA) key pair to enroll and a PKI in which to enroll.
- Your CA should be authenticated.
- Familiarity with the module “Cisco IOS PKI Overview: Understanding and Planning a PKI.”

**Note**

As of Cisco IOS Release 12.3(7)T, all commands that begin with “**crypto ca**” have been changed to begin with “**crypto pki**.” Although the router will still accept **crypto ca** commands, all output will be read back as **crypto pki**.

## Information About Certificate Enrollment for a PKI

Before configuring peers to request a certificate and enroll in the PKI, you should understand the following concepts:

- [What Are CAs?, page 2](#)
- [Authentication of the CA, page 3](#)
- [Supported Certificate Enrollment Methods, page 3](#)
- [Registration Authorities \(RA\), page 4](#)
- [Automatic Certificate Enrollment, page 4](#)
- [Certificate Enrollment Profiles, page 5](#)

## What Are CAs?

A CA manages certificate requests and issues certificates to participating network devices. These services (managing certificate requests and issuing certificates) provide centralized key management for the participating devices to validate identities and to create digital certificates. Before any PKI operations can begin, the CA generates its own public key pair and creates a self-signed CA certificate; thereafter, the CA can sign certificate requests and begin peer enrollment for the PKI.

You can use the Cisco IOS certificate server or a CA provided by a third-party CA vendor.

## Hierarchical PKI: Multiple CAs

A PKI can be set up in a hierarchical framework to support multiple CAs. At the top of the hierarchy is a root CA, which holds a self-signed certificate. The trust within the entire hierarchy is derived from the RSA key pair of the root CA. The subordinate CAs within the hierarchy can be enrolled with either the root CA or with another subordinate CA. Multiple tiers of CAs are configured by either the root CA or with another subordinate CA. Within a hierarchical PKI, all enrolled peers, can validate the certificate of one another if the peers share a trusted root CA certificate or a common subordinate CA.

### When to Use Multiple CAs

Multiple CAs provide users with added flexibility and reliability. For example, subordinate CAs can be placed in branch offices while the root CA is at the office headquarters. Also, different granting policies can be implemented per CA, so you can set up one CA to automatically grant certificate requests while another CA within the hierarchy requires each certificate request to be manually granted.

Scenarios in which at least a two-tier CA is recommended are as follows:

- Large and very active networks in which a large number of certificates are revoked and reissued. A multiple tier CA helps to control the size of the certificate revocation lists (CRLs).
- When online enrollment protocols are used, the root CA can be kept offline except to issue subordinate CA certificates. This scenario provides added security for the root CA.

## Authentication of the CA

The certificate of the CA must be authenticated before the device will be issued its own certificate and before certificate enrollment can occur. Authentication of the CA typically occurs only when you initially configure PKI support at your router. To authenticate the CA, issue the **crypto pki authenticate** command, which authenticates the CA to your router by obtaining the self-signed certificate of the CA that contains the public key of the CA.

### Authentication via the fingerprint Command

After Cisco IOS Release 12.3(12), you can issue the **fingerprint** command to preenter a fingerprint that can be matched against the fingerprint of a CA certificate during authentication.

If a fingerprint is not preentered for a trustpoint, and if the authentication request is interactive, you must verify the fingerprint that is displayed during authentication of the CA certificate. If the authentication request is noninteractive, the certificate will be rejected without a preentered fingerprint.



#### Note

If the authentication request is made using the command-line interface (CLI), the request is an interactive request. If the authentication request is made using HTTP or another management tool, the request is a noninteractive request.

## Supported Certificate Enrollment Methods

Cisco IOS software supports the following methods to obtain a certificate from a CA:

- Simple Certificate Enrollment Protocol (SCEP)—A Cisco developed enrollment protocol that uses HTTP to communicate with the CA or registration authority (RA). SCEP is the most commonly used method for sending and receiving requests and certificates.



#### Note

To take advantage of automated certificate and key rollover functionality, you must be running a CA that supports rollover and SCEP must be used as your client enrollment method.

If you are running a Cisco IOS CA, you must be running Cisco IOS Release 12.4(2)T or a later release for rollover support.

- PKCS12—The router imports certificates in PKCS12 format from an external server.
- IOS File System (IFS)—The router uses any file system that is supported by Cisco IOS software (such as TFTP, FTP, flash, and NVRAM) to send a certificate request and to receive the issued certificate. Users may enable IFS certificate enrollment when their CA does not support SCEP.



**Note** Prior to Cisco IOS Release 12.3(4)T, only the TFTP file system is supported within IFS.

- Manual cut-and-paste—The router displays the certificate request on the console terminal, allowing the user to enter the issued certificate on the console terminal. A user may manually cut-and-paste certificate requests and certificates when there is no network connection between the router and CA.
- Enrollment profiles—The router sends HTTP-based enrollment requests directly to the CA server instead of to the RA-mode CS. Enrollment profiles can be used if a CA server does not support SCEP.
- Self-signed certificate enrollment for a trustpoint—The secure HTTP (HTTPS) server generates a self-signed certificate that is to be used during the secure socket layer (SSL) handshake, establishing a secure connection between the HTTPS server and the client. The self-signed certificate is then saved in the router's startup configuration (NVRAM). The saved, self-signed certificate can then be used for future SSL handshakes, eliminating the user intervention that was necessary to accept the certificate every time the router reloaded.



**Note**

To take advantage of autoenrollment and auto reenrollment, do not use either TFTP or manual cut-and-paste enrollment as your enrollment method. Both TFTP and manual cut-and-paste enrollment methods are manual enrollment processes, requiring user input.

## Registration Authorities (RA)

A Cisco IOS certificate server can be configured to run in RA mode. An RA offloads authentication and authorization responsibilities from a CA. When the RA receives a SCEP or manual enrollment request, the administrator can either reject or grant it on the basis of local policy. If the request is granted, it will be forwarded to the issuing CA, and the CA can be configured to automatically generate the certificate and return it to the RA. The client can later retrieve the granted certificate from the RA.

## Automatic Certificate Enrollment

Certificate autoenrollment allows the CA client to automatically request a certificate from its CA sever. This automatic router request eliminates the need for operator intervention when the enrollment request is sent to the CA server. Automatic enrollment is performed on startup for any trustpoint CA that is configured and that does not have a valid client certificate. When the certificate expires, a new certificate is automatically requested.



**Note**

When automatic enrollment is configured, clients automatically request client certificates. The CA server performs its own authorization checks; if these checks include a policy to automatically issue certificates, all clients will automatically receive certificates, which is not very secure. Thus, automatic certificate enrollment should be combined with additional authentication and authorization mechanisms (such as Secure Device Provisioning (SDP), leveraging existing certificates, and one-time passwords).



### Automated Client Certificate and Key Rollover

By default, the automatic certificate enrollment function requests a new client certificate and keys from the CS before the client's current certificate expires. Certificate and key rollover allows the certificate renewal rollover request to be made before the certificate expires by retaining the current key and certificate until the new, or rollover, certificate is available. After a specified amount of time, the rollover certificate and keys will become the active certificate and keys. The expired certificate and keys are immediately deleted upon rollover and removed from the certificate chain and CRL.

The setup for automatic rollover is twofold: CA clients must be automatically enrolled and the client's CAs must be automatically enrolled and have the **auto-rollover** command enabled. For more information on configuring your CA servers for automatic certificate rollover see the section "Automatic CA Certificate and Key Rollover" in the chapter "[Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment](#)."

An optional renewal percentage parameter can be used with the **auto-enroll** command to allow a new certificate to be requested when a specified percentage of the lifetime of the certificate has passed. For example, if the renewal percentage is configured as 90 and the certificate has a lifetime of one year, a new certificate is requested 36.5 days before the old certificate expires. In order for automatic rollover to occur, the renewal percentage must be less than 100.



#### Tip

If CA autoenrollment is not enabled, you may manually initiate rollover on an existing client with the **crypto pki enroll** command if the expiration time of the current client certificate is equal to or greater than the expiration time of the corresponding CA certificate.

The client will initiate the rollover process, which only occurs if the server is configured for automated rollover and has an available rollover server certificate.



#### Note

A key pair is also sent if configured by the **auto-enroll re-generate** command and keyword. It is recommended that a new key pair be issued for security reasons.

## Certificate Enrollment Profiles

Enrollment profiles allow users to specify certificate authentication, enrollment, and reenrollment parameters when prompted. The values for these parameters are referenced by two templates that make up the profile. One template contains parameters for the HTTP request that is sent to the CA server to obtain the certificate of the CA (also known as certificate authentication); the other template contains parameters for the HTTP request that is sent to the CA for certificate enrollment.

Configuring two templates enables users to specify different URLs or methods for certificate authentication and enrollment; for example, authentication (getting the certificate of the CA) can be performed via TFTP (using the **authentication url** command) while enrollment can be performed manually (using the **enrollment terminal** command).

Prior to Cisco IOS Release 12.3(11)T, certificate requests could be sent only in a PKCS10 format; however, an additional parameter has now been added to the profile, allowing users to specify the PKCS7 format for certificate renewal requests.



#### Note

A single enrollment profile can have up to three separate sections for each task—certificate authentication, enrollment, and reenrollment.

# How to Configure Certificate Enrollment for a PKI

This section contains the following enrollment option procedures. If you configure enrollment or autoenrollment (the first task), you cannot configure manual certificate enrollment. Also, if you configure TFTP or manual cut-and-paste certificate enrollment, you cannot configure autoenrollment, auto reenrollment, an enrollment profile, nor can you utilize the automated CA certificate rollover capability.

- [Configuring Certificate Enrollment or Autoenrollment, page 6](#)
- [Configuring Manual Certificate Enrollment, page 11](#)
- [Configuring a Persistent Self-Signed Certificate for Enrollment via SSL, page 17](#)
- [Configuring a Certificate Enrollment Profile for Enrollment or Reenrollment, page 21](#)

## Configuring Certificate Enrollment or Autoenrollment

Perform this task to configure certificate enrollment for clients participating in your PKI.

### Prerequisites for Autoenrollment

Before configuring automatic certificate enrollment requests, you should ensure that all necessary enrollment information is configured.

#### Prerequisites for Enabling Automated Client Certificate and Key Rollover

CA client support for certificate rollover is automatically enabled when using autoenrollment. For automatic CA certificate rollover to run successfully, the following prerequisites are applicable:

- Your network devices must support shadow PKI.
- Your clients must be running Cisco IOS Release 12.4(2)T or a later release.
- The client's CS must support automatic rollover. See the section "Automatic CA Certificate and Key Rollover" in the chapter "[Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment](#)" for more information on CA server automatic rollover configuration.

#### Prerequisites for Specifying Autoenrollment Initial Key Generation Location

To specify the location of the autoenrollment initial key generation, you must be running Cisco IOS Release 12.4(11)T or a later release.

### Restrictions for Autoenrollment

#### RSA Key Pair Restriction for Autoenrollment

Trustpoints configured to generate a new key pair using the **regenerate** command or the **regenerate** keyword of the **auto-enroll** command must not share key pairs with other trustpoints. To give each trustpoint its own key pair, use the **rsakeypair** command in ca-trustpoint configuration mode. Sharing key pairs among regenerating trustpoints is not supported and will cause loss of service on some of the trustpoints because of key and certificate mismatches.

#### Restrictions for Automated Client Certificate and Key Rollover

In order for clients to run automatic CA certificate rollover successfully, the following restrictions are applicable:

- SCEP must be used to support rollover. Any device that enrolls with the PKI using an alternative to SCEP as the certificate management protocol or mechanism (such as enrollment profiles, manual enrollment, or TFTP enrollment) will not be able to take advantage of the rollover functionality provided by SCEP.
- If the configuration cannot be saved to the startup configuration after a shadow certificate is generated, rollover will not occur.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment** [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url* [**pem**]
5. **subject-name** [*x.500-name*]
6. **ip address** {*ip address* | *interface* | **none**}
7. **serial-number** [**none**]
8. **auto-enroll** [*percent*] [**regenerate**]
9. **usage** *method1* [*method2* [*method3*]]
10. **password** *string*
11. **rsa****keypair** *key-label* [*key-size* [*encryption-key-size*]]
12. **fingerprint** *ca-fingerprint*
13. **on** *devicename*:
14. **exit**
15. **crypto pki authenticate** *name*
16. **exit**
17. **copy system:running-config nvram:startup-config**
18. **show crypto pki certificates**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                       | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                               | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 3 | <b>crypto pki trustpoint name</b><br><br><b>Example:</b><br>Router(config)# crypto pki trustpoint mytp                                                                       | Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 4 | <b>enrollment [mode] [retry period minutes] [retry count number] url url [pem]</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# enrollment url<br>http://cat.example.com | Specifies the URL of the CA on which your router should send certificate requests. <ul style="list-style-type: none"> <li><b>mode</b>—Specifies RA mode if your CA system provides an RA.</li> <li><b>retry period minutes</b>—Specifies the wait period between certificate request retries. The default is 1 minute between retries.</li> <li><b>retry count number</b>— Specifies the number of times a router will resend a certificate request when it does not receive a response from the previous request. (Specify from 1 to 100 retries.)</li> <li><b>url url</b>—URL of the file system where your router should send certificate requests. For enrollment method options, see the <b>enrollment</b> command in the <a href="#">Cisco IOS Security Command Reference</a>.</li> <li><b>pem</b>—Adds privacy-enhanced mail (PEM) boundaries to the certificate request.</li> </ul> <p><b>Note</b> An enrollment method other than TFTP or manual cut-and-paste must be configured to support autoenrollment.</p> |
| Step 5 | <b>subject-name [x.500-name]</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# subject-name cat                                                                           | (Optional) Specifies the requested subject name that will be used in the certificate request. <ul style="list-style-type: none"> <li><b>x.500-name</b>—If it is not specified, the fully qualified domain name (FQDN), which is the default subject name, will be used.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 6 | <b>ip address {ip address   interface   none}</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# ip address 192.168.1.66                                                   | (Optional) Includes the IP address of the specified interface in the certificate request. <p>Issue the <b>none</b> keyword if no IP address should be included.</p> <p><b>Note</b> If this command is enabled, you will not be prompted for an IP address during enrollment for this trustpoint.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

|         | Command or Action                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7  | <b>serial-number</b> [none]<br><br><b>Example:</b><br>Router(ca-trustpoint)# serial-number                                   | (Optional) Specifies the router serial number in the certificate request, unless the <b>none</b> keyword is issued.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 8  | <b>auto-enroll</b> [percent] [regenerate]<br><br><b>Example:</b><br>Router(ca-trustpoint)# auto-enroll regenerate            | <p>(Optional) Enables autoenrollment, allowing the client to automatically request a rollover certificate from the CA. If autoenrollment is not enabled, the client must be manually reenrolled in your PKI upon certificate expiration.</p> <ul style="list-style-type: none"> <li>By default, only the Domain Name System (DNS) name of the router is included in the certificate.</li> <li>Use the <i>percent</i> argument to specify that a new certificate will be requested after the percentage of the lifetime of the current certificate is reached.</li> <li>Use the <b>regenerate</b> keyword to generate a new key for the certificate even if a named key already exists.</li> </ul> <p><b>Note</b> If the key pair being rolled over is exportable, the new key pair will also be exportable. The following comment will appear in the trustpoint configuration to indicate whether the key pair is exportable: “! RSA key pair associated with trustpoint is exportable.”</p> <p><b>Note</b> It is recommended that a new key pair be generated for security reasons.</p> |
| Step 9  | <b>usage</b> method1 [method2 [method3]]<br><br><b>Example:</b><br>Router(ca-trustpoint)# usage ssl-client                   | <p>(Optional) Specifies the intended use for the certificate. Available options are <b>ike</b>, <b>ssl-client</b>, and <b>ssl-server</b>; the default is <b>ike</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 10 | <b>password</b> string<br><br><b>Example:</b><br>Router(ca-trustpoint)# password meow                                        | <p>(Optional) Specifies the revocation password for the certificate. If this command is enabled, you will not be prompted for a password during enrollment for this trustpoint.</p> <p><b>Note</b> When SCEP is used, this password can be used to authorize the certificate request—often via a one-time password or similar mechanism.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 11 | <b>rsakeypair</b> key-label [key-size [encryption-key-size]]<br><br><b>Example:</b><br>Router(ca-trustpoint)# rsakeypair cat | <p>(Optional) Specifies which key pair to associate with the certificate.</p> <ul style="list-style-type: none"> <li>A key pair with <i>key-label</i> will be generated during enrollment if it does not already exist or if the <b>auto-enroll regenerate</b> command was issued.</li> <li>Specify the <i>key-size</i> argument for generating the key, and specify the <i>encryption-key-size</i> argument to request separate encryption, signature keys, and certificates.</li> </ul> <p><b>Note</b> If this command is not enabled, the FQDN key pair is used.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

|                | Command or Action                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 12</b> | <pre>fingerprint ca-fingerprint</pre> <p><b>Example:</b><br/> Router(ca-trustpoint)# fingerprint 12EF53FA 355CD23E 12EF53FA 355CD23E</p>       | <p>(Optional) Specifies a fingerprint that can be matched against the fingerprint of a CA certificate during authentication.</p> <p><b>Note</b> If the fingerprint is not provided and authentication of the CA certificate is interactive, the fingerprint will be displayed for verification.</p>                                                                                                                                                 |
| <b>Step 13</b> | <pre>on devicename:</pre> <p><b>Example:</b><br/> Router(ca-trustpoint)# on usbtokens0:</p>                                                    | <p>(Optional) Specifies that RSA keys will be created on the specified device upon autoenrollment initial key generation.</p> <p>Devices that may be specified include NVRAM, local disks, and USB tokens. USB tokens may be used as cryptographic devices in addition to a storage device. Using a USB token as a cryptographic device allows RSA operations such as key generation, signing, and authentication to be performed on the token.</p> |
| <b>Step 14</b> | <pre>exit</pre> <p><b>Example:</b><br/> Router(ca-trustpoint)# exit</p>                                                                        | Exits ca-trustpoint configuration mode and returns to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 15</b> | <pre>crypto pki authenticate name</pre> <p><b>Example:</b><br/> Router(config)# crypto pki authenticate mytp</p>                               | <p>Retrieves the CA certificate and authenticates it.</p> <ul style="list-style-type: none"> <li>Check the certificate fingerprint if prompted.</li> </ul> <p><b>Note</b> This command is optional if the CA certificate is already loaded into the configuration.</p>                                                                                                                                                                              |
| <b>Step 16</b> | <pre>exit</pre> <p><b>Example:</b><br/> Router(config)# exit</p>                                                                               | Exits global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 17</b> | <pre>copy system:running-config nvram:startup-config</pre> <p><b>Example:</b><br/> Router# copy system:running-config nvram:startup-config</p> | <p>(Optional) Copies the running configuration to the NVRAM startup configuration.</p> <p><b>Note</b> Autoenrollment will not update NVRAM if the running configuration has been modified but not written to NVRAM.</p>                                                                                                                                                                                                                             |
| <b>Step 18</b> | <pre>show crypto pki certificates</pre> <p><b>Example:</b><br/> Router# show crypto pki certificates</p>                                       | (Optional) Displays information about your certificates, including any rollover certificates.                                                                                                                                                                                                                                                                                                                                                       |

## Examples

The following example shows the configuration for the “mytp-A” certificate server and its associated trustpoint, where RSA keys generated by the initial autoenrollment for the trustpoint will be stored on a USB token, “usbtokens0”:

```
crypto pki server mytp-A
 database level complete
 issuer-name CN=company, L=city, C=country
 grant auto
! Specifies that certificate requests will be granted automatically.
```

```
!
```

```
crypto pki trustpoint mytp-A
 revocation-check none
 rsakeypair myTP-A
 storage usbtoken0:
! Specifies that keys will be stored on usbtoken0:.
 on usbtoken0:
! Specifies that keys generated on initial auto enroll will be generated on and stored on ! usbtoken0:
```

## Configuring Manual Certificate Enrollment

Manual certificate enrollment can be set up via TFTP or the manual cut-and-paste method. Both options can be used if your CA does not support SCEP or if a network connection between the router and CA is not possible. Perform one of the following tasks to set up manual certificate enrollment:

- [Configuring Cut-and-Paste Certificate Enrollment, page 11](#)
- [Configuring TFTP Certificate Enrollment, page 14](#)

## PEM-Formatted Files for Certificate Enrollment Request

Using PEM-formatted files for certificate requests can be helpful for customers who are using terminal or profile-based enrollment to request certificates from their CA server. Customers using PEM-formatted files can directly use existing certificates on their Cisco IOS routers.

## Restrictions for Manual Certificate Enrollment

### Switching Enrollment URLs When Using SCEP

We do not recommend switching URLs if SCEP is used; that is, if the enrollment URL is “http://myca,” do not change the enrollment URL after getting the CA certificate and before enrolling the certificate. A user can switch between TFTP and manual cut-and-paste

### Key Regeneration Restriction

Do not regenerate the keys manually using the **crypto key generate** command; key regeneration will occur when the **crypto pki enroll** command is issued if the **regenerate** keyword is specified.

## Configuring Cut-and-Paste Certificate Enrollment

Perform this task to configure manual certificate enrollment via the cut-and-paste method for peers participating in your PKI.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment terminal** [*pem*]
5. **fingerprint** *ca-fingerprint*
6. **exit**

7. **crypto pki authenticate** *name*
8. **crypto pki enroll** *name*
9. **crypto pki import** *name* **certificate**
10. **exit**
11. **show crypto pki certificates**



## DETAILED STEPS

|        | Command or Action                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                             | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                    |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                     | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 3 | <b>crypto pki trustpoint name</b><br><br><b>Example:</b><br>Router(config)# crypto pki trustpoint mytp                             | Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.                                                                                                                                                                                                                                                                                                                                                               |
| Step 4 | <b>enrollment terminal [pem]</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# enrollment terminal                              | Specifies manual cut-and-paste certificate enrollment method. The certificate request will be displayed on the console terminal so that you may manually copied (or cut). <ul style="list-style-type: none"> <li><b>pem</b>—Configures the trustpoint to generate PEM-formatted certificate requests to the console terminal.</li> </ul>                                                                                                            |
| Step 5 | <b>fingerprint ca-fingerprint</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# fingerprint 12EF53FA 355CD23E 12EF53FA 355CD23E | (Optional) Specifies a fingerprint that can be matched against the fingerprint of a CA certificate during authentication. <p><b>Note</b> If the fingerprint is not provided, it will be displayed for verification.</p>                                                                                                                                                                                                                             |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                         | Exits ca-trustpoint configuration mode and returns to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                    |
| Step 7 | <b>crypto pki authenticate name</b><br><br><b>Example:</b><br>Router(config)# crypto pki authenticate mytp                         | Retrieves the CA certificate and authenticates it.                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 8 | <b>crypto pki enroll name</b><br><br><b>Example:</b><br>Router(config)# crypto pki enroll mytp                                     | Generates certificate request and displays the request for copying and pasting into the certificate server. <p>You are prompted for enrollment information, such as whether to include the router FQDN and IP address in the certificate request. You are also given the choice about displaying the certificate request to the console terminal.</p> <p>The base-64 encoded certificate with or without PEM headers as requested is displayed.</p> |

|         | Command or Action                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 9  | <b>crypto pki import</b> <i>name</i> <b>certificate</b><br><br><b>Example:</b><br>Router(config)# <b>crypto pki import</b> mytp<br>certificate | Imports a certificate manually at the console terminal (pasting).<br><br>The base-64 encoded certificate is accepted from the console terminal and inserted into the internal certificate database.<br><br><b>Note</b> You must enter this command twice if usage keys, a signature key and an encryption key, are used. The first time the command is entered, one of the certificates is pasted into the router. The second time the command is entered, the other certificate is pasted into the router. It does not matter which certificate is pasted first.<br><br><b>Note</b> Some CAs ignore the usage key information in the certificate request and issue general purpose usage certificates. If this applies to the certificate authority you are using, import the general purpose certificate. The router will not use one of the two key pairs generated. |
| Step 10 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# <b>exit</b>                                                                              | Exits global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 11 | <b>show crypto pki certificates</b><br><br><b>Example:</b><br>Router# <b>show crypto pki certificates</b>                                      | (Optional) Displays information about your certificates, the certificates of the CA, and RA certificates.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Configuring TFTP Certificate Enrollment

Perform this task to configure manual certificate enrollment using a TFTP server.

### Prerequisites for TFTP Certificate Enrollment

- You must know the correct URL to use if you are configuring certificate enrollment via TFTP.
- The router must be able to write a file to the TFTP server for the **crypto pki enroll** command.
- If using a file specification with the **enrollment** command, the file must contain the CA certificate either in binary format or be base-64 encoded.
- You must know if your CA ignores key usage information in a certificate request and issues only a general purpose usage certificate.



#### Caution

Some TFTP servers require that the file must exist on the server before it can be written.

Most TFTP servers require that the file be “write-able” by the world. This requirement may pose a risk

because any router or other device may write or overwrite the certificate request; thus, the replacement certificate request will not be used by the CA administrator, who must first check the enrollment request fingerprint before granting the certificate request.

---

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint *name***
4. **enrollment [mode] [retry period *minutes*] [retry count *number*] url *url* [pem]**
5. **fingerprint *ca-fingerprint***
6. **exit**
7. **crypto pki authenticate *name***
8. **crypto pki enroll *name***
9. **crypto pki import *name* certificate**
10. **exit**
11. **show crypto pki certificates**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                  | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                          | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 3 | <b>crypto pki trustpoint name</b><br><br><b>Example:</b><br>Router(config)# crypto pki trustpoint mytp                                                                                  | Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Step 4 | <b>enrollment [mode] [retry period minutes] [retry count number] url url [pem]</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# enrollment url tftp://certserver/file_specification | Specifies TFTP as the enrollment method to send the enrollment request and to retrieve the CA certificate and router certificate and any optional parameters.<br><br><b>Note</b> For TFTP enrollment, the url must be configured as a TFTP url, tftp://example_tftp_url.<br><br>An optional file specification filename may be included in the TFTP url. If the file specification is not included, the FQDN will be used. If the file specification is included, the router will append the extension “.ca” to the specified file name. |
| Step 5 | <b>fingerprint ca-fingerprint</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# fingerprint 12EF53FA 355CD23E 12EF53FA 355CD23E                                                      | (Optional) Specifies the fingerprint of the CA certificate received via an out-of-band method from the CA administrator.<br><br><b>Note</b> If the fingerprint is not provided, it will be displayed for verification.                                                                                                                                                                                                                                                                                                                   |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                                                                              | Exits ca-trustpoint configuration mode and returns to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 7 | <b>crypto pki authenticate name</b><br><br><b>Example:</b><br>Router(config)# crypto pki authenticate mytp                                                                              | Retrieves the CA certificate and authenticates it from the specified TFTP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

|                | Command or Action                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 8</b>  | <b>crypto pki enroll</b> <i>name</i><br><br><b>Example:</b><br>Router(config)# crypto pki enroll mytp                                | Generates certificate request and writes the request out to the TFTP server.<br><br>You are prompted for enrollment information, such as whether to include the router FQDN and IP address in the certificate request. You are queried about whether or not to display the certificate request to the console terminal.<br><br>The filename to be written is appended with the extension “.req”. For usage keys, a signature key and an encryption key, two requests are generated and sent. The usage key request filenames are appended with the extensions “-sign.req” and “-encr.req” respectively.                                                                                                                                                                                                                                                   |
| <b>Step 9</b>  | <b>crypto pki import</b> <i>name</i> <b>certificate</b><br><br><b>Example:</b><br>Router(config)# crypto pki import mytp certificate | Imports a certificate via TFTP at the console terminal, which retrieves the granted certificate.<br><br>The router will attempt to retrieve the granted certificate via TFTP using the same filename used to send the request, except the extension is changed from “.req” to “.crt”. For usage key certificates, the extensions “-sign.crt” and “-encr.crt” are used.<br><br>The router will parse the received files, verify the certificates, and insert the certificates into the internal certificate database on the router.<br><br><b>Note</b> Some CAs ignore the usage key information in the certificate request and issue general purpose usage certificates. If your CA ignores the usage key information in the certificate request, only import the general purpose certificate. The router will not use one of the two keypairs generated. |
| <b>Step 10</b> | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                           | Exits global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Step 11</b> | <b>show crypto pki certificates</b><br><br><b>Example:</b><br>Router# show crypto pki certificates                                   | (Optional) Displays information about your certificates, the certificates of the CA, and RA certificates.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## Configuring a Persistent Self-Signed Certificate for Enrollment via SSL

This section contains the following tasks:

- [Configuring a Trustpoint and Specifying Self-Signed Certificate Parameters, page 18](#)
- [Enabling the HTTPS Server, page 20](#)



### Note

These tasks are optional because if you enable the HTTPS server, it generates a self-signed certificate automatically using default values.

## Persistent Self-Signed Certificates Overview

The SSL protocol can be used to establish a secure connection between an HTTPS server and a client (web browser). During the SSL handshake, the client expects the SSL server's certificate to be verifiable using a certificate the client already possesses.

If Cisco IOS software does not have a certificate that the HTTPS server can use, the server generates a self-signed certificate by calling a PKI application programming interface (API). When the client receives this self-signed certificate and is unable to verify it, intervention is needed. The client asks you if the certificate should be accepted and saved for future use. If you accept the certificate, the SSL handshake continues.

Future SSL handshakes between the same client and the server use the same certificate. However, if the router is reloaded, the self-signed certificate is lost. The HTTPS server must then create a new self-signed certificate. This new self-signed certificate does not match the previous certificate so you are once again asked to accept it.

Requesting acceptance of the router's certificate each time that the router reloads may present an opportunity for an attacker to substitute an unauthorized certificate when you are being asked to accept the certificate. Persistent self-signed certificates overcome all these limitations by saving a certificate in the router's startup configuration.

## Restrictions

You can configure only one trustpoint for a persistent self-signed certificate.

## Configuring a Trustpoint and Specifying Self-Signed Certificate Parameters

Perform the following task to configure a trustpoint and specify self-signed certificate parameters.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment selfsigned**
5. **subject-name** [*x.500-name*]
6. **rsa** *key-label* [*key-size* [*encryption-key-size*]]
7. **crypto pki enroll** *name*
8. **end**
9. **show crypto pki certificates** [*trustpoint-name* [*verbose*]]
10. **show crypto pki trustpoints** [*status* | *label* [*status*]]

## DETAILED STEPS

|        | Command or Action                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                 | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 3 | <b>crypto pki trustpoint name</b><br><br><b>Example:</b><br>Router(config)# crypto pki trustpoint local                                        | Declares the CA that your router should use and enters ca-trustpoint configuration mode.<br><br><b>Note</b> Effective with Cisco IOS Release 12.3(8)T, the <b>crypto pki trustpoint</b> command replaced the <b>crypto ca trustpoint</b> command.                                                                                                                                                                                                                                                                                                      |
| Step 4 | <b>enrollment selfsigned</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# enrollment selfsigned                                            | Specifies self-signed enrollment.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 5 | <b>subject-name [x.500-name]</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# subject-name                                                 | (Optional) Specifies the requested subject name to be used in the certificate request. <ul style="list-style-type: none"> <li>If the <i>x-500-name</i> argument is not specified, the FQDN, which is the default subject name, is used.</li> </ul>                                                                                                                                                                                                                                                                                                     |
| Step 6 | <b>rsakeypair key-label [key-size [encryption-key-size]]</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# rsakeypair examplekeys 1024 1024 | (Optional) Specifies which key pair to associate with the certificate. <ul style="list-style-type: none"> <li>The <i>key-label</i> argument will be generated during enrollment if it does not already exist or if the <b>auto-enroll regenerate</b> command was issued.</li> <li>Specify the <i>key-size</i> argument for generating the key, and specify the <i>encryption-key-size</i> argument to request separate encryption, signature keys, and certificates.</li> </ul> <b>Note</b> If this command is not enabled, the FQDN key pair is used. |
| Step 7 | <b>crypto pki enroll name</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# crypto pki enroll local                                         | Tells the router to generate the persistent self-signed certificate.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 8 | <b>end</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# end<br><br><b>Example:</b><br>Router(config)# end                                  | (Optional) Exits ca-trustpoint configuration mode and global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

|         | Command or Action                                                                                                                                                     | Purpose                                                                                                                            |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Step 9  | <b>show crypto pki certificates</b> [ <i>trustpoint-name</i> ]<br>[ <i>verbose</i> ]]<br><br><b>Example:</b><br>Router# show crypto pki certificates local<br>verbose | Displays information about your certificate, the certification authority certificate, and any registration authority certificates. |
| Step 10 | <b>show crypto pki trustpoints</b> [ <i>status</i>   <i>label</i> ]<br>[ <i>status</i> ]]<br><br><b>Example:</b><br>Router# show crypto pki trustpoints status        | Displays the trustpoints that are configured in the router.                                                                        |

## Enabling the HTTPS Server

Perform the following task to enable the HTTPS server.

### Prerequisites

To specify parameters, you must create a trustpoint and configure it. To use default values, delete any existing self-signed trustpoints. Deleting all self-signed trustpoints causes the HTTPS server to generate a persistent self-signed certificate using default values as soon as the server is enabled.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http secure-server**
4. **end**
5. **copy system:running-config nvram: startup-config**



## DETAILED STEPS

|        | Command or Action                                                                                                                        | Purpose                                                                                                           |
|--------|------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>  |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                           | Enters global configuration mode.                                                                                 |
| Step 3 | <b>ip http secure-server</b><br><br><b>Example:</b><br>Router(config)# ip http secure-server                                             | Enables the secure HTTP web server.<br><br><b>Note</b> A key pair (modulus 1024) and a certificate are generated. |
| Step 4 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                                 | Exits global configuration mode.                                                                                  |
| Step 5 | <b>copy system:running-config nvram:startup-config</b><br><br><b>Example:</b><br>Router# copy system:running-config nvram:startup-config | Saves the self-signed certificate and the HTTPS server in enabled mode.                                           |

## Configuring a Certificate Enrollment Profile for Enrollment or Reenrollment

Perform this task to configure an enrollment profile for certificate enrollment or reenrollment of a router with a Cisco IOS CA that is already enrolled with a third-party vendor CA.

Enable a router that is enrolled with a third-party vendor CA to use its existing certificate to enroll with the Cisco IOS certificate server so the enrollment request is automatically granted. To enable this functionality, you must issue the **enrollment credential** command. Also, you cannot configure manual certificate enrollment.

### Prerequisites

Before configuring a certificate enrollment profile for the client router that is already enrolled with a third party vendor CA so that the router can reenroll with a Cisco IOS certificate server, you should have already performed the following tasks at the client router:

- Defined a trustpoint that points to the third-party vendor CA.
- Authenticated and enrolled the client router with the third-party vendor CA.

### Restrictions

- To use certificate profiles, your network must have an HTTP interface to the CA.

- If an enrollment profile is specified, an enrollment URL may not be specified in the trustpoint configuration. Although both commands are supported, only one command can be used at a time in a trustpoint.
- Because there is no standard for the HTTP commands used by various CAs, the user is required to enter the command that is appropriate to the CA that is being used.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment profile** *label*
5. **exit**
6. **crypto pki profile enrollment** *label*
7. **authentication url** *url*  
or  
**authentication terminal**
8. **authentication command**
9. **enrollment url** *url*  
or  
**enrollment terminal**
10. **enrollment credential** *label*
11. **enrollment command**
12. **parameter** *number* {**value** *value* | **prompt** *string*}
13. **exit**
14. **show crypto pki certificates**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                       | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 3 | <b>crypto pki trustpoint name</b><br><br><b>Example:</b><br>Router(config)# crypto pki trustpoint Entrust                                                                                                                                            | Declares the trustpoint and a given name and enter ca-trustpoint configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 4 | <b>enrollment profile label</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# enrollment profile E                                                                                                                                                | Specifies that an enrollment profile is to be used for certificate authentication and enrollment.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(ca-trustpoint)# exit                                                                                                                                                                                    | Exits ca-trustpoint configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 6 | <b>crypto pki profile enrollment label</b><br><br><b>Example:</b><br>Router(config)# crypto pki profile enrollment E                                                                                                                                 | Defines an enrollment profile and enters ca-profile-enroll configuration mode. <ul style="list-style-type: none"> <li><b>label</b>—Name for the enrollment profile; the enrollment profile name must match the name specified in the <b>enrollment profile</b> command.</li> </ul>                                                                                                                                                                                                                                                                                                                        |
| Step 7 | <b>authentication url url</b><br><br><b>Example:</b><br>Router(ca-profile-enroll)# authentication url http://entrust:81<br><br>or<br><br><b>authentication terminal</b><br><br><b>Example:</b><br>Router(ca-profile-enroll)# authentication terminal | Specifies the URL of the CA server to which to send certificate authentication requests. <ul style="list-style-type: none"> <li><b>url</b>—URL of the CA server to which your router should send authentication requests.</li> </ul> <p>If using HTTP, the URL should read “http://CA_name,” where CA_name is the host DNS name or IP address of the CA.</p> <p>If using TFTP, the URL should read “tftp://certserver/file_specification.” (If the URL does not include a file specification, the FQDN of the router will be used.)</p> <p>Specifies manual cut-and-paste certificate authentication.</p> |

|         | Command or Action                                                                                                                                                                                                                                      | Purpose                                                                                                                                                                                                  |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 8  | <b>authentication command</b><br><br><b>Example:</b><br>Router(ca-profile-enroll)# authentication command                                                                                                                                              | (Optional) Specifies the HTTP command that is sent to the CA for authentication.<br><br>This command should be used after the <b>authentication url</b> command has been entered.                        |
| Step 9  | <b>enrollment url url</b><br><br><b>Example:</b><br>Router(ca-profile-enroll)# enrollment url http://entrust:81/cda-cgi/clientcgi.exe<br>or<br><br><b>enrollment terminal</b><br><br><b>Example:</b><br>Router(ca-profile-enroll)# enrollment terminal | Specifies the URL of the CA server to which to send certificate enrollment requests via HTTP or TFTP.<br><br><br><br><br>Specifies manual cut-and-paste certificate enrollment.                          |
| Step 10 | <b>enrollment credential label</b><br><br><b>Example:</b><br>Router(ca-profile-enroll)# enrollment credential Entrust                                                                                                                                  | (Optional) Specifies the third-party vendor CA trustpoint that is to be enrolled with the Cisco IOS CA.<br><br><b>Note</b> This command cannot be issued if manual certificate enrollment is being used. |
| Step 11 | <b>enrollment command</b><br><br><b>Example:</b><br>Router(ca-profile-enroll)# enrollment command                                                                                                                                                      | (Optional) Specifies the HTTP command that is sent to the CA for enrollment.                                                                                                                             |
| Step 12 | <b>parameter number {value value   prompt string}</b><br><br><b>Example:</b><br>Router(ca-profile-enroll)# parameter 1 value aaaa-bbbb-cccc                                                                                                            | (Optional) Specifies parameters for an enrollment profile.<br><br>This command can be used multiple times to specify multiple values.                                                                    |
| Step 13 | <b>exit</b><br><br><b>Example:</b><br>Router(ca-profile-enroll)# exit<br>Router(config)# exit                                                                                                                                                          | Enter this command two times—one time to exit ca-profile-enroll configuration mode and the second time to exit global configuration mode.                                                                |
| Step 14 | <b>show crypto pki certificates</b><br><br><b>Example:</b><br>Router# show crypto pki certificates                                                                                                                                                     | (Optional) Displays information about your certificates, the certificates of the CA, and RA certificates.                                                                                                |

## What to Do Next

If you configured the router to reenroll with a Cisco IOS CA, you should configure the Cisco IOS certificate server to accept enrollment requests only from clients already enrolled with the specified third-party vendor CA trustpoint to take advantage of this functionality. For more information, see the module “Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment.”

# Configuration Examples for PKI Certificate Enrollment Requests

This section contains the following configuration examples:

- [Configuring Autoenrollment: Example, page 25](#)
- [Configuring Certificate Autoenrollment with Key Regeneration: Example, page 26](#)
- [Configuring Cut-and-Paste Certificate Enrollment: Example, page 27](#)
- [Configuring Manual Certificate Enrollment with Key Regeneration: Example, page 30](#)
- [Creating and Verifying a Persistent Self-Signed Certificate: Example, page 30](#)
- [Configuring Direct HTTP Enrollment: Example, page 32](#)

## Configuring Autoenrollment: Example

The following example shows how to configure the router to automatically enroll with a CA on startup, enabling automatic rollover, and how to specify all necessary enrollment information in the configuration:

```
crypto pki trustpoint frog
 enrollment url http://frog.phoobin.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet-0
 serial-number none
 usage ike
 auto-enroll regenerate
 password revokeme
 rsa-key frog 2048
!
crypto pki certificate chain frog
certificate pki 0B
30820293 3082023D A0030201 0202010B 300D0609 2A864886 F70D0101 04050030
79310B30 09060355 04061302 5553310B 30090603 55040813 02434131 15301306
0355040A 130C4369 73636F20 53797374 656D3120 301E0603 55040B13 17737562
6F726420 746F206B 6168756C 75692049 50495355 31243022 06035504 03131B79
6E692D75 31302043 65727469 66696361 7465204D 616E6167 6572301E 170D3030
30373134 32303536 32355A17 0D303130 37313430 31323834 335A3032 310E300C
06035504 0A130543 6973636F 3120301E 06092A86 4886F70D 01090216 11706B69
2D343562 2E636973 636F2E63 6F6D305C 300D0609 2A864886 F70D0101 01050003
4B003048 024100B3 0512A201 3B4243E1 378A9703 8AC5E3CE F77AF987 B5A422C4
15E947F6 70997393 70CF34D6 63A86B9C 4347A81A 0551FC02 ABA62360 01EF7DD2
6C136AEB 3C6C3902 03010001 A381F630 81F3300B 0603551D 0F040403 02052030
1C060355 1D110415 30138211 706B692D 3435622E 63697363 6F2E636F 6D301D06
03551D0E 04160414 247D9558 169B9A21 23D289CC 2DDA2A9A 4F77C616 301F0603
551D2304 18301680 14BD742C E892E819 1D551D91 683F6DB2 D8847A6C 73308185
0603551D 1F047E30 7C307AA0 3CA03AA4 38303631 0E300C06 0355040A 13054369
73636F31 24302206 03550403 131B796E 692D7531 30204365 72746966 69636174
65204D61 6E616765 72A23AA4 38303631 0E300C06 0355040A 13054369 73636F31
24302206 03550403 131B796E 692D7531 30204365 72746966 69636174 65204D61
6E616765 72300D06 092A8648 86F70D01 01040500 03410015 BC7CECF9 696697DF
E887007F 7A8DA24F 1ED5A785 C5C60452 47860061 0C18093D 08958A77 5737246B
0A25550A 25910E27 8B8B428E 32F8D948 3DD1784F 954C70
quit
```



### Note

In this example, keys are neither regenerated nor rolled over.

## Configuring Certificate Autoenrollment with Key Regeneration: Example

The following example shows how to configure the router to automatically enroll with the CA named “trustme1” on startup and enable automatic rollover. The **regenerate** keyword is issued, so a new key will be generated for the certificate and reissued when the automatic rollover process is initiated. The renewal percentage is configured as 90 so if the certificate has a lifetime of one year, a new certificate is requested 36.5 days before the old certificate expires. The changes made to the running configuration are saved to the NVRAM startup configuration because autoenrollment will not update NVRAM if the running configuration has been modified but not written to NVRAM.

```
crypto pki trustpoint trustme1
 enrollment url http://trustme1.company.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet0
 serial-number none
 auto-enroll 90 regenerate
 password revokeme
 rsakeypair trustme1 2048
 exit
crypto pki authenticate trustme1
copy system:running-config nvram:startup-config
```

## Configuring Cut-and-Paste Certificate Enrollment: Example

The following example shows how to configure certificate enrollment using the manual cut-and-paste enrollment method:

```
Router(config)# crypto pki trustpoint TP
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# crypto pki authenticate TP
```

Enter the base 64 encoded CA certificate.  
End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
MIICNDCCAd6gAwIBAgIQOsCmXpVHwodKryRoqULV7jANBgkqhkiG9w0BAQUFADA5
MQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2l2Y28gU3lzdGVtczESMBAGA1UEAxMJ
bXNjYSl5b290MB4XDATyMDIxNDAwNDYwMVoXDATyMDIxNDAwNTQ0OjFwOTELMAkG
A1UEBhMCVVMxMjEwMDYwMDYwMDYwMDYwMDYwMDYwMDYwMDYwMDYwMDYwMDYwMDYw
cm9vdDBCMCA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCix8nIGFg+wvy3BjFbVi25wYoG
K2N0HWWHqpxFuFhgyBnIC00shIn9CtRdN3JvUNHr0N1KocEwNKUGYmPwWGTfAgMB
AAGjgcEwgb4wCwYDVR0PBAQDAgHGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYE
FKIacsl6dKAfuNDVQymLSp7esf8jMG0GA1UdHwRmMGQwL6AtoCuGKWh0dHA6Ly9t
c2NhLXJvb3QvQ2VydeVucm9sbC9tc2NhLXJvb3QvY3J3SMDGg6L6AthitmaWx1oi8v
XFxtc2NhLXJvb3RcQ2VydeVucm9sbC9tc2NhLXJvb3QvY3J3SMBAGCSsGAQQBgjcV
AQQDAgEAMA0GCSqGSIb3DQEBAQUAA0EAEuZkZMX9qkoLHfETYPVWjZPQbBmwNRA
oUDSDydtL3BcI/uLL5q7EmODyGfLyMGxuhQYx5r/40aSQgLCqBq+yg==
-----END CERTIFICATE-----
```

```
Certificate has the following attributes:
Fingerprint: D6C12961 CD78808A 4E02193C 0790082A
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

```
Router(config)# crypto pki enroll TP
% Start certificate enrollment..
```

```
% The subject name in the certificate will be: Router.company.com
% Include the router serial number in the subject name? [yes/no]: n
% Include an IP address in the subject name? [no]: n
Display Certificate Request to terminal? [yes/no]: y
Signature key certificate request -
Certificate Request follows:
```

```
MIIBhTCB7wIBADAlMSMwIQYJKoZIhvcNAQkCFhRTYw5kQmFnZ2VyLmNpc2NvLmNv
bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwGyKCGYEAxdhXFDiWAn/hIZs9zf0tssKA
daoWYu0ms9Fe/Pew01dh14vXdxgacst0s2Pr5wk6jLOPxpvx0JPWYQM6ipLmyVxv
ojhyLTrVohrh6Dnqcvk+G/5ohss9o9RxvONwx042pQchFn9EkMuZC7evwRxJEQR
mBHXBZ8GmP3jYQsjS8MCAwEAAaAhMB8GCSqGSIb3DQEJJDjESMBAwDgYDVR0PAAQh/
BAQDAgeAMA0GCSqGSIb3DQEBAQUAA4GBAMT6WtyFw95POY7UUtF+YIYHiVRUF4SCq
hRIAGrljUePLo9iTqyPU1Pnt8JnIZ5P5BHU3MfgP8sqodaWub6mubkzaohJ1qD06
087fnLCNid5Tov5jKogFHIki2EGGZxBosUw91JlenQdNdDPbJc5LIWdfDvcia6jO
N18rOtKnt8Q+
!
!
!
Redisplay enrollment request? [yes/no]:
Encryption key certificate request -
Certificate Request follows:
```

```
MIIBhTCB7wIBADAlMSMwIQYJKoZIhvcNAQkCFhRTYw5kQmFnZ2VyLmNpc2NvLmNv
bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwGyKCGYEAwG60QojpDbzbKnyj8FyTiOcv
ThkDP7XD4vLT1XaJ409z0gSiOgnIcdFtXhV1BWtpq3/09zyFXr1tH+BMCRQi3Lts
0IpxYa3D9iFPqev7SPXpsAIsY8a6FMq7TiwLObqiQjLKL4cbuV0Frj10Yuv5A/Z+
```

```
kqMOM7c+pWNWfDle9lsCAwEAAAhMB8GCSqGSIB3DQEJDjESMBAwDgYDVR0PAQH/
BAQDAgUGMA0GCSqGSIB3DQEBBAUAA4GBACF7feURj/fJMoJPBRL6fa9BrlMJx+2F
H91YM/Ciiz2n4mHTeWTKhLoT8wUfa9NGOk7yi+nF/F7035twLf6n2bSCTW4aem
8jLMMaeFwxkrV/ceQKrucmNC1uVx+fBy9rhnx8j60XE25tnp1U08r6om/pBQABU
eNPFhozcaQ/2
```

```
!
```

```
!
```

```
!
```

```
Redisplay enrollment request? [yes/no]: n
```

```
Router(config)# crypto pki import TP certificate
```

Enter the base 64 encoded certificate.

End with a blank line or the word "quit" on a line by itself

```
MIIDajCCAxSgAwIBAgIKFN7C6QAAAAAMRzANBgkqhkiG9w0BAQUFADA5MQswCQYD
VQQGEwJVUzEWMBQGA1UEChMNQ2l2Y28gU3lzdGVtczESMBAGA1UEAxMJbXNjYS1y
b290MB4XDFAyMDYwODAxMTY0MloXDFAzMDYwODAxMjY0MlowJTEjMCEGCSqGSIB3
DQEJAhMUU2FuZEJhZ2dlci5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAMUyVxQ4lgJ/4SGbPc3zrbLCgHWqFmLtrPRXvz3sNNXYdeL13cYnLL
TrNj6+cJOoyzj8ab8TiTlskDOogS5slcb6I4ci061aIa4eg56nL5Phv+aIbLPaPU
cbzjcMdonqUHIRZ8fRJDLMQu3r8EcSRKkZgR1wWfBpj942ELI0vDagMBAAGjggHM
MIIBYDALBgNVHQ8EBAMCB4AwHQYDVR0OBBYEF8Quz8dyz4EGIEKx9A8UMNHLE4s
MHAGA1UdIwRpmGeAFKIacsl6dKAfuNDVQym1Sp7esf8joT2kOzA5MQswCQYDVQGG
EwJVUzEWMBQGA1UEChMNQ2l2Y28gU3lzdGVtczESMBAGA1UEAxMJbXNjYS1yb290
ghA6wKZelUfCh0qvJGipQtXuMCIGA1UdEQEB/wQYMBaCFNhbmcRCYWDnZXIuY2l2
Y28uY29tMG0GA1UdHwRmMGQwL6AtoCuGKWh0dHA6Ly9tc2NhLXJvb3QvQ2VydEVu
cm9sbC9tc2NhLXJvb3QvY3J5MDGgG6AthitmaWx10i8vXFxtc2NhLXJvb3RcQ2Vy
dEVucm9sbFxtc2NhLXJvb3QvY3J5SMIGUBggrBgEFBQcBAQSBhzbCBhDA/BggrBgEF
BQcwAoYzahr0cDovL2l2Y2Etc9vdC9DZXJ0RW5yb2xsL2l2Y2Etc9vdF9tc2Nh
LXJvb3QvY3J0MEEGCCSGAQUFBzAchjVmaWx10i8vXFxtc2NhLXJvb3RcQ2VydEVu
cm9sbFxtc2NhLXJvb3RfbXNjYS1yb290LmNydANBgkqhkiG9w0BAQUFAANBAJo2
r6sHPGBdTX2EDoJpR/A2UHXxRYqVSHkFKZw0z31r5JzUM0oPNUETV7mnZlYNVRZ
CSEX/G8boi3W0jz9wZo=
```

```
% Router Certificate successfully imported
```

```
Router(config)# crypto pki import TP cert
```

Enter the base 64 encoded certificate.

End with a blank line or the word "quit" on a line by itself

```
MIIDajCCAxSgAwIBAgIKFN7OBQAAAAAMSDANBgkqhkiG9w0BAQUFADA5MQswCQYD
VQQGEwJVUzEWMBQGA1UEChMNQ2l2Y28gU3lzdGVtczESMBAGA1UEAxMJbXNjYS1y
b290MB4XDFAyMDYwODAxMTY0NVVoXDFAzMDYwODAxMjY0NVVowJTEjMCEGCSqGSIB3
DQEJAhMUU2FuZEJhZ2dlci5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAMUyVxQ4lgJ/4SGbPc3zrbLCgHWqFmLtrPRXvz3sNNXYdeL13cYnLL
TrNj6+cJOoyzj8ab8TiTlskDOogS5slcb6I4ci061aIa4eg56nL5Phv+aIbLPaPU
cbzjcMdonqUHIRZ8fRJDLMQu3r8EcSRKkZgR1wWfBpj942ELI0vDagMBAAGjggHM
MIIBYDALBgNVHQ8EBAMCB4AwHQYDVR0OBBYEF8Quz8dyz4EGIEKx9A8UMNHLE4s
MHAGA1UdIwRpmGeAFKIacsl6dKAfuNDVQym1Sp7esf8joT2kOzA5MQswCQYDVQGG
EwJVUzEWMBQGA1UEChMNQ2l2Y28gU3lzdGVtczESMBAGA1UEAxMJbXNjYS1yb290
ghA6wKZelUfCh0qvJGipQtXuMCIGA1UdEQEB/wQYMBaCFNhbmcRCYWDnZXIuY2l2
Y28uY29tMG0GA1UdHwRmMGQwL6AtoCuGKWh0dHA6Ly9tc2NhLXJvb3QvQ2VydEVu
cm9sbC9tc2NhLXJvb3QvY3J5MDGgG6AthitmaWx10i8vXFxtc2NhLXJvb3RcQ2Vy
dEVucm9sbFxtc2NhLXJvb3QvY3J5SMIGUBggrBgEFBQcBAQSBhzbCBhDA/BggrBgEF
BQcwAoYzahr0cDovL2l2Y2Etc9vdC9DZXJ0RW5yb2xsL2l2Y2Etc9vdF9tc2Nh
LXJvb3QvY3J0MEEGCCSGAQUFBzAchjVmaWx10i8vXFxtc2NhLXJvb3RcQ2VydEVu
cm9sbFxtc2NhLXJvb3RfbXNjYS1yb290LmNydANBgkqhkiG9w0BAQUFAANBAHaU
hyCwLirUghNxCmLzXRG7C3W1j0kSX7a4fX9OxKR/Z2SoMjdmNPPyApuh8SoT2zBP
ZKjZU2WjczG/nZF4W5k=
```

```
% Router Certificate successfully imported
```



You can verify that the certificate was successfully imported by issuing the **show crypto pki certificate** command.

```
Router# show crypto pki certificate
Certificate
 Status: Available
 Certificate Serial Number: 14DECE05000000000C48
 Certificate Usage: Encryption
 Issuer:
 CN = TPCA-root
 O = Company
 C = US
 Subject:
 Name: Router.company.com
 OID.1.2.840.113549.1.9.2 = Router.company.com
 CRL Distribution Point:
 http://tpca-root/CertEnroll/tpca-root.crl
 Validity Date:
 start date: 18:16:45 PDT Jun 7 2002
 end date: 18:26:45 PDT Jun 7 2003
 renew date: 16:00:00 PST Dec 31 1969
 Associated Trustpoints: TP
```

```
Certificate
 Status: Available
 Certificate Serial Number: 14DEC2E9000000000C47
 Certificate Usage: Signature
 Issuer:
 CN = tpca-root
 O = company
 C = US
 Subject:
 Name: Router.company.com
 OID.1.2.840.113549.1.9.2 = Router.company.com
 CRL Distribution Point:
 http://tpca-root/CertEnroll/tpca-root.crl
 Validity Date:
 start date: 18:16:42 PDT Jun 7 2002
 end date: 18:26:42 PDT Jun 7 2003
 renew date: 16:00:00 PST Dec 31 1969
 Associated Trustpoints: TP
```

```
CA Certificate
 Status: Available
 Certificate Serial Number: 3AC0A65E9547C2874AAF2468A942D5EE
 Certificate Usage: Signature
 Issuer:
 CN = tpca-root
 O = Company
 C = US
 Subject:
 CN = tpca-root
 O = company
 C = US
 CRL Distribution Point:
 http://tpca-root/CertEnroll/tpca-root.crl
 Validity Date:
 start date: 16:46:01 PST Feb 13 2002
 end date: 16:54:48 PST Feb 13 2007
 Associated Trustpoints: TP
```

## Configuring Manual Certificate Enrollment with Key Regeneration: Example

The following example shows how to regenerate new keys with a manual certificate enrollment from the CA named “trustme2”:

```
crypto pki trustpoint trustme2
 enrollment url http://trustme2.company.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet0
 serial-number none
 regenerate
 password revokeme
 rsakeypair trustme2 2048s
 exit
crypto pki authenticate trustme2
crypto pki enroll trustme2
```

## Creating and Verifying a Persistent Self-Signed Certificate: Example

The following example shows how to declare and enroll a trustpoint named “local” and generate a self-signed certificate with an IP address:

```
crypto pki trustpoint local
 enrollment selfsigned
 end
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

crypto pki enroll local
Nov 29 20:51:13.067: %SSH-5-ENABLED: SSH 1.99 has been enabled
Nov 29 20:51:13.267: %CRYPTO-6-AUTOGEN: Generated new 512 bit key pair
% Include the router serial number in the subject name? [yes/no]: yes
% Include an IP address in the subject name? [no]: yes
Enter Interface name or IP Address[]: ethernet 0
Generate Self Signed Router Certificate? [yes/no]: yes
Router Self Signed Certificate successfully created
```



### Note

A router can have only one self-signed certificate. If you attempt to enroll a trustpoint configured for a self-signed certificate and one already exists, you receive a notification and are asked if you want to replace it. If so, a new self-signed certificate is generated to replace the existing one.

### Enabling the HTTPS Server: Example

The following example shows how to enable the HTTPS server and generate a default trustpoint because one was not previously configured:

```
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

ip http secure-server
% Generating 1024 bit RSA keys ...[OK]
*Dec 21 19:14:15.421:%PKI-4-NOAUTOSAVE:Configuration was modified. Issue "write memory"
to save new certificate
Router(config)#
```



### Note

You need to save the configuration to NVRAM if you want to keep the self-signed certificate and have the HTTPS server enabled following router reloads.

The following message also appears:

```
*Dec 21 19:14:10.441:%SSH-5-ENABLED:SSH 1.99 has been enabled
```



#### Note

Creation of the key pair used with the self-signed certificate causes the Secure Shell (SSH) server to start. This behavior cannot be suppressed. You may want to modify your access control lists (ACLs) to permit or deny SSH access to the router.

### Verifying the Self-Signed Certificate Configuration: Example

The following example displays information about the self-signed certificate that you just created:

```
Router# show crypto pki certificates
```

```
Router Self-Signed Certificate
 Status: Available
 Certificate Serial Number: 01
 Certificate Usage: General Purpose
 Issuer:
 cn=IOS-Self-Signed-Certificate-3326000105
 Subject:
 Name: IOS-Self-Signed-Certificate-3326000105
 cn=IOS-Self-Signed-Certificate-3326000105
 Validity Date:
 start date: 19:14:14 GMT Dec 21 2004
 end date: 00:00:00 GMT Jan 1 2020
 Associated Trustpoints: TP-self-signed-3326000105
```



#### Note

The number 3326000105 above is the router's serial number and varies depending on the router's actual serial number.

The following example displays information about the key pair corresponding to the self-signed certificate:

```
Router# show crypto key mypubkey rsa
```

```
% Key pair was generated at: 19:14:10 GMT Dec 21 2004
Key name: TP-self-signed-3326000105
Usage: General Purpose Key
Key is not exportable.
Key Data:
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00B88F70
6BC78B6D 67D6CFF3 135C1D91 8F360292 CA44A032 5AC1A8FD 095E4865 F8C95A2B
BFD1C2B7 E64A3804 9BBD7326 207BD456 19BAB78B D075E78E 00D2560C B09289AE
6DEC8B80 6672FB3A 5CDAEE92 9D4C4F71 F3BCB269 214F6293 4BA8FABF 9486BCFC
2B941BCA 550999A7 2EFE12A5 6B7B669A 2D88AB77 39B38E0E AA23CB8C B7020301 0001
% Key pair was generated at: 19:14:13 GMT Dec 21 2004
Key name: TP-self-signed-3326000105.server
Usage: Encryption Key
Key is not exportable.
Key Data:
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00C5680E 89777B42
463E5783 FE96EA9E F446DC7B 70499AF3 EA266651 56EE29F4 5B003D93 2FC9F81D
8A46E12F 3FBAC2F3 046ED9DD C5F27C20 1BBA6B9B 08F16E45 C34D6337 F863D605
34E30F0E B4921BC5 DAC9EBBA 50C54AA0 BF551BDD 88453F50 61020301 0001
```



#### Note

The second key pair with the name TP-self-signed-3326000105.server is the SSH key pair and is generated when any key pair is created on the router and SSH starts up.

The following example displays information about the trustpoint named “local”:

```
Router# show crypto pki trustpoints
```

```
Trustpoint local:
 Subject Name:
 serialNumber=C63EBBE9+ipaddress=10.3.0.18+hostname=test.company.com
 Serial Number: 01
 Persistent self-signed certificate trust point
```

## Configuring Direct HTTP Enrollment: Example

The following example show how to configure an enrollment profile for direct HTTP enrollment with a CA server:

```
crypto pki trustpoint Entrust
 enrollment profile E
 serial

crypto pki profile enrollment E
 authentication url http://entrust:81
 authentication command GET /certs/cacert.der
 enrollment url http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command POST reference_number=$P2&authcode=$P1
 &retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

## Additional References

The following sections provide references related to certificate enrollment for a PKI.

## Related Documents

| Related Topic                                                              | Document Title                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| USB Token RSA Operations: Benefits of using USB tokens                     | “ <a href="#">Storing PKI Credentials</a> ” module in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4T                                                                                                                                                                                                              |
| USB Token RSA Operations: Certificate server configuration                 | “ <a href="#">Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment</a> ” chapter in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4T.<br><br>See the “Generating a Certificate Server RSA Key Pair” section, the “Configuring a Certificate Server Trustpoint” section, and related examples. |
| Overview of PKI, including RSA keys, certificate enrollment, and CAs.      | “ <a href="#">Cisco IOS PKI Overview: Understanding and Planning a PKI</a> ” module in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4                                                                                                                                                                              |
| Secure Device Provisioning: functionality overview and configuration tasks | “ <a href="#">Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI</a> ” module in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4T                                                                                                                                                                  |
| RSA key generation and deployment                                          | “ <a href="#">Deploying RSA Keys Within a PKI</a> ” module in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4T                                                                                                                                                                                                      |
| Cisco IOS certificate server overview information and configuration tasks  | “ <a href="#">Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment</a> ” module in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4T                                                                                                                                                           |
| Setting up and using a USB token                                           | “ <a href="#">Storing PKI Credentials</a> ” module in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4T                                                                                                                                                                                                              |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Feature Information for PKI Certificate Enrollment

[Table 1](#) lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Implementing and Managing PKI Features Roadmap](#).”

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

---

[Table 1](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

---

**Table 1**      **Feature Information for PKI Certificate Enrollment**

| Feature Name                                 | Releases  | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco IOS USB Token PKI Enhancements—Phase 2 | 12.4(11)T | <p>This feature enhances USB token functionality by using the USB token as a cryptographic device. USB tokens may be used for RSA operations such as key generation, signing, and authentication.</p> <p>The following sections in this document provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuring Certificate Enrollment or Autoenrollment</a></li> </ul> <p><b>Note</b> This document covers the use of utilizing USB tokens for RSA operations during initial autoenrollment for a trustpoint. For other documents on this topic, see the “<a href="#">Related Documents</a>” section.</p>                                                                                                                                                  |
| Certificate Authority (CA) Key Rollover      | 12.4(2)T  | <p>This feature introduces the ability for root CAs to roll over expiring CA certificates and keys and to have these changes propagate through the PKI network without manual intervention.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Automatic Certificate Enrollment</a></li> <li>• <a href="#">Configuring Certificate Enrollment or Autoenrollment</a></li> </ul> <p>The following commands were introduced or modified by this feature: <b>auto-rollover</b>, <b>crypto pki certificate chain</b>, <b>crypto pki export pem</b>, <b>crypto pki server</b>, <b>crypto pki server info request</b>, <b>show crypto pki certificates</b>, <b>show crypto pki server</b>, and <b>show crypto pki trustpoint</b></p> |
| Certificate Autoenrollment                   | 12.2(8)T  | <p>This feature introduces certificate autoenrollment, which allows the router to automatically request a certificate from the CA that is using the parameters in the configuration.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Automatic Certificate Enrollment</a></li> <li>• <a href="#">Configuring Certificate Enrollment or Autoenrollment</a></li> </ul> <p>The following commands were introduced by this feature: <b>auto-enroll</b>, <b>rsa keypair</b>, <b>show crypto ca timers</b></p>                                                                                                                                                                                                                   |

**Table 1** *Feature Information for PKI Certificate Enrollment (continued)*

| Feature Name                                          | Releases | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Certificate Enrollment Enhancements                   | 12.2(8)T | <p>This feature introduces five new <b>crypto ca trustpoint</b> subcommands that provide new options for certificate requests and allow users to specify fields in the configuration instead of having to go through prompts.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuring Certificate Enrollment or Autoenrollment</a></li> </ul> <p>The following commands were introduced by this feature:<br/> <b>ip-address (ca-trustpoint), password (ca-trustpoint), serial-number, subject-name, usage</b></p>                                                                                                                                                                                                                           |
| Direct HTTP Enrollment with CA Servers                | 12.3(4)T | <p>This feature allows users to configure an enrollment profile if their CA server does not support SCEP and they do not want to use an RA-mode CS. The enrollment profile allows users to send HTTP requests directly to the CA server instead of to an RA-mode CS.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Certificate Enrollment Profiles</a></li> <li>• <a href="#">Configuring a Certificate Enrollment Profile for Enrollment or Reenrollment</a></li> </ul> <p>The following commands were introduced by this feature:<br/> <b>authentication command, authentication terminal, authentication url, crypto ca profile enrollment, enrollment command, enrollment profile, enrollment terminal, enrollment url, parameter</b></p> |
| Import of RSA Key Pair and Certificates in PEM Format | 12.3(4)T | <p>This feature allows customers to issue certificate requests and receive issued certificates in PEM-formatted files.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuring Manual Certificate Enrollment</a></li> </ul> <p>The following commands were modified by this feature:<br/> <b>enrollment, enrollment terminal</b></p>                                                                                                                                                                                                                                                                                                                                                                                                        |



**Table 1** *Feature Information for PKI Certificate Enrollment (continued)*

| Feature Name                                       | Releases                                | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Key Rollover for Certificate Renewal               | 12.3(7)T                                | <p>This feature allows the certificate renewal request to be made before the certificate expires and retains the old key and certificate until the new certificate is available.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Automatic Certificate Enrollment</a></li> <li>• <a href="#">Configuring Certificate Enrollment or Autoenrollment</a></li> <li>• <a href="#">Configuring Manual Certificate Enrollment</a></li> </ul> <p>The following commands were introduced or modified by this feature: <b>auto-enroll, regenerate</b></p>                                                                                                   |
| Manual Certificate Enrollment (TFTP Cut-and-Paste) | 12.2(13)T                               | <p>This feature allows users to generate a certificate request and accept CA certificates as well as the router's certificates via a TFTP server or manual cut-and-paste operations.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Supported Certificate Enrollment Methods</a></li> <li>• <a href="#">Configuring Manual Certificate Enrollment</a></li> </ul> <p>The following commands were introduced or modified by this feature: <b>crypto ca import, enrollment, enrollment terminal</b></p>                                                                                                                                             |
| Multiple-Tier CA Hierarchy <sup>1</sup>            | 12.2(15)T                               | <p>This enhancement enables users to set up a PKI in a hierarchical framework to support multiple CAs. Within a hierarchical PKI, all enrolled peers can validate the certificate of one another as long as the peers share a trusted root CA certificate or a common subordinate CA.</p> <p>The following section provides information about this enhancement:</p> <ul style="list-style-type: none"> <li>• <a href="#">Hierarchical PKI: Multiple CAs</a></li> </ul>                                                                                                                                                                                                                                                           |
| Persistent Self-Signed Certificates                | 12.2(33)SXH<br>12.2(33)SRA<br>12.3(14)T | <p>This feature allows the HTTPS server to generate and save a self-signed certificate in the router startup configuration. Thus, future SSL handshakes between the client and the HTTPS server can use the same self-signed certificate without user intervention.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Supported Certificate Enrollment Methods</a></li> <li>• <a href="#">Configuring a Persistent Self-Signed Certificate for Enrollment via SSL</a></li> </ul> <p>The following commands were introduced or modified by this feature: <b>enrollment selfsigned, show crypto pki certificates, show crypto pki trustpoints</b></p> |

**Table 1** *Feature Information for PKI Certificate Enrollment (continued)*

| Feature Name                                           | Releases                 | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PKI Status <sup>1</sup>                                | 12.3(11)T                | <p>This enhancement added the <b>status</b> keyword to the <b>show crypto pki trustpoints</b> command, which allows you to view the current status of the trustpoint. Prior to this enhancement, you had to issue the <b>show crypto pki certificates</b> and the <b>show crypto pki timers</b> commands for the current status.</p> <p>The following section provides information about this enhancement:</p> <ul style="list-style-type: none"> <li>• <a href="#">How to Configure Certificate Enrollment for a PKI</a></li> </ul> |
| Reenroll Using Existing Certificates                   | 12.3(11)T                | <p>This feature allows users to reenroll a router with a Cisco IOS CA via existing certificates from a third-party vendor CA.</p> <p>The following section provides information about this enhancement:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuring a Certificate Enrollment Profile for Enrollment or Reenrollment</a></li> </ul> <p>The following commands were introduced by this feature:<br/><b>enrollment credential, grant auto trustpoint</b></p>                                                   |
| Trustpoint CLI                                         | 12.2(8)T                 | This feature introduces the <b>crypto pki trustpoint</b> command, which adds support for trustpoint CAs.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Certificate - Auto Enrollment                          | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Certificate - Enrollment Enhancements                  | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Direct http enroll with CA servers                     | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Key Rollover for Certificate Renewal                   | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Manual certificate enrollment (TFTP and cut-and-paste) | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Manual Certificate Enrollment via TFTP                 | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Persistent Self-Signed Certificates                    | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Re-Enroll Using Existing Certificate                   | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

1. This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator.



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





# Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI

---

**First Published: May 2, 2005**

**Last Updated: July 11, 2008**

This module describes how to use Secure Device Provisioning (SDP) in a public key infrastructure (PKI). SDP is a web-based certificate enrollment interface that can be used to easily deploy PKI between two end devices, such as a Cisco IOS client and a Cisco IOS certificate server. The end devices may or may not be directly connected to the network at the time of deployment or provisioning. SDP provides a solution for users deploying a large number of peer devices (including certificates and configurations).

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for SDP in a PKI” section on page 46](#).

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for Setting Up SDP, page 2](#)
- [Information About Setting Up SDP for Enrollment in a PKI, page 2](#)
- [How to Set Up SDP for a PKI, page 21](#)
- [Configuration Examples for Setting Up a PKI via SDP, page 33](#)
- [Additional References, page 45](#)
- [Feature Information for SDP in a PKI, page 46](#)



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

# Prerequisites for Setting Up SDP

## Setting Up SDP for Enrollment in a PKI

Before you set up SDP, your environment should meet the following requirements:

- The petitioner device and the server must have IP connectivity between each other.
- The introducer must have a web browser that supports JavaScript.
- The introducer must have enable privileges on the client device.
- A Cisco IOS Release 12.3(8)T PKI-enabled image or a later image.

## Setting Up SDP for Enrollment in a PKI Using USB Tokens

To leverage USB tokens to provision devices with SDP, your environment should meet the following requirements:

- Both the petitioner device and the server must have IP connectivity between each other.
- The introducer must have a web browser that supports JavaScript.
- The introducer must have enable privileges on the client device.
- The introducer must have access to a petitioner device.
- The introducer must have access to the USB token and PIN, if configured.
- A Cisco IOS Release 12.4(15)T PKI-enabled image or a later image.



### Note

Cisco IOS Release 12.4(15)T or a later release provides the flexibility to move credentials stored on the USB token. However, the device used to configure the USB token may run any Cisco IOS Release 12.3(14)T PKI-enabled image or a later image.

## Using SDP to Configure a Device for an Internet Connection Through a Service Provider

To leverage SDP to configure a device that is not connected to the Internet, your environment should meet the following requirements:

- The introducer must have a web browser that supports JavaScript.
- The introducer must have enable privileges on the client device.
- A Cisco router that supports a DHCP client and a PPPoE client and has a configured LAN or WAN interface.
- A Cisco IOS Release 12.4(20)T PKI-enabled image or a later image. If a previous Cisco IOS release is used on one of the devices, the SDP functionality will default to the earlier Cisco IOS version.

# Information About Setting Up SDP for Enrollment in a PKI

Before using SDP for certificate enrollment, you should understand the following concepts:

- [SDP Overview, page 3](#)
- [How SDP Works, page 4](#)
- [SDP Leveraging USB Tokens, page 10](#)

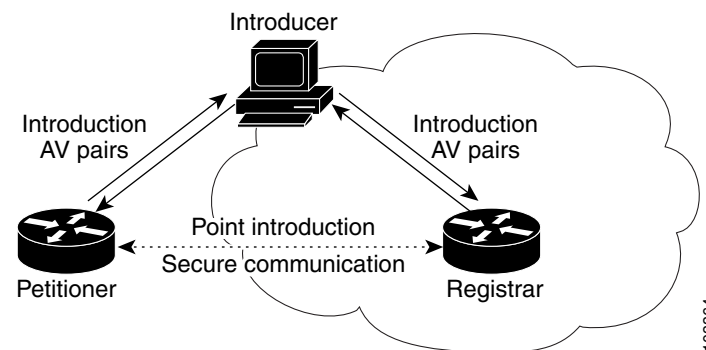
- [How SDP Uses an External AAA Database, page 13](#)
- [How Custom Templates Work with SDP, page 15](#)

## SDP Overview

SDP (also referred to as Trusted Transitive Introduction [TTI]) is a communication protocol that provides a bidirectional introduction between two end entities, such as a new network device and a Virtual Private Network (VPN). SDP involves the following three entities (see [Figure 1](#)):

- **Introducer**—A mutually trusted device that introduces the petitioner to the registrar. The introducer can be a device user, such as a system administrator.
  - An introducer can be configured as an administrative introducer, which allows an administrator performing the introduction to supply the name for the device being introduced. The supplied device name is used as if it were the name of an introducer in the normal SDP mechanisms, preserving the existing functionality of the SDP configuration. For more information on function of the administrative introducer, see the section “[Authentication and Authorization Lists for an Administrative Introducer.](#)”
- **Petitioner**—A client, or new device, to be introduced to the secure network.
- **Registrar**—A server that authorizes the petitioner. The registrar can be a certificate server.

**Figure 1** *Post-Introduction Secure Communication*



As of Cisco IOS Release 12.4(20)T or a later release, the introducer can start the SDP process without establishing prior Internet connectivity on the petitioner. The use of the prep-connect phase and the connect phase provides the ability to configure a petitioner for Internet connectivity through a service provider. For more information on the prep-connect phase and the connect phase, see the section “[How SDP Works.](#)”

The registrar communicates directly with an external authentication, authorization, and accounting (AAA) server to verify petitioner credentials, permit or deny enrollment, and retrieve specific petitioner configuration information. The petitioner and registrar serve web pages to the introducer, the end user. The petitioner receives the bootstrap configuration from a remote management system via the introducer’s web browser.

SDP is implemented over a web browser with six possible phases—prep-connect (optional), connect, start (optional), welcome, introduction, and completion. Each phase is shown to the user via a web page. For more information on each phase, see the section “[How SDP Works.](#)”

## How SDP Works

The following sections describe how SDP deploys PKI between two devices:

- [SDP Prep-Connect Phase](#)
- [SDP Connect Phase](#)
- [SDP Start Phase](#)
- [SDP Welcome Phase](#)
- [SDP Introduction Phase](#)
- [SDP Completion Phase](#)

The SDP process starts with one of three entry pages being loaded into the web browser by the introducer: the SDP prep-connect phase received from the administrator; the start phase loaded from the registrar; or the welcome phase loaded from the petitioner.

The sample figures show how to introduce the local device (the petitioner) to the secure domain of the registrar. The “introducer” is referred to as the end user.

### SDP Prep-Connect Phase

The prep-connect page is optional. Without the prep-connect page, the petitioner must have IP connectivity established.

The administrator must configure the prep-connect template and send the prep-connect page to the introducer. For more information on configuring the prep-connect template, see the section “[Default Prep-Connect Template](#).”

The administrator must also obtain and communicate the username and password for the secure network to the introducer by a telephone call, an e-mail, a secure e-mail, a CD, or a USB token. The registrar may be configured to authenticate the introducer using an existing AAA infrastructure (for example, an existing username and password database that is part of the existing corporate domain). The SDP prep-connect phase supports a one time password mechanism as is used by common AAA infrastructures. For more information on SDP and AAA, see the section “[How SDP Uses an External AAA Database](#).”

After receiving the prep-connect page, the introducer must load the page onto the computer where the HTTP browser will run. The introducer then loads the prep-connect page into the HTTP browser as a local file and then the prep-connect page is displayed (see [Figure 2](#)).

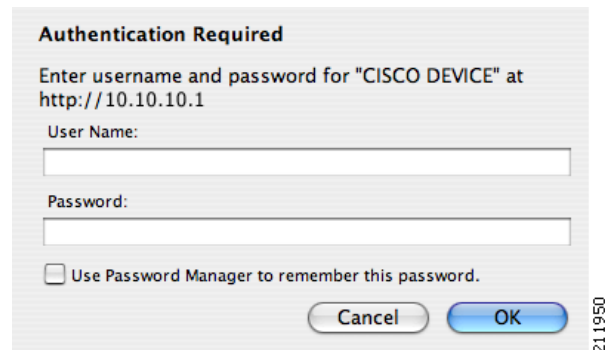
**Figure 2**      **Sample SDP Prep-Connect Page**





After the introducer clicks the Log onto Cisco Device button, the login dialog box is displayed (see [Figure 3](#)). The introducer enters the factory default username (cisco) and password (cisco) of the Cisco device.

**Figure 3** *Sample Petitioner Login Dialog Box*



The introducer authenticates with the petitioner and then Internet connectivity is tested by attempting to access a known URL. Access to [www.cisco.com](http://www.cisco.com) (198.133.219.25) is tested by default. The administrator can modify the URL to be used for testing connectivity by modifying the default prep-connect template. For more information about modifying the default test URL and other fields that the administrator may configure for the prep-connect page, see the section [“Default Prep-Connect Template.”](#)



**Note**

To mitigate the possibility that the prep-connect page could be modified to contain an IP address of an untrusted registrar or that a prep-connect page might be e-mailed from an untrusted source, use a secure method, such as secure e-mail, to send the prep-connect page.

If Internet connectivity is established either the start page or welcome page is displayed, depending on the prep-connect template setting as defined by the administrator. If Internet connectivity is not established, the connect page is displayed.

## SDP Connect Phase

The connect page is displayed only if the prep-connect page is used and there is no IP connectivity for the petitioner at the completion of the prep-connect phase. The connect page has three IP address assignment methods to allow flexibility for your Cisco IOS platform: Dynamic Host Configuration Protocol (DHCP), Point to Point Protocol over Ethernet (PPPoE), or static IP address assignment.



**Note**

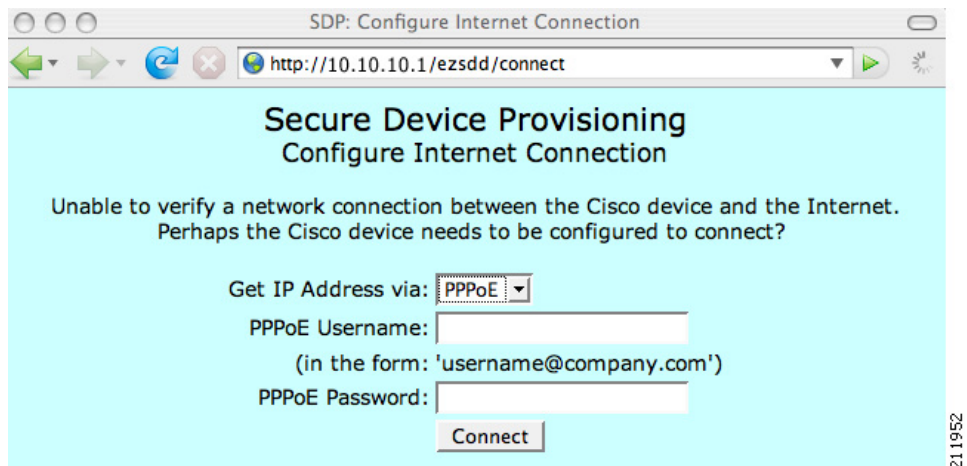
SDP functionality is not used with the Cisco IOS configuration to establish Internet connectivity. SDP functionality includes a signature on the Cisco IOS configuration, guaranteeing that the values have not changed in transit.

### DHCP IP Address Assignment Method

If the introducer chooses DHCP, the default method, for the IP address assignment method option (see [Figure 4](#)), clicking the Connect button causes the petitioner to be configured for Internet connectivity.

**Figure 4** *Sample Connect Page for DHCP IP Address Assignment Method***PPPoE IP Address Assignment Method**

If the introducer chooses PPPoE, input fields for PPPoE username and password are displayed (see [Figure 5](#)). The introducer must enter the username and password as supplied by the Internet service provider (ISP) and then click the Connect button, which causes petitioner to be configured for Internet connectivity.

**Figure 5** *Sample Connect Page for PPPoE IP Address Assignment Method***Static IP Address Assignment Method**

If the introducer chooses static, input fields for the IP address, netmask, and the default gateway are displayed (see [Figure 6](#)). The introducer must enter the configuration values as supplied by the ISP and then click the Connect button, which causes petitioner to be configured for Internet connectivity.

**Figure 6** *Connect Page for Static IP Address Assignment Method*

#### Connect Page IP Address Configuration

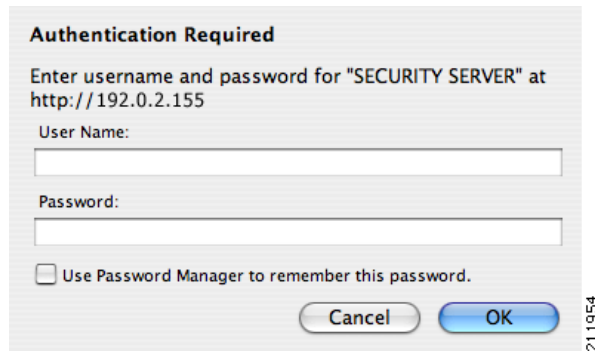
After IP address configuration, Internet connectivity is tested again by attempting to access a known URL configured by the administrator in the prep-connect template ([www.cisco.com](http://www.cisco.com) by default). If Internet connectivity is now established either the start page or welcome page is displayed, depending on the prep-connect template setting as defined by the administrator. If Internet connectivity is not established, the introducer should verify the settings entered or contact their administrator.

## SDP Start Phase

The start page is optional. Without the start page, during the SDP exchange, the user clicks the Next button on the welcome page and is sent to the registrar's introduction page. Because the user has not previously connected to the registrar, the user is required to log in to the registrar using available credentials (per the registrar configuration). Some browsers fail to reconnect to the registrar after the user credentials are requested (after the user has entered the login data). As of Cisco IOS Release 12.4(4)T, users may configure their browsers to begin the SDP exchange by contacting the registrar's introduction URL via a start page. Thereafter, the registrar can direct the user to the welcome page, which is on the petitioner device. The SDP transaction will then continue through the welcome, introduction, and completion phases as described in this document.

To begin the SDP transaction from the registrar, the user must configure the browser via the **template http start** command; otherwise, the SDP transaction must begin from the welcome page on the petitioner. For more information on how to configure a custom template, see the section "[How Custom Templates Work with SDP](#)."

Before the welcome page is displayed, the user must direct his or her browser to the start page via the URL <http://registrar/ezsdd/intro>. A login dialog box is then displayed, and the end user can log into the registrar via a username and password supplied by the administrator to access the secure network (see [Figure 7](#)).

**Figure 7** Registrar Remote Login Dialog Box

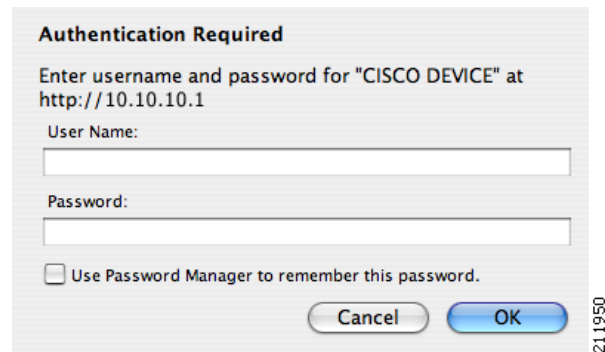
After entering a valid username and password, the start page is displayed (see [Figure 8](#)).

**Figure 8** Sample SDP Start Page

After entering the URL of the petitioner's welcome page (for example, <http://10.10.10.1/ezsdd/welcome>) and clicking the Next button on the start web page, the end user enters the SDP welcome phase and logs into his or her petitioner as shown in [Figure 9](#).

## SDP Welcome Phase

The welcome phase begins when the user clicks the Next button on the start page. Before the welcome page is displayed, the user must log into the petitioner via the URL “<http://10.10.10.1/ezsdd/welcome>.” The local login dialog box is then displayed (see [Figure 9](#)). The end user can then log into the local device via the factory default username (cisco) and password (cisco).

**Figure 9**      **Petitioner Local Login Dialog Box**

After the password is successfully entered, the welcome web page is displayed (see [Figure 10](#)), which is served by the petitioner.

**Figure 10**      **Sample SDP Welcome Page**

After entering the URL of the registrar (for example, <http://192.0.2.155/ezsdd/intro>) and clicking the Next button on the welcome web page, the SDP introduction phase begins and the introduction page, which is served by the registrar, is displayed.

## SDP Introduction Phase

Before the introduction page is displayed, the end user must log into the registrar if the user has not already done so from the start page (see [“SDP Start Phase”](#)), which utilizes the external AAA database.

With an external AAA database, the introducer can use an account on the database to perform the introduction without requiring knowledge of the enable password of the registrar. Without an external AAA database, the introducer may use the enable password of the registrar for authentication.



### Note

Using the enable password of the registrar exposes the password to end users; therefore, it is recommended that the enable password be used for administrative testing only.

The administrative introducer is identified by the HTTP authentication for the introduction page (or the start page), with the AAA database query returning administrative privilege for the user. If the introducer has administrator privilege, the device name is that which was entered in the administrative introduction page. If the introducer does not have administrative privileges, the device name is the introducer name. The existing device certificate is the current certificate on the petitioner, which may be the

manufacturing identification certificate (MIC). This certificate may or may not exist. For more information on the function of the external AAA database, see the section “[How SDP Uses an External AAA Database](#).”

After the end user successfully enters his or her password, the introduction web page is displayed (see [Figure 11](#)).

**Figure 11** *Sample SDP Introduction Page*



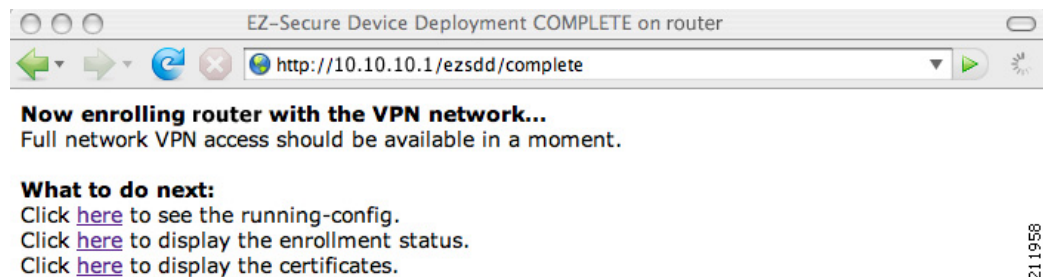
At this point, the registrar passes device information to the external management system to obtain a bootstrap configuration file. For more information on options available to identify a customized bootstrap configuration file, see the section “[Custom HTML Template Expansion Rules](#).”

After the end user clicks the Next button on the introduction page, the end user enters the completion phase and automatically returns to his or her local device.

## SDP Completion Phase

Now that the end user has enrolled the petitioner with the registrar, the petitioner will serve the completion page (see [Figure 12](#)).

**Figure 12** *Sample SDP Completion Page*



The SDP exchange is now complete. The petitioner has received configuration information from the registrar and should receive a certificate from the registrar shortly.

## SDP Leveraging USB Tokens

SDP provides for highly scalable deployments and streamlines the deployment of an individual device or multiple devices. USB tokens provide for secure storage and configuration distribution.

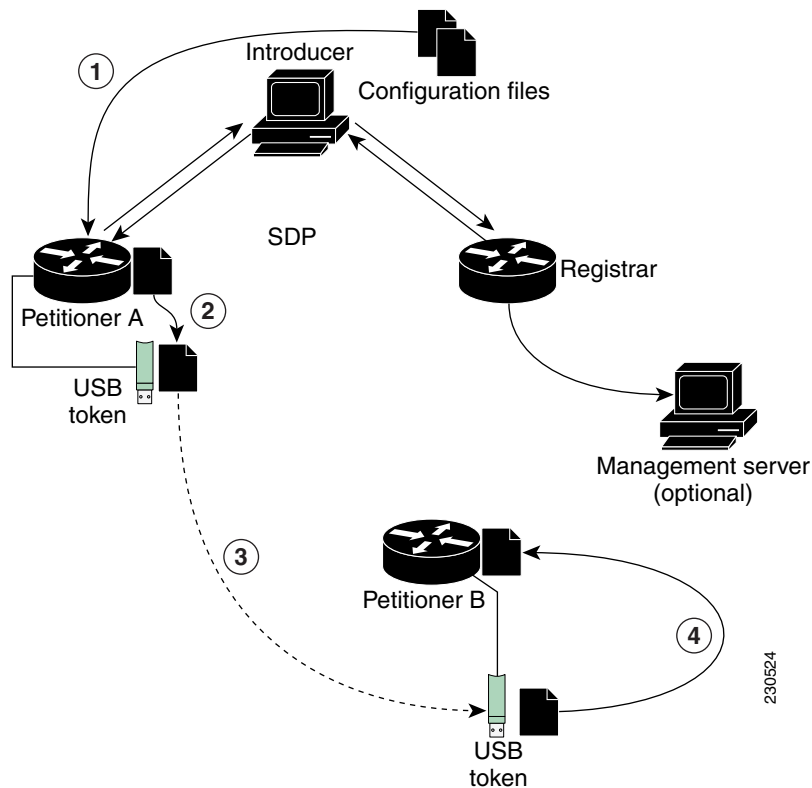
As of Cisco IOS Release 12.4(15)T or a later release, USB tokens may be utilized to transfer PKI credentials using SDP to a remote device, and SDP may be used to configure the USB token. The USB token may then be used to provision a device at the same location, or the USB token may be transported to another location where it may be used to provision a remote device. For more information about configuring and using USB tokens, see the “[Related Documents](#)” section.

An example SDP deployment using a USB token to transfer PKI credentials is shown in [Figure 13](#). The required devices include the USB token and the SDP entities required to provision a device. These SDP entities are the introducer, the registrar, a petitioner at the local location, Petitioner A, and a petitioner at the remote location, Petitioner B. Optionally, a management server may be used.


**Note**

An optional configuration would be to configure one device as both the registrar and a petitioner, which may be beneficial when the USB token is transported to a remote location. The remote location would not require a separate petitioner device.

**Figure 13** Example SDP Environment Using USB Tokens to Transfer Credentials



230524

## Use of SDP to Configure the USB Token

Prior to initiating an SDP introduction a USB token is inserted into the petitioner device. In the example configuration shown in [Figure 13](#), the USB token would be inserted into Petitioner A. The petitioner may be configured to ignore any existing information on the USB token. As in regular SDP operations, for a scalable configuration of USB tokens, an initial template configuration has to be prepared and placed onto each SDP device with appropriate target configuration information.



Files used to provision a device are moved in the following sequence, shown by the numbered arrows in [Figure 13](#).

1. One petitioner, Petitioner A, is at the local location. petitioner A engages directly with the SDP exchange to perform the initial configuration of the USB token. Files used to configure the USB token, binary files and template files, are retrieved from the registrar and moved to Petitioner A. The URL for the binary file location is expanded on the registrar. Binary files are not processed through the template expansion functions. The template expansion occurs on the registrar for both the source URL and destination URL. By default, binary files and template files will be retrieved from and stored to NVRAM on the registrar and petitioner respectively. The binary file location on the registrar and the destination binary file location on Petitioner A may be specified with the **binary file** command. The template file location on the registrar and the destination template file location on Petitioner A may be specified with the **template file** command.
2. The RSA keys and certificate chain information are moved from Petitioner A to the USB token.
3. The USB token is transported to the remote location where it is inserted into Petitioner B.
4. The configuration files on the USB token are used to provision the local device. Files from the USB token may be moved to a storage location on Petitioner B with the **crypto key move rsa** command.

## SDP Phases with a USB Token

The same SDP phase concepts introduced in the “[SDP Overview](#)” section are used, with the following distinctions in the SDP welcome phase, the SDP introduction phase, and the SDP completion phase.

### SDP Welcome Phase with a USB Token

The SDP welcome phase begins as usual, when an introduction is initiated by connecting to the welcome user interface. If there is an existing certificate on the USB token, it will be used for signing the SDP exchange. Instead of a local RSA key pair, a new RSA key pair on the token is used.



#### Note

The RSA key pair generation may take a substantial length of time, anywhere from 5 to 10 minutes if the key is generated on the token. The length of time is dependent on hardware key generation routines available on the USB token. An informative web page will be presented to the introducer, indicating that RSA key pair generation is occurring.

The new key pair generated by Petitioner A is added to the USB token without removing any existing RSA key pairs. SDP AV pairs indicate both that a token is being used and if there is any token secondary configuration information. If an optional management server is in use, the AV pair information is used to determine if any special configuration commands are needed.

### SDP Introduction Phase with a USB Token

The SDP Introduction phase begins with AV pairs being transferred to the registrar. When the registrar detects USB token related AV pairs, the registrar, if previously configured, may prepare configuration information destined for the USB token. Currently configuration commands are sent as a specific configuration files that are subsequently merged with the running configuration.

The administrator can leverage normal SDP configuration commands to configure the USB token. USB token information that should be configured includes the certificate, the bootstrap configuration, and the PIN number configuration.



### **SDP Completion Phase with a USB Token**

At the beginning of the completion phase, the introduction proceeds with AV pairs being transferred to the petitioner (in [Figure 13](#), this would be Petitioner A). The various files are stored in the specified file system locations and then the existing configuration file processing proceeds. This ordering allows the configuration to take advantage of the new files that have been transferred.

## **Use of the Configured USB Token**

After the USB token is configured by Petitioner A, it is transported from its current location to the remote location, where the second petitioner, Petitioner B is located. The USB token is inserted into the target device, Petitioner B, which then inherits the USB token configuration and cryptographic material from the USB token. The end user at the remote location must have the PIN number on the USB token. The PIN number is either the default factory PIN or the PIN number the administrator configured during the introduction phase.

## **How SDP Uses an External AAA Database**

The external AAA database is accessed twice during the SDP exchange. The first time the AAA database is accessed the introducer is authenticated; that is, when the registrar receives an introduction request via the secure HTTP (HTTPS) server, the registrar does an AAA lookup based on the introducer's username and password to authorize the request. The second time the AAA database is accessed authorization information is obtained and applied to the configuration and certificates that are issued to the petitioner device; that is, the registrar checks the integrity of the request by verifying the request signature using the petitioner-signing certificate. The certificate subject name may be specified in the AAA database, and up to nine configuration template variables may be specified and expanded into the template configuration.

### **Use of a Self-Signed Certificate Versus a Certificate Issued by Another CA Server**

By default, the SDP exchange results in only one certificate being issued to the petitioner device. Although just one certificate is issued, the introducer is not restricted from introducing multiple devices and thus obtaining multiple certificates. By specifying the subject name in the certificate that is issued, you can be assured that all certificates that are issued in this way are associated with the introducer. You can use PKI AAA integration to further restrict the use of these certificates. Additionally, the AAA database can be configured to accept only one authentication and authorization request per user.

Because the petitioner certificate is self-signed, it is just used to convey the public key of the petitioner. No verification or authorization check is performed on the certificate; thus, authorization is per-user based and no per-device information is used.

There are some scenarios when per-device authorization is preferred. Therefore, if the petitioner is able to use certificates issued by other certification authority (CA) servers for SDP transactions, the existing PKI can be used and authorization can be achieved over the certificate attributes.

Configuring the petitioner and the registrar for certificate-based authorization provides authorization of the specific device being deployed. Previously, introducer-to-petitioner device communication was secured only using physical security between the introducer and the petitioner device. SDP certificate-based authorization gives the registrar an opportunity to validate the current device identity before accepting the introduction.

## Authentication and Authorization Lists for SDP

When you are configuring your SDP registrar, if you specify an authentication list and an authorization list, the registrar uses the specified lists for all introducer requests. The authentication list is used when authenticating the introducer (the AAA server checks for a valid account by looking at the username and password). The authorization list is used to receive the appropriate authorized fields for the certificate subject name and a list of template variables to be expanded into the Cisco IOS command-line interface (CLI) snippet that is sent back to the petitioner. The authentication and authorization lists will usually point to the same AAA server list, but it is possible to use a different database for authentication and authorization. (Storing files on different databases is not recommended.)

When a petitioner makes an introduction request, multiple queries are sent to the AAA list database on the RADIUS or TACACS+ server. The queries search for entries of the following form:

```
user Password <userpassword>
 cisco-avpair="ttdi:subjectname=<<DN subjectname>>"
 cisco-avpair="ttdi:iosconfig#<<value>>"
 cisco-avpair="ttdi:iosconfig#<<value>>"
 cisco-avpair="ttdi:iosconfig#=<<value>>"
```



### Note

The existence of a valid AAA username record is enough to pass the authentication check. The “cisco-avpair=tdi” information is necessary only for the authorization check.

If a subject name was received in the authorization response, the SDP registrar stores it in the enrollment database, and that “subjectname” overrides the subject name that is supplied in the subsequent certificate request (PKCS10) from the petitioner device.

The numbered “tdi:iosconfig” values are expanded into the SDP Cisco IOS snippet that is sent to the petitioner. The configurations replace any numbered (\$1 through \$9) template variable. Because the default Cisco IOS snippet template does not include the variables \$1 through \$9, these variables are ignored unless you configure an external Cisco IOS snippet template. To specify an external configuration, use the **template config** command. For more information on external configurations, see the section [“Custom Configuration and File Template Variable Expansion Rules at the Petitioner.”](#)



### Note

The template configuration location may include a variable “\$n,” which is expanded to the name with which the user is logged in.

## Authentication and Authorization Lists for an Administrative Introducer

The SDP mechanisms assume a permanent relationship between the introducer and the device. As a result, the introducer username is used to define the device name.

In some SDP deployment scenarios, the introducer is an administrator doing the introduction for many devices. However, using the introducer (the administrator) name to define the device name results in multiple devices being incorrectly deployed with the same device name. Instead, an administrative introducer allows the administrator to specify the correct device name during the introduction.

More generally stated, the introducer username is used as the database record locator to determine all other information about the device including the Cisco IOS configuration template, various template variables (pulled from an AAA database and expanded into the template), and the appropriate subject name for PKI certificates issued to the device. For simplicity, this database record locator is called the user/device name.

The administrative introducer provides a device name. In that way, an administrator can provide the appropriate record locator when doing an introduction. For example, if an administrator is trying to introduce a device for username “user1,” the administrator introduces the device into the PKI network and provides user1 as the record locator after logging into the registrar using the administrator’s own credentials. The record locator, user1, becomes the device name. All other template and PKI certificate subject name information specific to the introduction is then provided by the user1 username records instead of by the administrator’s record.

The registrar device uses the supplied username information with a user introducer name. The username allows the existing mechanisms for determining a user’s authorization, template, and PKI certificate information to be supported without modification.

## How Custom Templates Work with SDP

You may use custom templates to streamline the SDP process.

- Custom templates allow you to complete the web pages with the required start information, so the introducer is no longer required to contact the registrar and can immediately begin the SDP transaction.
- Custom templates allow customized deployment information to be displayed on the web pages, thereby tailoring the user experience.

An easy way to define a custom template is to modify the default template. Without custom templates, the introducer must contact the registrar for information to begin the SDP transaction. For a list of the default templates, see the section “[Default Templates for SDP Transaction Web Pages](#).”



### Note

It is recommended that only advanced SDP users configure custom templates because problems can result from modifying templates incorrectly before the templates are displayed in the introducer’s browser.

## Custom Template Variable Expansion

There are expansion variables in the templates that are replaced by the Cisco IOS SDP registrar or petitioner. These variables are expanded as follows:

- \$\$—“\$”
- \$a—attribute-value (AV) pairs
- \$c—Trusted certificate
- \$d—Dump AV pairs in browser
- \$h—Hostname
- \$k—Keylabel or “tti”
- \$l—Trustpoint label = “tti”
- \$n—HTTP client’s username
- \$s—Default TTI key size
- \$t—Trustpoint configuration
- \$u—Completion URL
- \$1 to \$9—Variables retrieved from AAA server during user authentication

## Custom Template Variable Expansion Rules

Configuration and templates are used during an SDP exchange. Prior to use and after distribution, these templates are expanded using the following rules based in the SDP communication stage.

### Custom HTML Template Expansion Rules

HTML templates are expanded immediately before being served to the HTTP client. The HTTP templates are expanded as follows:

- \$u—Completion url, which is be populated with the SDP completion URL (for example: `http://10.10.10.1/ezsdd/completion`). This variable is used internally by SDP as the internal “wizard” state. It is expected that the SDP introduction page include something similar to the following text: “<FORM action=“\$u”method=“post”>” for normal wizard processing.
- \$n—introducer name or the device name entered by the administrative introducer.
- \$\$—\$
- \$h—Hostname
- \$a—All AV pairs with or without a specified template character will be written out in the following HTML form format. (Because these AV pairs are not “INPUT type=hidden,” they are directly displayed on the web page for debugging templates or the SDP process.)

```
<INPUT type=hidden NAME=“attribute string here”
```

```
value=“variable string here”>

```

all HTML templates should have this!

```
$d = dump all av pairs in: attribute = value

```

### URL Template Expansion Rules

There are URLs for the configuration template source, the file template source, and the file destination. These variables are expanded when the registrar prepares the URL, just before retrieving the configuration or file. For the file destination, these variables are expanded just before the petitioner copies the file to the file destination.

- \$\$—\$
- \$h—Hostname

### Custom Configuration and File Template Variable Expansion Rules

Custom configuration and file template variables are expanded both when the registrar prepares the configuration or file template and when the petitioner receives the configuration or file template.

#### Custom Configuration and File Template Variable Expansion Rules at the Registrar

When the registrar expands the configuration or file template, the following variables are used by the Cisco IOS CA. These variables are expanded before being sent through the SDP wizard.

- \$\$—\$
- \$h—Hostname
- \$t—A simple default trustpoint configuration that includes \$l, \$k, and \$s to be expanded at the client
- \$1 to \$9—Variables retrieved from AAA server during user authentication (not applicable to the file template)

### Custom Configuration and File Template Variable Expansion Rules at the Petitioner

When the petitioner expands the configuration or file template, the following variables are expanded:

- \$\$—\$
- \$h—Hostname
- \$k—Keylabel
- \$l—Trustpoint label
- \$s—Key size
- \$c—Expanded to certificate chain
- \$n—Expanded to username (not applicable to the file template)

### Custom Configuration HTTP Template Variable Expansion Rules

Custom configuration HTTP templates provide flexibility for backend Common Gateway Interface (CGI) scripts and integration with external management systems. Template URLs run through the HTTP template expansions before registrar retrieves the bootstrap configuration from the external management system. The device name (\$n) is expanded into the URL and passed to the external management system so that a specific bootstrap configuration file can be located based on the device information.



#### Note

You should only modify the HTML text that is displayed. The existing expansion variables, Javascript, and forms in the default templates should not be removed when customizing the templates. They are required for SDP to function properly.

The HTTP template expansion and **template config** command allow you to specify either of the following file types to obtain a customized bootstrap configuration file:

- A configuration file based on the device name (for example, template config  
http://myserver/\$n-config-file.conf)
- A CGI script based on the device name (for example, template config  
http://myserver/cgi-bin/mysdpcgi post)

As of Cisco IOS Release 12.4(6)T, the CGI support has been expanded so that the bootstrap configuration can be identified by not only the device name, but also the type, current Cisco IOS version information, and current configuration. This functionality expands the **template config** command with the **post** keyword, which tells the registrar to send this additional device information to the external management system via a CGI script with the HTTP or HTTPS protocol only.

The registrar passes the device information via AV pairs (\$a) to the external management system. Using the AV pair information, the management system identifies the appropriate bootstrap configuration files and sends it back to the registrar. The additional AV pairs that are sent with the expanded CGI support for identification of customized bootstrap configuration file are shown in [Table 1](#).

**Table 1** AV Pairs Sent During HTTP Post to External Management System

| AV Pair             | Description                                                                                               |
|---------------------|-----------------------------------------------------------------------------------------------------------|
| TTIFixSubjectName   | AAA_AT_TTI_SUBJECTNAME (sent only if the realm authentication user is not the root user on the registrar) |
| TTIIosRunningConfig | Output of <b>show running-config brief</b>                                                                |
| TTIKeyHash          | Digest calculated over the device public key                                                              |

**Table 1** *AV Pairs Sent During HTTP Post to External Management System (continued)*

| AV Pair        | Description                                                                                                                                                                                                                                    |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TTIPrivilege   | AAA_AT_TTI_PRIVILEGE—"admin" is sent if the user is an administrator, "user" is sent if the user is not an administrator (sent only if the realm authentication user is an administrator and the information is available from the AAA server) |
| TTISignature   | Digest calculated over all AV pairs except UserDeviceName and TTISignCert                                                                                                                                                                      |
| TTISignCert    | Device current certificate (sent only if the device currently has a certificate)                                                                                                                                                               |
| TTITemplateVar | AAA_AT_TTI_IOSCONFIG(1-9) (sent only if the realm authentication user is not the root user on the registrar)                                                                                                                                   |
| TTIUserName    | Device name                                                                                                                                                                                                                                    |
| TTIVersion     | TTI version of the registrar                                                                                                                                                                                                                   |
| UserDeviceName | Device name as entered by the administrative introducer (sent only if the realm authentication user is an administrator)                                                                                                                       |

**Note**

The registrar must be running Cisco IOS Release 12.4(6)T, the **template config** command must be issued with the **post** keyword, and the *url* argument must include either HTTP or HTTPS. No other protocol is supported for the expanded CGI template functionality (for example, FTP).

## Default Templates for SDP Transaction Web Pages

The following default templates exist for each SDP transaction web page:

- [Default Prep-Connect Template](#)
- [Default Start Page Template](#)
- [Default Welcome Page Template](#)
- [Default Introduction Page Template](#)
- [Default Admin-Introduction Page Template](#)
- [Default Completion Page Template](#)

### Default Prep-Connect Template

The prep-connect template may be modified by the administrator to contain values that are appropriate for their environment. The format of the prep-connect page may also be modified by the settings contained in the template.

Except for the registrar IP address, which the administrator must customize, the prep-connect template may be used as shown below.

```
<html><head><title>
SDP: Test Internet Connection</title></head>
<noscript>
If you see this message, your browser is not running JavaScript,

which is required by Cisco Secure Device Provisioning.

If you cannot enable JavaScript, please contact your system administrator.

</noscript>
<body style="background-color: rgb(204, 255, 255);">
```

```

<div style="text-align: center;"><big><big>
Secure Device Provisioning</big>

Test Internet Connection</big>

<form action="http://10.10.10.1/ezsdd/connect" method="post">
<input type="submit" value="Log onto Cisco Device">

Default username/password is cisco/cisco.
<input type="hidden" name="TTIAfterConnectURL"
value="http://10.10.10.1/ezsdd/welcome">
<!-- Note, that for the below, 198.133.219.25 = www.cisco.com. -->
<input type="hidden" name="TTIConnectTestURL" value="http://198.133.219.25">
<input type="hidden" name="TTIInsideAddr" value="10.10.10.1">
<input type="hidden" name="TTIlanport" value="Vlan1">
<input type="hidden" name="TTIwanport" value="FastEthernet4">
</form></div></body></html>

```

### Hidden HTML Form Fields

The hidden HTML form fields communicate initial configuration information to the browser as set by the administrator and are not signed.



#### Note

The term “hidden” refers to the fact that these HTML form fields are not displayed on the prep-connect page to reduce potential confusion to the introducer.

The administrator can set hidden HTML form fields in the prep-connect template as shown in [Table 2](#).

**Table 2 Administrator Defined AV Pairs Sent During Prep-Connect Phase**

AV Pair	Description
TTIAfterConnectURL	The administrator may set the TTIAfterConnectURL field to either the welcome page URL or the start page URL. The welcome page URL is specified with the factory default petitioner IP address. The connect after URL may be any valid URL if SDP is not going to be used after establishing Internet connectivity.
TTIConnectTestURL	The administrator may set the TTIConnectTestURL field to a valid URL that should be accessible when Internet connectivity is established. The default prep-connect template value is www.cisco.com (198.133.219.25).
TTIInsideAddr	The administrator may set the TTIInsideAddr field to the factory default IP address of the petitioner. For the Cisco 871 ISR, the IP address is 10.10.10.1.
TTIlanportx	The administrator may set the TTIlanportx field to the LAN interface name of the petitioner platform. This field is used to apply the Cisco IOS connect configuration. For the Cisco 871, the field value is “Vlan1.”
TTIwanport	The administrator may set the TTIwanport field to the WAN interface name of the petitioner. This field is used to apply the Cisco IOS connect configuration. For the Cisco 871, the field value is “FastEthernet4.”



#### Note

The connect template cannot be customized.

## Default Start Page Template

```
<html><head><title>EZ-Secure Device Deployment Start page on $h</title></head>
<NOSCRIPT>
If you see this message, your browser is not running JavaScript.

Cisco Secure Device Deployment requires JavaScript.
 Please contact
your system administrator.

</NOSCRIPT>
<SCRIPT LANGUAGE="JavaScript">
function submit_to_url(form){
form.action=form.TTIWelcomeURL.value;return true;}</SCRIPT>
Welcome to Cisco Secure Device Deployment Server $h <FORM
action="" method="post" onSubmit="return submit_to_url(this)"> Your
device:
 <INPUT type="text" name="TTIWelcomeURL" size=80
value="">
 <INPUT type="submit" value="Next">

$a</FORM></html>
```

## Default Welcome Page Template

```
<html><head><title>EZ-Secure Device Deployment WELCOME to $h</title></head>
<NOSCRIPT>
If you see this message, your browser is not running JavaScript.

Cisco Secure Device Deployment requires JavaScript.
 Please contact
your system administrator.

</NOSCRIPT>
<SCRIPT LANGUAGE="JavaScript">
function submit_to_url(form){
natURL=location.href.split("/");
localURL=form.TTICompletionURL.value.split("/");
if(natURL[2]!=localURL[2]){
form.TTICompletionURL.value=localURL[0]+"//"+natURL[2]+"/"
+"/"+localURL[3]+
+"/"+localURL[4];}
form.action=form.vpnserviceurl.value;
return true;}</SCRIPT>
Welcome to Cisco Secure Device Deployment for $h <FORM
action="" method="post" onSubmit="return submit_to_url(this)">
To join a Virtual Private Network (VPN) enter the web
 site URL
provided by your network administrator:
 <INPUT type="text"
name="vpnserviceurl" size=80 value="">

<INPUT
type="submit" value="Next">
 $a</FORM></html>
```

## Default Introduction Page Template

```
<html><head><title>EZ-Secure Device Deployment INTRODUCTION to $h</title>
</head>Welcome to the VPN network gateway on $h <FORM
action=""$u" method="post"> Your 'username' and 'password' entered
have been accepted.
 Your device will now be allowed to
automatically join the VPN network.

Press Next to complete
automatic configuration of your VPN Device.

<INPUT
type="submit" value="Next">
 $a</P></FORM></html>
```

## Default Admin-Introduction Page Template

```
<html><head><title>EZ-Secure Device Deployment ADMINISTRATIVE
INTRODUCTION to $h</title></head> <NOSCRIPT> If you see this
message, your browser is not running JavaScript.
 Cisco Secure
Device Deployment requires JavaScript.
 Please contact your system
administrator.

</NOSCRIPT>
<SCRIPT LANGUAGE="JavaScript">
function submit_to_url(form){
form.introadminurl.value=location.href+"/admin";
form.action=form.introadminurl.value;
return true;}</SCRIPT>
```



```
Welcome to the VPN network gateway on $h <FORM action="\\"
method="post\" onSubmit=\"return submit_to_url (this)\"> Your
administrator 'username' and 'password' entered have been
accepted.
 Please provide the name to be associated with this
device:
 <INPUT type=\"text\" name=\"userdevicename\" size=64
value=\"\">

 <INPUT type=\"submit\" value=\"Next>\">
 <INPUT
type=\"hidden\" name=\"introadminurl\" value=\"\">

$a</FORM></html>
```

### Default Completion Page Template

```
<html><head><title>EZ-Secure Device Deployment COMPLETE on $h</title></head>
Now enrolling $h with the VPN network...
 Full network VPN
access should be available in a moment.

 $d
</html>
```

### Default Template for the Configuration File

The default configuration template is shown below. This default configuration file is used if a configuration template is not specified or if the **template config** command is issued *without* the **post** keyword. For more information on using the default configuration template, see the section “[Using a Configuration Template File: Example.](#)”

```
$t
!
$c

!
end
```

## How to Set Up SDP for a PKI

This section contains the following procedures that should be followed when setting up SDP for your PKI. You can configure the registrar according to only one of the registrar configuration tasks.

- [Enabling the SDP Petitioner, page 21](#)
- [Enabling the SDP Registrar and Adding AAA Lists to the Server, page 23](#)
- [Enabling the SDP Registrar for Certificate-Based Authorization, page 27](#)
- [Configuring an Administrative Introducer, page 29](#)
- [Configuring Custom Templates, page 32](#)

### Enabling the SDP Petitioner

Perform this task to enable or disable the petitioner and associate a trustpoint with the SDP exchange.

You can also use this task to configure the petitioner to use a certificate and the Rivest, Shamir, and Adelman (RSA) keys associated with a specific trustpoint.



#### Note

The petitioner is enabled by default on a Cisco device that contains a crypto image; thus, you have only to issue the **crypto provisioning petitioner** command if you have previously disabled the petitioner or if you want to use an existing trustpoint instead of the automatically generated trustpoint.



Note

By default, the SDP petitioner device uses an existing certificate. If multiple certificates and one specific certificate exist, use this task to make a choice. However, this task is not necessary to enable the default behavior.

## Prerequisites

- The HTTP server must be enabled via the **ip http server** command. (The HTTP server is typically enabled by default on many default Cisco IOS configurations.)
- If you are configuring the petitioner to use a certificate and RSA keys, your SDP petitioner device must have an existing manufacturer’s or a third-party certificate.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto provisioning petitioner**
4. **trustpoint** *trustpoint-label*  
or  
**trustpoint signing** *trustpoint-label*
5. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto provisioning petitioner</b>  <b>Example:</b> Router(config)# crypto provisioning petitioner	Allows SDP petitioner device behavior to be modified and enters tti-petitioner configuration mode. <div> <div>Note</div> <div>Effective with Cisco IOS Release 12.3(14)T, the <b>crypto provisioning petitioner</b> command replaced the <b>crypto wui tti petitioner</b> command.</div> </div>

	Command or Action	Purpose
Step 4	<b>trustpoint</b> <i>trustpoint-label</i>	(Optional) Specifies the trustpoint that is to be associated with the SDP exchange between the petitioner and the registrar.
	<b>Example:</b> Router(tti-petitioner)# <b>trustpoint</b> mytrust  or  <b>trustpoint signing</b> <i>trustpoint-label</i>  <b>Example:</b> Router(tti-petitioner)# <b>trustpoint</b> signing mytrust	<b>Note</b> If this command is not issued, the <i>trustpoint-label</i> argument is automatically labeled “tti.”  (Optional) Specifies the trustpoint and associated certificate that are used when signing all introduction data during the SDP exchange.
Step 5	<b>end</b>	(Optional) Exits tti-petitioner configuration mode.
	<b>Example:</b> Router(tti-petitioner)# <b>end</b>	

## Troubleshooting Tips

After the SDP exchange is complete, a new trustpoint-label named “tti” will exist. The trustpoint will be automatically enrolled with the certificate server (the registrar). To verify that the trustpoint is really there, use the **show running-config** command.

## What to Do Next

If you set up the petitioner to use a certificate and the RSA keys associated with the specified trustpoint, you should configure the registrar as shown in the task [“Enabling the SDP Registrar for Certificate-Based Authorization.”](#)

## Enabling the SDP Registrar and Adding AAA Lists to the Server

Perform this task to enable the registrar and associate a certificate server with the SDP exchange.

You can also use this task if you want to add an authentication list and an authorization list to the RADIUS or TACACS+ server.

## Prerequisites

Before configuring an registrar, ensure the following tasks are complete:

- Enable the HTTP server or the HTTPS server.



### Note

It is recommended that you issue the **ip http secure-server** command to enable the HTTPS web server. If you enable a secure server, you should issue the **ip http secure-trustpoint** command. You must disable the standard HTTP server via the **no ip http server** command (if the standard server is enabled). The specified trustpoint is a registrar local trustpoint appropriate for HTTPS communication between the registrar and the user’s browser.

- Configure the Cisco IOS certificate server (via the **crypto pki server** command).

If you are configuring AAA lists, you should complete the prerequisites required for the registrar in addition to completing the following tasks:

- Add user information to the AAA server database. To configure a RADIUS or TACACS+ AAA server, see the “Configuring RADIUS” and “Configuring TACACS+” chapters of the *Cisco IOS Security Configuration Guide*.
- Configure new AAA lists. To configure AAA lists, see the following chapters in the *Cisco IOS Security Configuration Guide*: “Configuring RADIUS,” “Configuring TACACS+,” “Configuring Authentication,” and “Configuring Authorization.”

## Restrictions

### Cisco IOS CA Device Requirement

During the SDP process, a Cisco IOS CA certificate is automatically issued to the peer device. If an SDP registrar is configured on a third-party vendor’s CA device, the SDP process will not work.

## The template config Command

There are nine Cisco IOS configuration variables. If you require more configuration flexibility, the **template config** command can be used to reference a configuration template that is specific to the introducer. For more information on configuration flexibility, see the “[Custom Configuration and File Template Variable Expansion Rules](#)” section.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto provisioning registrar**
4. **pki-server** *label*
5. **authentication list** *list-name*
6. **authorization list** *list-name*
7. **template username** *name* [**password** *password*]
8. **template config** *url* [**post**]
9. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto provisioning registrar</b>  <b>Example:</b> Router(config)# crypto provisioning registrar	Configures a device to become a registrar for the SDP exchange and enters tti-registrar configuration mode. <p><b>Note</b> Effective with Cisco IOS Release 12.3(14)T, the <b>crypto provisioning registrar</b> command replaced the <b>crypto wui tti registrar</b> command.</p>
Step 4	<b>pki-server label</b>  <b>Example:</b> Router(tti-registrar)# pki-server mycs	Specifies the certificate server that is to be associated with the SDP exchange between the petitioner and the registrar.
Step 5	<b>authentication list list-name</b>  <b>Example:</b> Router (tti-registrar)# authentication list authen-tac	(Optional) Authenticates the introducer in an SDP exchange.
Step 6	<b>authorization list list-name</b>  <b>Example:</b> Router (tti-registrar)# authorization list author-rad	(Optional) Receives the appropriate authorized fields for the certificate subject name and list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner.
Step 7	<b>template username name [password password]</b>  <b>Example:</b> Router(tti-registrar)# template username ftpuser password ftppwd	(Optional) Establishes a username and password in which to access the configuration template on the file system.

	Command or Action	Purpose
Step 8	<b>template config url [post]</b>  <b>Example:</b> Router(tti-registrar)# template config http://myserver/cgi-bin/mycgi post	(Optional) Specifies a remote URL for the Cisco IOS CLI configuration template.  The <i>url</i> can reference a configuration file allows you to specify the device name (\$n) to identify a bootstrap configuration. CGI support allows you to reference a CGI script via HTTP or HTTPS and identify the bootstrap configuration by not only the device name, but also by the type, current Cisco IOS version information, and current configuration.  The <b>post</b> keyword must be used for CGI support.  <b>Note</b> The registrar must be running Cisco IOS Release 12.4(6)T or later to utilize expanded CGI support. If the registrar is running an earlier version of Cisco IOS, the additional device identification information will be ignored.
Step 9	<b>end</b>  <b>Example:</b> Router(tti-registrar)# end	(Optional) Exits tti-registrar configuration mode.

## Examples

To help troubleshoot the SDP transaction, you can issue the **debug crypto provisioning** command, which displays output from the petitioner and registrar devices.

The following is output for the **debug crypto provisioning** command. The output from the petitioner and registrar devices are shown below.

```
Petitioner device
! The user starts the Welcome phase.
Nov 7 03:15:48.171: CRYPTO_PROVISIONING: received welcome get request.
! The router generates a Rivest, Shamir, and Adelman (RSA) keypair for future enrollment.
Nov 7 03:15:48.279: CRYPTO_PROVISIONING: keyhash 'A506BE3B83C6F4B4A6EFCEB3D584AACA'
! The TTI transaction is completed.
Nov 7 03:16:10.607: CRYPTO_PROVISIONING: received completion post request.
```

```
Registrar device
!. During the introduction phase, the browser prompts for login information.
06:39:18: CRYPTO_PROVISIONING: received introduction post request.
06:39:18: CRYPTO_PROVISIONING: checking AAA authentication (ipsecca_script_aalist,
ttiuser)
! This happens if the user types in the wrong username or password.
06:39:19: CRYPTO_PROVISIONING: authentication declined by AAA, or AAA server not found -
0x3
06:39:19: CRYPTO_PROVISIONING: aaa query fails!
! The user re-enters login information.
06:39:19: CRYPTO_PROVISIONING: received introduction post request.
06:39:19: CRYPTO_PROVISIONING: checking AAA authentication (ipsecca_script_aalist,
ttiuser)
06:39:20: CRYPTO_PROVISIONING: checking AAA authorization (ipsecca_script_aalist,
ttiuser)
! The login attempt succeeds and authorization information is retrieved from the AAA
database.
06:39:21: CRYPTO_PROVISIONING: aaa query ok!
```

```

! These attributes are inserted into the configuration template.
06:39:21: CRYPTO_PROVISIONING: building TTI av pairs from AAA attributes
06:39:21: CRYPTO_PROVISIONING: "subjectname" = "CN=user1, O=company, C=US"
06:39:21: CRYPTO_PROVISIONING: "$1" = "ntp server 10.3.0.1"
06:39:21: CRYPTO_PROVISIONING: "$2" = "hostname user1-vpn"
! The registrar stores this subject name and overrides the subject name in the subsequent
enrollment request.
06:39:21: CRYPTO_PROVISIONING: subjectname=CN=user1, O=company, C=US
! The registrar stores this key information so that it may be used to automatically grant
the subsequent enrollment request.
06:39:21: CRYPTO_PROVISIONING: key_hash=A506BE3B83C6F4B4A6EFCEB3D584AACA

```

## Enabling the SDP Registrar for Certificate-Based Authorization

Perform this task to enable the SDP registrar to perform the following functions:

- Verify the petitioner-signing certificate using a specified trustpoint or any configured trustpoint.
- Initiate authorization lookups using the introducer username and the certificate name field.

### Prerequisites

You must also configure the SDP petitioner to use a certificate and RSA keys associated with a specific trustpoint. To complete this task, use the trustpoint signing command as shown in the task [“Enabling the SDP Petitioner.”](#)

### Restrictions

Because RADIUS does not differentiate between authentication and authorization, you need to use the default password, cisco, for certificate authorization.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto provisioning registrar**
4. **template file** *sourceURL destinationURL*
5. **binary file** *sourceURL destinationURL*
6. **authentication trustpoint** {*trustpoint-label* | **use-any**}
7. **authorization** {**login** | **certificate** | **login certificate**}
8. **authorization username** {**subjectname** *subjectname*}
9. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto provisioning registrar</b>  <b>Example:</b> Router(config)# crypto provisioning registrar	Configures a device to become an SDP registrar and enters tti-registrar configuration mode.
Step 4	<b>template file</b> <i>sourceURL destinationURL</i>  <b>Example:</b> Router(tti-registrar)# template file http://myserver/registrar_file_r1 http://myserver/petitioner_file_p1	(Optional) Specifies the source template file location on the registrar and the destination template file location on the petitioner.  <b>Note</b> This command is useful when using a USB token to provision a device.  The template expansion occurs on the registrar for both the source URL and file content. The destination URL is expanded on the petitioner.
Step 5	<b>binary file</b> <i>sourceURL destinationURL</i>  <b>Example:</b> Router(tti-registrar)# binary file http://myserver/registrar_file_a1 http://myserver/petitioner_file_b1	(Optional) Specifies the binary file location on the registrar and the destination binary file location on the petitioner.  <b>Note</b> This command is useful when using a USB token to provision a device.  Both the source and destination URL are expanded on the registrar. Also, the destination URL and file content are expanded on the petitioner. Binary files are not processed through the template expansion functions.
Step 6	<b>authentication trustpoint</b> { <i>trustpoint-label</i>   <b>use-any</b> }  <b>Example:</b> Router(tti-registrar)# authentication trustpoint mytrust	(Optional) Specifies the trustpoint used to authenticate the SDP petitioner device's existing certificate. <ul style="list-style-type: none"> <li><i>trustpoint-label</i>—Specifies a specific trustpoint.</li> <li><b>use-any</b>—Specifies any configured trustpoint.</li> </ul> <b>Note</b> If you do not use this command to specify a trustpoint, the existing petitioner certificate is not validated. (This functionality provides compatibility with self-signed petitioner certificates.)



	Command or Action	Purpose
Step 7	<b>authorization {login   certificate   login certificate}</b>  <b>Example:</b> Router(tti-registrar)# authorization login certificate	(Optional) Enables AAA authorization for an introducer or a certificate. <ul style="list-style-type: none"> <li>Use the <b>login</b> keyword for authorization based on the introducer's username.</li> <li>Use the <b>certificate</b> keyword for authorization based on the petitioner's certificate.</li> <li>Use the <b>login certificate</b> keyword for authorization based on the introducer's username and the petitioner's certificate.</li> </ul>
Step 8	<b>authorization username subjectname subjectname</b>  <b>Example:</b> Router(tti-registrar)# authorization username subjectname all	Sets parameters for the different certificate fields that are used to build the AAA username. <ul style="list-style-type: none"> <li>The <b>all</b> keyword specifies that the entire subject name if the certificate is used as the authorization username.</li> </ul>
Step 9	<b>end</b>  <b>Example:</b> Router(tti-registrar)# end	(Optional) Exits tti-registrar configuration mode.

## Configuring an Administrative Introducer

Perform the following task to configure an administrative introducer using administrator authentication and authorization lists.

### Prerequisites

The administrative introducer must have enable privileges on the client device and administrator privileges on the server.

### Restrictions

When using RADIUS, a user/device that needs to be introduced by the administrative introducer must always use cisco as its own password. TACACS+ does not have this limitation; a user/device can have any password and be introduced by the administrative introducer.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto provisioning registrar**
4. **administrator authentication list** *list-name*
5. **administrator authorization list** *list-name*
6. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto provisioning registrar</b>  <b>Example:</b> Router(config)# crypto provisioning registrar	Configures a device to become an SDP registrar and enters tti-registrar configuration mode.
Step 4	<b>administrator authentication list list-name</b>  <b>Example:</b> Router(tti-registrar)# administrator authentication list authen-tac	Configures the AAA list used to authenticate an administrator during an introduction.
Step 5	<b>administrator authorization list list-name</b>  <b>Example:</b> Router(tti-registrar)# administrator authorization list author-tac	Configures the AAA list used to obtain authorization information for an administrator during an introduction. Information that can be obtained includes the certificate subject name and/or the list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner.
Step 6	<b>end</b>  <b>Example:</b> Router(tti-registrar)# end	(Optional) Exits tti-registrar configuration mode.

## Examples

The following example from the **show running-config** command allows you to verify that an administrative introducer using administrator authentication and authorization lists have been created:

```
Router# show running-config

Building configuration...

Current configuration : 2700 bytes
!
! Last configuration change at 01:22:26 GMT Fri Feb 4 2005
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router
!
```

```

boot-start-marker
boot-end-marker
!
memory-size iomem 5
enable secret 5 1tpBS$PXnBDTIDXfX5pWa//1JX20
enable password lab
!
aaa new-model
!
!
!
aaa session-id common
!
resource manager
!
clock timezone GMT 0
ip subnet-zero
no ip routing
!
!
no ip dhcp use vrf connected
!
!
no ip cef
no ip domain lookup
ip domain name company.com
ip host router 10.3.0.6
ip host router.company.com 10.3.0.6
no ip ips deny-action ips-interface
!
no ftp-server write-enable
!
crypto pki server mycs
!
crypto pki trustpoint mycs
 revocation-check crl
 rsakeypair mycs
!
crypto pki trustpoint tti
 revocation-check crl
 rsakeypair tti
!
crypto pki trustpoint mic
 enrollment url http://router:80
 revocation-check crl
!
crypto pki trustpoint cat
 revocation-check crl
!
!
!
crypto pki certificate map cat 10
!
crypto pki certificate chain mycs
 certificate ca 01
crypto pki certificate chain tti
crypto pki certificate chain mic
 certificate 02
 certificate ca 01
crypto pki certificate chain cat
!
crypto provisioning registrar <----- !SDP registrar device parameters!
 administrator authentication list authen-tac
 administrator authorization list author-tac

```

```

!
no crypto engine onboard 0
username qa privilege 15 password 0 lab

```

## Configuring Custom Templates

Perform this task to create and configure custom templates.

### SUMMARY STEPS

- enable
- configure terminal
- crypto provisioning registrar
- template http start *URL*
- template http welcome *URL*
- template http introduction *URL*
- template http admin-introduction *URL*
- template http completion *URL*
- template http error *URL*
- end

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto provisioning registrar</b>  <b>Example:</b> Router(config)# crypto provisioning registrar	Configures a device to become an SDP registrar and enters tti-registrar configuration mode.
Step 4	<b>template http start <i>URL</i></b>  <b>Example:</b> Router(tti-registrar)# template http start tftp://registrar.company.com/start.html	Directs the TTI registrar to use the custom start page template.  <b>Note</b> This command is required to use the start page functionality. If this command is not issued, the welcome page will be the initial communication between the introducer and the petitioner.

	Command or Action	Purpose
Step 5	<b>template http welcome URL</b>  <b>Example:</b> Router(tti-registrar)# template http welcome tftp://registrar.company.com/welcome.html	(Optional) Uses a custom welcome template rather than the default template.
Step 6	<b>template http introduction URL</b>  <b>Example:</b> Router(tti-registrar)# template http introduction tftp://registrar.company.com/intro.html	(Optional) Uses a custom introduction template rather than the default template.
Step 7	<b>template http admin-introduction URL</b>  <b>Example:</b> Router(tti-registrar)# template http admin-introduction tftp://registrar.company.com/admin-intro.html	(Optional) Uses a custom admin-introduction template rather than the default template.
Step 8	<b>template http completion URL</b>  <b>Example:</b> Router(tti-registrar)# template http completion tftp://registrar.company.com/completion.html	(Optional) Uses a custom completion template rather than the default template.
Step 9	<b>template http error URL</b>  <b>Example:</b> Router(tti-registrar)# template http error tftp://registrar.company.com/error.html	(Optional) Uses a custom error template rather than the default template.
Step 10	<b>end</b>  <b>Example:</b> Router(tti-registrar)# end	(Optional) Exits tti-registrar configuration mode.

## Examples

The following example shows the use of custom start, introduction, and completion templates:

```
template http start tftp://registrar.company.com/start.html
template http introduction tftp://registrar.company.com/intro.html
template http completion tftp://registrar.company.com/completion.html
```

## Configuration Examples for Setting Up a PKI via SDP

This section contains the following configuration examples:

- [Verifying the SDP Registrar: Example, page 34](#)
- [Verifying the SDP Petitioner: Example, page 37](#)
- [Adding AAA Lists to a RADIUS or TACACS+ Server: Examples, page 39](#)

- [Using a Configuration Template File: Example, page 41](#)
- [CGI Script: Example, page 41](#)
- [Configuring the Petitioner and Registrar for Certificate-Based Authentication: Example, page 43](#)
- [Configuring an Administrative Introducer Using Authentication and Authorization Lists: Example, page 44](#)

## Verifying the SDP Registrar: Example

The following sample output from the **show running-config** command verifies that the certificate server “cs1” was configured and associated with the SDP exchange between the registrar and petitioner:

```
Router# show running-config

Building configuration...

Current configuration : 5902 bytes
!
! Last configuration change at 09:34:44 GMT Sat Jan 31 2004
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname pki-36a
!
boot-start-marker
boot-end-marker
!
logging buffered 32768 debugging
no logging console
enable secret 5 1b3jz$CKquLGjFIE3AdXA2/Rl9./
enable password lab
!
clock timezone GMT 0
no aaa new-model
ip subnet-zero
!
!
ip cef
ip domain name company.com
ip host msca-root
ip host yni-u10
ip host pki-36a 10.23.2.131
ip host pki-36a.company.com 10.23.2.131
!
!
crypto pki server cs1
 issuer-name CN=company,L=city,C=US
 lifetime crl 336
 lifetime certificate 730
!
crypto pki trustpoint pki-36a
 enrollment url http://pki-36a:80
 ip-address FastEthernet0/0
 revocation-check none
!
crypto pki trustpoint cs1
 revocation-check crl
```

```

rsakeypair cs1
!
!
crypto pki certificate chain pki-36a
certificate 03
308201D0 30820139 A0030201 02020103 300D0609 2A864886 F70D0101 04050030
34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
39333334 345A170D 30363031 33303039 33333434 5A303A31 38301606 092A8648
86F70D01 09081309 31302E32 332E322E 32301E06 092A8648 86F70D01 09021611
706B692D 3336612E 63697363 6F2E636F 6D305C30 0D06092A 864886F7 0D010101
0500034B 00304802 4100AFFA 8F429618 112FAB9D 01F3352E 59DD3D2D AE67E31D
370AC4DA 619735DF 9CF4EA13 64E4B563 C239C5F0 1578B773 07BED641 A18CA629
191884B5 61B66ECF 4D110203 010001A3 30302E30 0B060355 1D0F0404 030205A0
301F0603 551D2304 18301680 141DA8B1 71652961 3F7D69F0 02903AC3 2BADB137
C6300D06 092A8648 86F70D01 01040500 03818100 67BAE186 327CED31 D642CB39
AD585731 95868683 B950DF14 3BCB155A 2B63CFAD B34B579C 79128AD9 296922E9
4DEDFCAF A7B5A412 AB1FC081 09951CE3 08BFFDD9 9FB1B9DA E9AA42C8 D1049268
C524E58F 11C6BA7F C750320C 03DFB6D4 CBB3E739 C8C76359 CE939A97 B51B3F7F
3FF;A9D82 9CFDB6CF E2503A14 36D0A236 A1CCFEAE
quit
certificate ca 01
30820241 308201AA A0030201 02020101 300D0609 2A864886 F70D0101 04050030
34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
39333132 315A170D 30373031 33303039 33313231 5A303431 0B300906 03550406
13025553 31143012 06035504 07130B20 53616E74 61204372 757A310F 300D0603
55040313 0620696F 73637330 819F300D 06092A86 4886F70D 01010105 0003818D
00308189 02818100 FC0695AF 181CE90A 1B34B348 BA957178 680C8B51 07802AC3
BF77B9C6 CB45092E 3C22292D C7D5FFC1 899185A1 FD8F37D5 C44FC206 6D1FA581
E2264C83 1CC7453E 548C89C6 F3CD25BC 9BFFE7C5 E6653A06 62133950 78BED51B
49128428 AB237F80 83A530EA 6F896193 F2134B54 D181F059 348AA84B 21EE6D80
727BF668 EB004341 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
01FF300E 0603551D 0F0101FF 04040302 0186301D 0603551D 0E041604 141DA8B1
71652961 3F7D69F0 02903AC3 2BADB137 C6301F06 03551D23 04183016 80141DA8
B1716529 613F7D69 F002903A C32BADB1 37C6300D 06092A86 4886F70D 01010405
00038181 00885895 A0141169 3D754EB2 E6FEC293 5BF0A80B E424AA2F A3F59765
3463AAD1 55E71F0F B5D1A35B 9EA79DAC DDB40721 1344C01E 015BAB73 1E148E03
9DD01431 A5E2887B 4AEC8EF4 48ACDB66 A6F9401E 8F7CA588 8A4199BB F8A437A0
F25064E7 112805D3 074A154F 650D09B9 8FA19347 ED359EAD 4181D9ED 0C667C10
8A7BCFB0 FB
quit
crypto pki certificate chain cs1
certificate ca 01
30820241 308201AA A0030201 02020101 300D0609 2A864886 F70D0101 04050030
34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
39333132 315A170D 30373031 33303039 33313231 5A303431 0B300906 03550406
13025553 31143012 06035504 07130B20 53616E74 61204372 757A310F 300D0603
55040313 0620696F 73637330 819F300D 06092A86 4886F70D 01010105 0003818D
00308189 02818100 FC0695AF 181CE90A 1B34B348 BA957178 680C8B51 07802AC3
BF77B9C6 CB45092E 3C22292D C7D5FFC1 899185A1 FD8F37D5 C44FC206 6D1FA581
E2264C83 1CC7453E 548C89C6 F3CD25BC 9BFFE7C5 E6653A06 62133950 78BED51B
49128428 AB237F80 83A530EA 6F896193 F2134B54 D181F059 348AA84B 21EE6D80
727BF668 EB004341 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
01FF300E 0603551D 0F0101FF 04040302 0186301D 0603551D 0E041604 141DA8B1
71652961 3F7D69F0 02903AC3 2BADB137 C6301F06 03551D23 04183016 80141DA8
B1716529 613F7D69 F002903A C32BADB1 37C6300D 06092A86 4886F70D 01010405
00038181 00885895 A0141169 3D754EB2 E6FEC293 5BF0A80B E424AA2F A3F59765
3463AAD1 55E71F0F B5D1A35B 9EA79DAC DDB40721 1344C01E 015BAB73 1E148E03
9DD01431 A5E2887B 4AEC8EF4 48ACDB66 A6F9401E 8F7CA588 8A4199BB F8A437A0;
F25064E7 112805D3 074A154F 650D09B9 8FA19347 ED359EAD 4181D9ED 0C667C10
8A7BCFB0 FB
quit

```

```

!
crypto provisioning registrar
 pki-server cs1
!
!
!
crypto isakmp policy 1
 hash md5
!
!
crypto ipsec transform-set test_transformset esp-3des
!
crypto map test_cryptomap 10 ipsec-isakmp
 set peer 10.23.1.10
 set security-association lifetime seconds 1800
 set transform-set test_transformset
 match address 170
!
!
interface Loopback0
 ip address 10.23.2.131 255.255.255.255
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
!
interface FastEthernet0/0
 ip address 10.23.2.2 255.255.255.192
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 duplex auto
 speed auto
 crypto map test_cryptomap
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip default-gateway 10.23.2.62
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 10.23.2.62
!
!
access-list 170 permit ip host 10.23.2.2 host 10.23.1.10
dialer-list 1 protocol ip permit
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 speed 115200
line aux 0
line vty 0 4
 password lab
 login
!
!
end

```



## Verifying the SDP Petitioner: Example

After the SDP exchange is complete, the petitioner will automatically enroll with the registrar and obtain a certificate. The following sample output via the **show running-config** command shows the automatically generated configuration, which verifies that the trustpoint is really there:

```
Router# show running-config

Building configuration...

Current configuration : 4650 bytes
!
! Last configuration change at 09:34:53 GMT Sat Jan 31 2004
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname pki-36b
!
boot-start-marker
boot-end-marker
!
logging buffered 32768 debugging
no logging console
enable secret 5 1JYgw$060JKXgl6dERLZpU9J3gb.
enable password lab
!
clock timezone GMT 0
no aaa new-model
ip subnet-zero
!
!
ip cef
ip domain name company.com
ip host msca-root
ip host yni-u10
ip host pki-36a 10.23.2.131
ip host pki-36a.company.com 10.23.2.131
!
!
crypto pki trustpoint tti
 enrollment url http://pki-36a.company.com:80
 revocation-check crl
 rsakeypair tti 1024
 auto-enroll 70
!
!
crypto pki certificate chain tti
certificate 02
 308201FC 30820165 A00302012;02020102 300D0609 2A864886 F70D0101 04050030
 34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
 4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
 39333333 385A170D 30363031 33303039 33333338 5A302231 20301E06 092A8648
 86F70D01 09021611 706B692D 3336622E 63697363 6F2E636F 6D30819F 300D0609
 2A864886 F70D0101 01050003 818D0030 81890281 8100E383 35584B6C 24751E2C
 F4088F06 C00BFECF 84CFF8EB 50D52044 03D14A2B 91E5A260 7D07ED24 DB599D27
 432065D9 0E459248 D7CDC15D 654E2AF6 BA27D79C 23850306 3E96C508 F311D333
 76FDCC9C A810F75C FCD10F1B 9A142F0C 338B6DB3 346D3F24 97A4B15D 0A9504E7
 1F6CB769 85E9F52B FE907AAF 63D54D66 1A715A20 D7DB0203 010001A3 30302E30
 0B060355 1D0F0404 030205A0 301F0603 551D2304 18301680 141DA8B1 71652961
 3F7D69F0 02903AC3 2BADB137 C6300D06 092A8648 86F70D01 01040500 03818100
```

```

C5E2DA0E 4312BCF8 0396014F E18B3EE9 6C970BB7 B8FAFC61 EF849568 D546F73F
67D2A73C 156202DC 7404A394 D6124DAF 6BACB8CF 96C3141D 109C5B0E 46F4F827
022474ED 8B59D654 F04E31A2 C9AA1152 75A0C455 FD7EEEF5 A505A648 863EE9E6
C361D9BD E12BBB36 16B729DF 823AD5CC 404CCE48 A4379CDC 67FF6362 0601B950
quit
certificate ca 01
30820241 308201AA A0030201 02020101 300D0609 2A864886 F70D0101 04050030
34310B30 09060355 04061302 55533114 30120603 55040713 0B205361 6E746120
4372757A 310F300D 06035504 03130620 696F7363 73301E17 0D303430 31333130
39333132 315A170D 30373031 33303039 33313231 5A303431 0B300906 03550406
13025553 31143012 06035504 07130B20 53616E74 61204372 757A310F 300D0603
55040313 0620696F 73637330 819F300D 06092A86 4886F70D 01010105 0003818D
00308189 02818100 FC0695AF 181CE90A 1B34B348 BA957178 680C8B51 07802AC3
BF77B9C6 CB45092E 3C22292D C7D5FFC1 899185A1 FD8F37D5 C44FC206 6D1FA581
E2264C83 1CC7453E 548C89C6 F3CD25BC 9BFFE7C5 E6653A06 62133950 78BED51B
49128428 AB237F80 83A530EA 6F896193 F2134B54 D181F059 348AA84B 21EE6D80
727BF668 EB004341 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
01FF300E 0603551D 0F0101FF 04040302 0186301D 0603551D 0E041604 141DA8B1
71652961 3F7D69F0 02903AC3 2BADB137 C6301F06 03551D23 04183016 80141DA8
B1716529 613F7D69 F002903A C32BADB1 37C6300D 06092A86 4886F70D 01010405
00038181 00885895 A0141169 3D754EB2 E6FEC293 5BF0A80B E424AA2F A3F59765
3463AAD1 55E71F0F B5D1A35B 9EA79DAC DDB40721 1344C01E 015BAB73 1E148E03
9DD01431 A5E2887B 4AEC8EF4 48ACDB66 A6F9401E 8F7CA588 8A4199BB F8A437A0
F25064E7 112805D3 074A154F 650D09B9 8FA19347 ED359EAD 4181D9ED 0C667C10
8A7BCFB0 FB
quit
!
no crypto engine accelerator
!
!
crypto isakmp policy 1
 hash md5
!
!
crypto ipsec transform-set test_transformset esp-3des
!
crypto map test_cryptomap 10 ipsec-isakmp
 set peer 10.23.2.2
 set security-association lifetime seconds 1800
 set transform-set test_transformset
 match address 170
!
!
interface Ethernet0/0
 ip address 10.23.1.10 255.255.255.192
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 half-duplex
 crypto map test_cryptomap
!
interface Ethernet0/1
 no ip address
 shutdown
 half-duplex
!
interface Ethernet0/2
 no ip address
 shutdown
 half-duplex
!
interface Ethernet0/3
 no ip address
 shutdown

```

```
half-duplex
!
interface Serial1/0
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/3
no ip address
shutdown
serial restart-delay 0
!
ip default-gateway 10.23.1.62
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 10.23.1.62
!
!
access-list 170 permit ip host 10.23.1.10 host 10.23.2.2
dialer-list 1 protocol ip permit
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
speed 115200
line aux 0
line vty 0 4
password lab
login
!
!
end
```

## Adding AAA Lists to a RADIUS or TACACS+ Server: Examples

This section contains the following configuration examples:

- [TACACS+ AAA Server Database: Example, page 40](#)
- [RADIUS AAA Server Database: Example, page 40](#)
- [AAA List on a TACACS+ and a RADIUS AAA Server: Example, page 40](#)

## TACACS+ AAA Server Database: Example

In the following example, user information has been added to a TACACS+ AAA database. The username is “user1.” The password is “cisco.” Two Cisco IOS configuration template variables are configured for “user1”: iosconfig1 and iosconfig2. The variables will replace \$1 and \$2 in the configuration template file. The subject name “CN=user1, O=company, C=US” is also configured. This subject name will replace the subject name field in the subsequent enrollment request (PKCS10) that is received from the petitioner device.

```
user = user1
 password = clear "pswd"

 service=tti
 ! The certificate server inserts the following subject name to the certificate.
 set subjectname="CN=user1, O=company, C=US"

 ! Up to nine template variables may be added.
 set iosconfig1="ntp server 10.3.0.1"
 set iosconfig2="hostname user1-vpn"
```

## RADIUS AAA Server Database: Example

User information has been added to the RADIUS AAA server database in the following example. The username is “user1.” The password is “cisco.” Two Cisco IOS configuration template variables are configured for “user1”: iosconfig1 and iosconfig2. The variables will replace \$1 and \$2 in the configuration template file. The subject name “CN=user1, O=company, C=US” is also configured. This subject name will replace the subject name field in the subsequent enrollment request (PKCS10) that is received from the petitioner device.

```
user = user1
 password = clear "pswd"
 radius=company
 reply_attributes=9,1="tti:subjectname=CN=user1, O=company, C=US"
 ! Up to nine template variables may be added.
 9,1="tti:iosconfig1=ntp server 10.3.0.5"
 9,1="tti:iosconfig2=hostname user1-vpn"
```

## AAA List on a TACACS+ and a RADIUS AAA Server: Example

The following is a configuration example showing that AAA authentication has been configured on a TACACS+ server and that AAA authorization has been configured on a RADIUS server.



### Note

---

Authentication and authorization usually point to the same server.

---

```
Router(config)# tacacs-server host 10.0.0.48 key cisco
Router(config)# aaa authentication login authen-tac group tacacs+
```

```
Router(config)# radius-server host 10.0.1.49 key cisco
Router(config)# aaa authorization network author-rad group radius
```

## Using a Configuration Template File: Example

You can use a different configuration template file on the basis of the introducer name. For example, if you have multiple template files for different users, each with the username in the filename, configure the following under the registrar:

```
Router(config)# crypto provisioning registrar
Router (tti-registrar)# pki-server cs1
Router (tti-registrar)# template config tftp://server/config-$n.txt
```

In this example, the default configuration file shown in the section “[Default Template for the Configuration File](#)” will be used because the **template config** command does not reference a CGI script.

## CGI Script: Example

The following example would execute a CGI script named “mysdpcgi”:

```
Router(config)# crypto provisioning registrar
Router (tti-registrar)# pki-server cs1
Router (tti-registrar)# template config tftp://server/cgi-bin/mysdpcgi post
```

The following is an example CGI script, named “mysdpcgi”, that would be executed with the example **template config** command above:

```
#!/usr/bin/perl -w

for debugging use the -debug form
use CGI (-debug);
use CGI;

base64 decoding is being used.
use MIME::Base64;

The following has been commented out, but left for your information.
#
Reading everything that has been received from stdin and writing it to the debug log to
see what has been sent from the registrar.
#
Remember to reset the STDIN pointer so that the normal CGI processing can get the input.
#
print STDERR "mysdpcgi.cgi dump of stdin:\n";
if($ENV{'REQUEST_METHOD'} eq "GET"){
$input_data = $ENV{'QUERY_STRING'};
}
else {
$data_length = $ENV{'CONTENT_LENGTH'};
$bytes_read = read(STDIN, $input_data, $data_length);
}
print STDERR $input_data, "\n";
exit;

$query = new CGI;
my %av_table;

A basic configuration file is being sent back, therefore it is being indicated as plain
text in the command below.
```

```

print $query->header ("text/plain");
print "\n";

For testing, parameters can be passed in so that the test applications can
see what has been received.
#
print STDERR "The following are the raw AV pairs mysdp.cgi received:\n";
for each $key ($query->param) {
print STDERR "! $key is: \n";
$value = $query->param($key);
print STDERR "! ", $value;
print STDERR "! \n";
}

The post process AV pairs are identical to those in Cisco IOS and may be used to produce
AV pair specific configurations as needed.

%av_table = &postprocessavpairs($query->param);

Decoded values may be written out.
WARNING: Some error_logs cannot handle the amount of data and will freeze.
print STDERR "The following are the decoded AV pairs mysdp.cgi received:\n";
now write the values out
while (($a, $v) = each(%av_table)) {
print STDERR "$a = $v\n";
}

Identifying the AV pairs and specifying them in the config.

while (($a, $v) = each(%av_table)) {
 if ($a eq "TTIIosRunningConfig") {
 $search = "hostname ";
 $begin = index($v, $search) + length($search);
 $end = index($v, "\n", $begin);
 $hostname = substr($v, $begin, $end - $begin);
 }
 if ($a eq "TTIIosVersion") {
 $search = "Version ";
 $begin = index($v, $search) + length($search);
 $end = index($v, "(", $begin);
 $version = substr($v, $begin, $end - $begin);
 }
}

print <<END_CONFIG;
!
! Config auto-generated by sdp.cgi
! This is for SDP testing only and is not a real config
!
!
\st
!
\sc
!
cry pki trust Version-$version-$hostname

! NOTE: The last line of the config must be 'end' with a blank line after the end
statement.

END_CONFIG
;

Emulate IOS tti_postprocessavpairs functionality
sub postprocessavpairs {

```

```

@attributes = @_;

Combine any AV pairs that were split apart
$n = 0; #element index counter
while ($attributes[$n]) {
see if we are at the start of a set
if ($attributes[$n] =~ m/_0/) {
 # determine base attribute name
 $a = (split /_0/, $attributes[$n])[0];
 # set initial (partial) value
 $v = $query->param($attributes[$n]);

 # loop and pull the rest of the matching
 # attributes's values into v (would be
 # faster if we stop at first non-match)
 $c = $n+1;
 while ($attributes[$c]) {
 if ($attributes[$c] =~ m/$a/) {
 $v = $v.$query->param($attributes[$c]);
 }
 $c++;
 }

 # store in the av hash table
 $av_table{$a} = $v;
} else {
 # store in hash table if not part of a set
 if ($attributes[$n] !~ m/_\d/) {
 $av_table{$attributes[$n]} = $query->param($attributes[$n]);
 }
}
$n++;
}

de-base64 decode all AV pairs except userdevicename
while (($a, $v) = each(%av_table)) {
 if ($a ne "userdevicename") {
 $av_table{$a} = decode_base64($av_table{$a});
 }
}

return %av_table;
}

```

**Note**

A CGI script cannot be executed without using the **post** keyword with the **template config** command in Cisco IOS Release 12.4(6)T or a later release.

## Configuring the Petitioner and Registrar for Certificate-Based Authentication: Example

The following examples shows how to configure a petitioner to use the certificate issued by the trustpoint named mytrust:

```

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# crypto provisioning petitioner
Router(tti-petitioner)# trustpoint signing mytrust
Router(tti-petitioner)# end

```

The following example shows how to configure a registrar to verify the petitioner-signing certificate and to perform authorization lookups:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# crypto provisioning registrar
Router(tti-registrar)# authentication trustpoint mytrust
Router(tti-registrar)# authorization login certificate
Router(tti-registrar)# authorization username subjectname all
Router(tti-registrar)# end
```

## Configuring an Administrative Introducer Using Authentication and Authorization Lists: Example

The following example shows how to configure an administrative introducer with the authentication list “authen-tac” and the authorization list “author-tac”:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# crypto provisioning registrar
Router(tti-registrar)# administrator authentication list authen-tac
Router(tti-registrar)# administrator authorization list author-tac
Router(tti-registrar)# end
```



# Additional References

The following sections provide references related to SDP.

## Related Documents

Related Topic	Document Title
Certificate enrollment	“Configuring Certificate Enrollment for a PKI” module
Certificate server configuration	“Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment” module
PKI AAA integration concepts and configuration tasks	“Configuration Revocation and Authorization of Certificates in a PKI” module
PKI commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<i>Cisco IOS Security Command Reference</i> , Release 12.4T
USB token configuration	“Storing PKI Credentials” chapter in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4T  For other 12.4T features about using SDP and USB tokens to deploy PKI credentials, see the Feature Information Table.

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Feature Information for SDP in a PKI

Table 3 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “Implementing and Managing PKI Features Roadmap.”

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



### Note

Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 3** Feature Information for SDP in a PKI

Feature Name	Releases	Feature Information
Secure Device Provisioning (SDP) Connect Template	12.4(20)T	<p>This feature provides the ability to configure a device for Internet connectivity through a service provider.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Prerequisites for Setting Up SDP</a></li> <li>• <a href="#">SDP Overview</a></li> <li>• <a href="#">How SDP Works</a></li> <li>• <a href="#">Default Templates for SDP Transaction Web Pages</a></li> </ul>
USB Token and Secure Device Provisioning (SDP) Integration	12.4(15)T	<p>This feature provides the ability to provision remote devices using a USB token as a mechanism to transfer credentials from one network device to a remote device via SDP.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Prerequisites for Setting Up SDP</a></li> <li>• <a href="#">SDP Leveraging USB Tokens</a></li> <li>• <a href="#">Enabling the SDP Registrar for Certificate-Based Authorization</a></li> </ul> <p>The following commands were introduced by this feature: <b>binary file, crypto key move rsa, template file.</b></p> <p><b>Note</b> For other documentation on this topic, see the “<a href="#">Related Documents</a>” section.</p>

**Table 3** *Feature Information for SDP in a PKI (continued)*

Feature Name	Releases	Feature Information
SDP Expanded Template CGI Support	12.4(6)T	<p>This feature allows users to configure the SDP registrar to send a bootstrap configuration to the SDP petitioner based on not only the device name, but also its current Cisco IOS version and current configuration.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">SDP Introduction Phase</a></li> <li>• <a href="#">Custom Configuration and File Template Variable Expansion Rules</a></li> <li>• <a href="#">Default Template for the Configuration File</a></li> <li>• <a href="#">Enabling the SDP Registrar and Adding AAA Lists to the Server</a></li> <li>• <a href="#">CGI Script: Example</a></li> </ul> <p>The following command was modified by this feature: <b>template config</b></p>
Secure Device Provisioning (SDP) Start Page	12.4(4)T	<p>This feature allows users to configure their browsers to begin the TTI transaction by contacting the registrar's introduction URL via a start page. Thus, users no longer have to begin the TTI transaction from the welcome page on the petitioner.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">How Custom Templates Work with SDP</a></li> <li>• <a href="#">Configuring Custom Templates</a></li> </ul> <p>The following commands were introduced by this feature: <b>template http admin-introduction, template http completion, template http error, template http introduction, template http start, template http welcome</b></p>
Administrative Secure Device Provisioning Introducer	12.3(14)T	<p>This feature allows you to act as an administrative introducer to introduce a device into a PKI network and then provide a username as the device name for the record locator in the AAA database.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Authentication and Authorization Lists for an Administrative Introducer</a></li> <li>• <a href="#">Configuring an Administrative Introducer</a></li> </ul> <p>The following commands were introduced by this feature: <b>administrator authentication list, administrator authorization list</b></p>

**Table 3** *Feature Information for SDP in a PKI (continued)*

Feature Name	Releases	Feature Information
Easy Secure Device Deployment	12.3(8)T	<p>This feature introduces support for SDP, which offers a web-based enrollment interface that enables network administrators to deploy new devices in large networks.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Information About Setting Up SDP for Enrollment in a PKI</a></li> <li>• <a href="#">Enabling the SDP Registrar and Adding AAA Lists to the Server</a></li> </ul> <p>The following commands were introduced or modified by this feature: <b>crypto wui tti petitioner</b>, <b>crypto wui tti registrar</b>, <b>pki-server</b>, <b>template config</b>, <b>template username</b>, <b>trustpoint (tti-petitioner)</b></p>
Easy Secure Device Deployment AAA Integration	12.3(8)T	<p>This feature integrates an external AAA database, allowing the SDP introducer to be authenticated against a AAA database instead of having to use the enable password of the local Cisco certificate server.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">How SDP Uses an External AAA Database</a></li> <li>• <a href="#">Enabling the SDP Registrar and Adding AAA Lists to the Server</a></li> </ul> <p>The following commands were introduced or modified by this feature: <b>authentication list (tti-registrar)</b>, <b>authorization list (tti-registrar)</b>, <b>debug crypto wui template config</b>, <b>template username</b></p>
Secure Device Provisioning (SDP) Certificate-Based Authorization	12.3(14)T	<p>This feature allows certificates issued by other authority (CA) servers to be used for SDP introductions.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Use of a Self-Signed Certificate Versus a Certificate Issued by Another CA Server</a></li> <li>• <a href="#">Enabling the SDP Registrar for Certificate-Based Authorization</a></li> </ul> <p>The following commands were introduced by this feature: <b>administrator authentication list</b>, <b>administrator authorization list</b></p>

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2005–2008 Cisco Systems, Inc. All rights reserved.





# Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment

---

**First Published: May 2, 2005**

**Last Updated: November 17, 2006**

This module describes how to set up and manage a Cisco IOS certificate server for public key infrastructure (PKI) deployment. A certificate server embeds a simple certificate server, with limited certification authority (CA) functionality, into the Cisco IOS software. Thus, the following benefits are provided to the user:

- Easier PKI deployment by defining default behavior. The user interface is simpler because default behaviors are predefined. That is, you can leverage the scaling advantages of PKI without all of the certificate extensions that a CA provides, thereby allowing you to easily enable a basic PKI-secured network.
- Direct integration with Cisco IOS software.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for the Cisco IOS Certificate Server](#)” section on page 50.*

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for Configuring a Cisco IOS Certificate Server, page 2](#)
- [Restrictions for Configuring a Cisco IOS Certificate Server, page 3](#)
- [Information About Cisco IOS Certificate Servers, page 3](#)
- [How to Set Up and Deploy a Cisco IOS Certificate Server, page 10](#)



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2005–2007 Cisco Systems, Inc. All rights reserved.

- [Configuration Examples for Using a Certificate Server, page 36](#)
- [Where to Go Next, page 48](#)
- [Additional References, page 48](#)
- [Feature Information for the Cisco IOS Certificate Server, page 50](#)

## Prerequisites for Configuring a Cisco IOS Certificate Server

### Planning Your PKI Before Configuring the Certificate Server

Before configuring a Cisco IOS certificate server, it is important that you have planned for and chosen appropriate values for the settings you intend to use within your PKI (such as certificate lifetimes and certificate revocation list (CRL) lifetimes). After the settings have been configured in the certificate server and certificates have been granted, settings cannot be changed without having to reconfigure the certificate server and reenrolling the peers. For information on certificate server default settings and recommended settings, see the section “[Certificate Server Default Values and Recommended Values](#).”

### Enabling an HTTP Server

The certificate server supports Simple Certificate Enrollment Protocol (SCEP) over HTTP. The HTTP server must be enabled on the router for the certificate server to use SCEP. (To enable the HTTP server, use the **ip http server** command.) The certificate server will automatically enable or disable SCEP services after the HTTP server is enabled or disabled. If the HTTP server is not enabled, only manual PKCS10 enrollment is supported.



#### Note

To take advantage of automatic CA certificate and key pair rollover functionality for all types of certificate servers, Cisco IOS Release 12.4(4)T or a later release must be used and SCEP must be used as the enrollment method.

### Configuring Reliable Time Services

Time services must be running on the router because the certificate server must have reliable time knowledge. If a hardware clock is unavailable, the certificate server will depend on manually configured clock settings, such as Network Time Protocol (NTP). If there is not a hardware clock or the clock is invalid, the following message will be displayed at bootup:

```
% Time has not been set. Cannot start the Certificate server.
```

After the clock has been set, the certificate server will automatically switch to running status.

For information on manually configuring clock settings, see the section “Setting Time and Calendar Services” in the chapter “Performing Basic System Management” of the *Cisco IOS Network Management Configuration Guide*.

### “crypto ca” to “crypto pki” CLI Change

As of Cisco IOS Release 12.3(7)T, all commands that begin as “crypto ca” have been changed to begin as “crypto pki.” Although the router will still accept crypto ca commands, all output will be read back as crypto pki.



# Restrictions for Configuring a Cisco IOS Certificate Server

The certificate server does not provide a mechanism for modifying the certificate request that is received from the client; that is, the certificate that is issued from the certificate server matches the requested certificate without modifications. If a specific certificate policy, such as name constraints, must be issued, the policy must be reflected in the certificate request.

## Information About Cisco IOS Certificate Servers

Before setting up and deploying a certificate server in your PKI, you should understand the following concepts:

- [RSA Key Pair and Certificate of the Certificate Server, page 3](#)
- [Certificate Server Database, page 4](#)
- [Trustpoint of the Certificate Server, page 6](#)
- [Certificate Revocation Lists \(CRLs\), page 6](#)
- [Certificate Server Error Conditions, page 7](#)
- [Certificate Enrollment Using a Certificate Server, page 8](#)
- [Types of CA Servers: Subordinate and Registration Authorities \(RAs\), page 8](#)
- [Automatic CA Certificate and Key Rollover, page 9](#)

## RSA Key Pair and Certificate of the Certificate Server

The certificate server automatically generates a 1024-bit Rivest, Shamir, and Adelman (RSA) key pair. You must manually generate an RSA key pair if you prefer a different key pair modulus. For information on completing this task, see the section “[Generating a Certificate Server RSA Key Pair.](#)”

**Note**

---

The recommended modulus for a certificate server key pair is 2048 bits.

---

The certificate server will use a regular Cisco IOS RSA key pair as its CA key. This key pair must have the same name as the certificate server. If you do not generate the key pair before the certificate server is created on the router, a general-purpose key pair will be automatically generated during the configuration of the certificate server.

As of Cisco IOS Release 12.3(11)T and later releases, the CA certificate and CA key can be backed up automatically one time after they are generated by the certificate server. As a result, it is not necessary to generate an exportable CA key for backup purposes.

**What to Do with Automatically Generated Key Pairs in Cisco IOS Software Prior to Release 12.3(11)T**

If the key pair is automatically generated, it will not be marked as exportable. Thus, you must manually generate the key pair as exportable if you want to back up the CA key. For information on how to complete this task, see the section “[Generating a Certificate Server RSA Key Pair.](#)”

## How the CA Certificate and CA Key Are Automatically Archived

At initial certificate server setup, you can enable the CA certificate and the CA key to be automatically archived so that they may be restored later if either the original copy or the original configuration is lost.

When the certificate server is turned on the first time, the CA certificate and CA key will be generated. If automatic archive is also enabled, the CA certificate and the CA key will be exported (archived) to the server database. The archive can be in PKCS12 or privacy-enhanced mail (PEM) format.

**Note**

- This CA key backup file is extremely important and should be moved immediately to another secured place.
- This archiving action occurs only one time. Only the CA key that is (1) manually generated and marked exportable or (2) automatically generated by the certificate server will be archived (this key will be marked nonexportable).
- Autoarchiving will not occur if you generate the CA key manually and mark it “nonexportable.”
- In addition to the CA certificate and CA key archive file, you should also regularly back up the serial number file (.ser) and the CRL file (.crl). The serial file and the CRL file are both critical for CA operation if you need to restore your certificate server.
- It is not possible to manually back up a server that uses nonexportable RSA keys or manually generated, nonexportable RSA keys. Although automatically generated RSA keys are marked as nonexportable, they are automatically archived once.

## Certificate Server Database

The Cisco IOS certificate server stores files for its own use and may publish files for other processes to use. Critical files generated by the certificate server that are needed for its ongoing operation are stored to only one location per file type for its exclusive use. The certificate server reads from and writes to these files. The critical certificate server files are the serial number file (.ser) and the CRL storage location file (.crl). Files that the certificate server writes to, but does not read from again, may be published and available for use by other processes. An example of a file that may be published is the issued certificates file (.crt).

Performance of your certificate server may be affected by the following factors, which should be considered when you choose storage options and publication options for your certificate server files.

- The storage or publish locations you choose may affect your certificate server performance. Reading from a network location takes more time than reading directly from a router’s local storage device.
- The number of files you choose to store or publish to a specific location may affect your certificate server performance. The local Cisco IOS file system may not always be suitable for a large number of files.
- The file types you choose to store or publish may affect your certificate server performance. Certain files, such as the .crl files, can become very large.

**Note**

It is recommended that you store .ser and .crl files to your local Cisco IOS file system and publish your .crt files to a remote file system.

## Certificate Server Database File Storage

The certificate server allows the flexibility to store different critical file types to different storage locations depending on the database level set (see the **database level** command for more information). When choosing storage locations, consider the file security needed and server performance. For instance, serial number files and archive files (.p12 or .pem) might have greater security restrictions than the issued certificates file storage location (.crt) or the name file storage location (.cnm).

Table 1 shows the critical certificate server file types by file extension that may be stored to a specific location.

**Table 1**      **Certificate Server Storage Critical File Types**

File Extension	File Type
.ser	The main certificate server database file.
.crl	The CRL storage location.
.crt	The issued certificates storage location.
.cnm	The certificate name and expiration file storage location.
.p12	The certificate server certificate archive file location in PKCS12 format.
.pem	The certificate server certificate archive file location in PEM format.

Cisco IOS certificate server files may be stored to three levels of specificity:

- Default location, NVRAM
- Specified primary storage location for all critical files
- Specified storage location for specific critical file(s).

A more specific storage location setting overrides a more general storage location setting. For instance, if you have not specified any certificate server file storage locations, all certificate server files will be stored to NVRAM. If you specify a storage location for the name file, only the name file will be stored there; all other files will still be stored to NVRAM. If you then specify a primary location, all files except the name file will now be stored to this location, instead of NVRAM.

**Note**

You may specify either .p12 or .pem; you cannot specify both types of archive files.

## Certificate Server Database File Publication

A publish file is a copy of the original file and is available for other processes to use or for your use. If the certificate server fails to publish a file, it does cause the server to shut down. You may specify one publish location for the issued certificates file and name file and multiple publish locations for the CRL file. See Table 2 for files types available for publication. You may publish files regardless of the database level that is set.

Table 2 Certificate Server Publish File Types

File Extension	File Type
.crl	The CRL publish location.
.crt	The issued certificates publish location.
.cnm	The certificate name and expiration file publish location.

## Trustpoint of the Certificate Server

The certificate server will also have an automatically generated trustpoint of the same name; the trustpoint will store the certificate of the certificate server. After the router detects that a trustpoint is being used to store the certificate of the certificate server, the trustpoint will be locked so that it cannot be modified.

Before configuring the certificate server you can perform the following:

- Manually create and set up this trustpoint (using the **crypto pki trustpoint** command), which allows you to specify an alternative RSA key pair (using the **rsa keypair** command).
- Specify that the initial autoenrollment key pair will be generated on a specific device, such as a configured and available USB token, using the **on** command.



### Note

The automatically generated trustpoint and the certificate server certificate are not available for the certificate server device identity. Thus, any command-line interface (CLI) (such as the **ip http secure-trustpoint** command) that is used to specify the CA trustpoint to obtain certificates and authenticate the connecting client's certificate must point to an additional trustpoint configured on the certificate server device.

If the server is a root certificate server, it will use the RSA key pairs and several other attributes to generate a self-signed certificate. The associated CA certificate will have the following key usage extensions—Digital Signature, Certificate Sign, and CRL Sign.

After the CA certificate is generated, attributes can be changed only if the certificate server is destroyed.



### Note

A certificate server trustpoint must not be automatically enrolled using the **auto-enroll** command. Initial enrollment of the certificate server must be initiated manually and ongoing automatic rollover functionality may be configured with the **auto-rollover** command. For more information on automatic rollover functionality, see the section [“Automatic CA Certificate and Key Rollover.”](#)

## Certificate Revocation Lists (CRLs)

By default, CRLs are issued once every 168 hours (1 calendar week). To specify a value other than the default value for issuing the CRL, execute the **lifetime crl** command. After the CRL is issued, it is written to the specified database location as *ca-label.crl*, where *ca-label* is the name of the certificate server.

CRLs can be distributed via SCEP, which is the default method, or a CRL distribution point (CDP), if configured and available. If you set up a CDP, use the **cdp-url** command to specify the CDP location. If the **cdp-url** command is not specified, the CDP certificate extension will not be included in the

certificates that are issued by the certificate server. If the CDP location is not specified, Cisco IOS PKI clients will automatically request a CRL from the certificate server with a SCEP GetCRL message. The CA then returns the CRL in a SCEP CertRep message to the client. Because all SCEP messages are enveloped and signed PKCS#7 data, the SCEP retrieval of the CRL from the certificate server is costly and not highly scalable. In very large networks, an HTTP CDP provides better scalability and is recommended if you have many peer devices that will be checking CRLs. You may specify the CDP location by a simple HTTP URL string for example,

```
cdp-url http://my-cdp.company.com/filename.crl
```

The certificate server supports only one CDP; thus, all certificates that are issued include the same CDP.

If you have PKI clients that are not running Cisco IOS software and that do not support a SCEP GetCRL request and wish to use a CDP you may set up an external server to distribute CRLs and configure the CDP to point to that server. Or, you can specify a non-SCEP request for the retrieval of the CRL from the certificate server by specifying the **cdp-url** command with the URL in the following format where *cs-addr* is the location of the certificate server:

```
cdp-url http://cs-addr/cgi-bin/pkiclient.exe?operation=GetCRL
```

**Note**

If your Cisco IOS CA is also configured as your HTTP CDP server, specify your CDP with the **cdp-url** `http://cs-addr/cgi-bin/pkiclient.exe?operation=GetCRL` command syntax.

It is the responsibility of the network administrator to ensure that the CRL is available from the location that is specified via the **cdp-url** command.

The CDP location may be changed after the certificate server is running via the **cdp-url** command. New certificates will contain the updated CDP location, but existing certificates will not be reissued with the newly specified CDP location. When a new CRL is issued, the certificate server uses its current cached CRL to generate a new CRL. (When the certificate server is rebooted, it reloads the current CRL from the database.) A new CRL cannot be issued unless the current CRL has expired. After the current CRL expires, a new CRL is issued only after a certificate is revoked from the CLI.

## Certificate Server Error Conditions

At startup, the certificate server checks the current configuration before issuing any certificates. It reports the last known error conditions via the **show crypto pki server** command output. Example errors can include any of the following conditions:

- Storage inaccessible
- Waiting for HTTP server
- Waiting for time setting

If the certificate server experiences a critical failure at any time, such as failing to publish a CRL, the certificate server will automatically enter a disabled state. This state allows the network administrator to fix the condition; thereafter, the certificate server will return to the previous normal state.

## Certificate Enrollment Using a Certificate Server

A certificate enrollment request functions as follows:

- The certificate server receives the enrollment request from an end user, and the following actions occur:
  - A request entry is created in the enrollment request database with the initial state. (See [Table 3](#) for a complete list of certificate enrollment request states.)
  - The certificate server refers to the CLI configuration (or the default behavior any time a parameter is not specified) to determine the authorization of the request. Thereafter, the state of the enrollment request is updated in the enrollment request database.
- At each SCEP query for a response, the certificate server examines the current request and performs one of the following actions:
  - Responds to the end user with a “pending” or “denied” state.
  - Generates and signs the appropriate certificate and stores the certificate in the enrollment request database.

If the connection of the client has closed, the certificate server will wait for the client to request another certificate.

All enrollment requests transition through the certificate enrollment states that are defined in [Table 3](#). To see current enrollment requests, use the **crypto pki server request pkcs10** command.

**Table 3** *Certificate Enrollment Request State Descriptions*

Certificate Enrollment State	Description
authorized	The certificate server has authorized the request.
denied	The certificate server has denied the request for policy reasons.
granted	The CA core has generated the appropriate certificate for the certificate request.
initial	The request has been created by the SCEP server.
malformed	The certificate server has determined that the request is invalid for cryptographic reasons.
pending	The enrollment request must be manually accepted by the network administrator.

### SCEP Enrollment

All SCEP requests are treated as new certificate enrollment requests, even if the request specifies a duplicate subject name or public key pair as a previous certificate request.

## Types of CA Servers: Subordinate and Registration Authorities (RAs)

CA servers have the flexibility to be configured as a subordinate certificate server or an RA-mode certificate server.

### Why Configure a Subordinate CA?

A subordinate certificate server provides all the same features as a root certificate server. The root RSA key pairs are extremely important in a PKI hierarchy, and it is often advantageous to keep them offline or archived. To support this requirement, PKI hierarchies allow for subordinate CAs that have been signed by the root authority. In this way, the root authority can be kept offline (except to issue occasional CRL updates), and the subordinate CA can be used during normal operation.

### Why Configure an RA-Mode Certificate Server?

A Cisco IOS certificate server can be configured to run in RA mode. An RA offloads authentication and authorization responsibilities from a CA. When the RA receives a SCEP or manual enrollment request, the administrator can either reject or grant it on the basis of local policy. If the request is granted, it will be forwarded to the issuing CA, and the CA will automatically generate the certificate and return it to the RA. The client can later retrieve the granted certificate from the RA.

An RA is the authority charged with recording or verifying some or all of the data required for the CA to issue certificates. In many cases the CA will undertake all of the RA functions itself, but where a CA operates over a wide geographical area or when there is security concern over exposing the CA to direct network access, it may be administratively advisable to delegate some of the tasks to an RA and leave the CA to concentrate on its primary tasks of signing certificates and CRLs.

## Automatic CA Certificate and Key Rollover

CAs—root CAs, subordinate CAs, and RA-mode CAs—like their clients, have certificates and key pairs with expiration dates that need to be reissued when the current certificate and key pair are about to expire. When a root CA's certificate and key pair are expiring it must generate a self-signed rollover certificate and key pair. If a subordinate CA or an RA-mode CA's certificate and key pair are expiring, it will request a rollover certificate and key pair from its superior CA, obtaining the superior CA's new self-signed rollover certificates at the same time. The CA must distribute the new CA rollover certificate and keys too all its peers. This process, called rollover, allows for continuous operation of the network while the CAs and their clients are switching from an expiring CA certificate and key pair to a new CA certificate and key pair.

Rollover relies on the PKI infrastructure requirements of trust relationships and synchronized clocks. The PKI trust relationships allow (1) the new CA certificate to be authenticated, and (2) the rollover to be accomplished automatically without the loss of security. Synchronized clocks allow the rollover to be coordinated throughout your network.

## Automatic CA Certificate Rollover: How It Works

The CA server must have rollover configured. All levels of CAs must be automatically enrolled and have **auto-rollover** enabled. CA clients support rollover automatically when automatically enrolled. For more information about clients and automatic rollover, see the section “[Automatic Certificate Enrollment](#)” in the chapter “Configuring Certificate Enrollment for a PKI”.

After CAs have rollover enabled and their clients are automatically enrolled, there are three stages to the automatic CA certificate rollover process.

### Stage One: Active CA Certificate and Key Pair Only

In stage one, there is an active CA certificate and key pair only.

**Stage Two: Rollover CA Certificate and Key Pair Generation and Distribution**

In stage two, the rollover CA certificate and key pair are generated and distributed. The superior CA generates a rollover certificate and key pair. After the CA successfully saves its active configuration, the CA is ready to respond to client requests for the rollover certificate and key pair. When the superior CA receives a request for the new CA certificate and key pair from a client, the CA responds by sending the the new rollover CA certificate and key pair to the requesting client. The clients store the rollover CA certificate and key pair.

**Note**

When a CA generates its rollover certificate and key pair, it must be able to save its active configuration. If the current configuration has been altered, saving of the rollover certificate and key pair will not happen automatically. In this case, the administrator must save the configuration manually or rollover information will be lost.

**Stage Three: Rollover CA Certificate and Key Pair Become the Active CA Certificate and Key Pair**

In stage three, the rollover CA certificate and key pair become the active CA certificate and key pair. All devices that have stored a valid rollover CA certificate rename the rollover certificate to the active certificate and the once-active certificate and key pair are deleted.

## How to Set Up and Deploy a Cisco IOS Certificate Server

This section contains the following procedures:

- [Generating a Certificate Server RSA Key Pair, page 10](#)
- [Configuring Certificate Servers, page 13](#)
- [Configuring Certificate Server Functionality, page 24](#)
- [Working with Automatic CA Certificate Rollover, page 28](#)
- [Maintaining, Verifying, and Troubleshooting the Certificate Server, Certificates, and the CA, page 30](#)

### Generating a Certificate Server RSA Key Pair

Perform this task to manually generate an RSA key pair for the certificate server. Manually generating a certificate server RSA key pair allows you to specify the type of key pair you want to generate, to create an exportable key pair for backup purposes, to specify the key pair storage location, or to specify the key generation location.

If you are running Cisco IOS Release 12.3(8)T or earlier releases, you may want to create an exportable certificate server key pair for backup, or archive purposes. If this task is not performed, the certificate server will automatically generate a key pair, which will not be marked as exportable. Automatic CA certificate archiving was introduced in Cisco IOS Release 12.3(11)T.

As of Cisco IOS Release 12.4(11)T and later releases, if your router has a USB token configured and available, the USB token can be used as cryptographic device in addition to a storage device. Using a USB token as a cryptographic device allows RSA operations such as key generation, signing, and authentication of credentials to be performed on a USB token. The private key never leaves the USB token and is not exportable. The public key is exportable. For titles of specific documents about configuring a USB token and making it available to use as a cryptographic device, see the [“The following sections provide references related to Cisco IOS certificate server.Related Documents”](#) section.



**Note**

It is recommended that the private key be kept in a secure location and that you regularly archive the certificate server database.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **crypto key generate rsa** [**general-keys** | **usage-keys** | **signature** | **encryption**] [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] [**storage** *devicename:*] [**on** *devicename:*]
4. **crypto key export rsa** *key-label* **pem** {**terminal** | **url** *url*} {**3des** | **des**} *passphrase*
5. **crypto key import rsa** *key-label* **pem** [**usage-keys** | **signature** | **encryption**] {**terminal** | **url** *url*} [**exportable**] [**on** *devicename:*] *passphrase*
6. **exit**
7. **show crypto key mypubkey rsa**

**DETAILED STEPS**

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto key generate rsa</b> [ <b>general-keys</b>   <b>usage-keys</b>   <b>signature</b>   <b>encryption</b> ] [ <b>label</b> <i>key-label</i> ] [ <b>exportable</b> ] [ <b>modulus</b> <i>modulus-size</i> ] [ <b>storage</b> <i>devicename:</i> ] [ <b>on</b> <i>devicename:</i> ]  <b>Example:</b> Router (config)# crypto key generate rsa label mycs exportable modulus 2048	<p>Generates the RSA key pair for the certificate server.</p> <p>When specifying a label name, you must use the same name for the label that you plan to use for the certificate server (via the <b>crypto pki server cs-label</b> command). By default, the fully qualified domain name (FQDN) of the router is used for the key label.</p> <p>If you manually generate the exportable RSA key pair but wait until after the CA certificate has been generated before issuing the <b>no shutdown</b> command, you can use the <b>crypto ca export pkcs12</b> command to export a PKCS12 file that contains the certificate server certificate and the private key.</p> <p>By default, the modulus size of a CA key is 1024 bits. The recommended modulus for a CA key is 2048 bits. The range for a CA key is from 350 to 2048 bits.</p>

	Command or Action	Purpose
Step 4	<b>crypto key export rsa</b> <i>key-label</i> <b>pem</b> [ <b>terminal</b>   <b>url</b> <i>url</i> ] { <b>3des</b>   <b>des</b> } <i>passphrase</i>  <b>Example:</b> Router (config)# <b>crypto key export rsa</b> mycs pem url nvram: 3des PASSWORD	(Optional) Exports the generated RSA key pair.  Allows you to export the generated keys.
Step 5	<b>crypto key import rsa</b> <i>key-label</i> <b>pem</b> [ <b>usage-keys</b>   <b>signature</b>   <b>encryption</b> ] { <b>terminal</b>   <b>url</b> <i>url</i> } [ <b>exportable</b> ] [ <b>on</b> <i>devicename:</i> ] <i>passphrase</i>  <b>Example:</b> Router (config)# <b>crypto key import rsa</b> mycs2 pem url nvram:mycs PASSWORD	(Optional) Imports RSA key pair.  To create the imported keys on a USB token, use the <b>on</b> keyword and specify the appropriate device location.  If you exported the RSA keys using the <b>exportable</b> keyword and you want to change the RSA key pair to nonexportable, import the key back to the certificate server without the <b>exportable</b> keyword. The key cannot be exported again.
Step 6	<b>exit</b>  <b>Example:</b> Router (config)# <b>exit</b>	Exits global configuration.
Step 7	<b>show crypto key mypubkey rsa</b>  <b>Example:</b> Router# <b>show crypto key mypubkey rsa</b>	Displays the RSA public keys of your router.

## Examples

The following example generates a general usage 1024-bit RSA key pair on a USB token with the label “ms2” with crypto engine debugging messages shown:

```
Router(config)# crypto key generate rsa on usbtoken0 label ms2 modulus 1024
The name for the keys will be: ms2
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be on-token, non-exportable...
Jan 7 02:41:40.895: crypto_engine: Generate public/private keypair [OK]
Jan 7 02:44:09.623: crypto_engine: Create signature
Jan 7 02:44:10.467: crypto_engine: Verify signature
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_CREATE_PUBKEY(hw) (ipsec)
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_PUB_DECRYPT(hw) (ipsec)
```

Now, the on-token keys labeled “ms2” may be used for enrollment.

The following example shows the successful import of an encryption key to a configured and available USB tokens:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# crypto key import rsa encryption on usbtoken0 url nvram:e password
% Importing public Encryption key or certificate PEM file...
filename [e-encr.pub]?
Reading file from nvram:e-encr.pub
% Importing private Encryption key PEM file...
Source filename [e-encr.prv]?
Reading file from nvram:e-encr.prv
% Key pair import succeeded.
```

## Configuring Certificate Servers

The following tasks explain how to configure a certificate server, a subordinate certificate server, or an RA-mode certificate server, and how to enable automatic rollover.

- [Configuring a Certificate Server, page 13](#)
- [Configuring a Subordinate Certificate Server, page 15](#)
- [Configuring a Certificate Server to Run in RA Mode, page 21](#)
- [Configuring the Root Certificate Server to Delegate Enrollment Tasks to the RA Mode Certificate Server, page 23](#)

### Prerequisites for Automatic CA Certificate Rollover

When configuring a certificate server, for automatic CA certificate rollover to run successfully, the following prerequisites are applicable for your CA servers:

- You must be running Cisco IOS Release 12.4(2)T or a later release on your CA servers.
- Your CA server must be enabled and fully configured with a reliable time of day, an available key pair, a self-signed, valid CA certificate associated with the key pair, a CRL, an accessible storage device, and an active HTTP/SCEP server.
- CA clients must have successfully completed automatic enrollment and have autoenrollment enabled with the same certificate server.

**Note**

If you are running Cisco IOS 12.4(2)T or earlier releases, only your root CA will support automatic CA certificate rollover functionality. Cisco IOS 12.4(4)T or later releases support all CAs—root CAs, subordinate CAs, and RA-mode CAs.

### Restrictions for Automatic CA Certificate Rollover

When configuring a certificate server, in order for automatic CA certificate rollover to run successfully, the following restrictions are applicable:

- SCEP must be used to support rollover. Any device that enrolls with the PKI using an alternative to SCEP as the certificate management protocol or mechanism (such as enrollment profiles, manual enrollment, or TFTP enrollment) will not be able to take advantage of the rollover functionality provided by SCEP.
- If you have automatic archive configured on your network and the archive fails, rollover will not occur because the certificate server will not enter the rollover state, and the rollover certificate and key pair will not be automatically saved.

### Configuring a Certificate Server

Perform this task to configure a Cisco IOS certificate server and enable automatic rollover.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **ip http server**
4. **crypto pki server** *cs-label*
5. **no shutdown**
6. **auto-rollover** [*time-period*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip http server</b>  <b>Example:</b> Router(config)# ip http server	Enables the HTTP server on your system.
Step 4	<b>crypto pki server</b> <i>cs-label</i>  <b>Example:</b> Router(config)# crypto pki server server-pki	Defines a label for the certificate server and enters certificate server configuration mode. <p><b>Note</b> If you manually generated an RSA key pair, the <i>cs-label</i> argument must match the name of the key pair.</p>
Step 5	<b>no shutdown</b>  <b>Example:</b> Router(cs-server)# no shutdown	(Optional) Enables the certificate server. <p><b>Note</b> Only use this command at this point if you want to use the preconfigured default functionality. That is, do not issue this command just yet if you plan to change any of the default settings as shown in the task <a href="#">“Configuring Certificate Server Functionality.”</a></p>
Step 6	<b>auto-rollover</b> [ <i>time-period</i> ]  <b>Example:</b> Router(cs-server)# auto-rollover 90	(Optional) Enables the automated CA certificate rollover functionality. <ul style="list-style-type: none"> <li><i>time-period</i>—default is 30 days.</li> </ul>

## Examples

The following example shows how to configure the certificate server “ca”:

```
Router(config)# crypto pki server ca
Router(cs-server)# no shutdown
```

```
% Once you start the server, you can no longer change some of
% the configuration.
Are you sure you want to do this? [yes/no]: yes
% Generating 1024 bit RSA keys ...[OK]
```

```
% Certificate Server enabled.
Router(cs-server)# end
!
Router# show crypto pki server

Certificate Server ca:
 Status: enabled, configured
 CA cert fingerprint: 5A856122 4051347F 55E8C246 866D0AC3
 Granting mode is: manual
 Last certificate issued serial number: 0x1
 CA certificate expiration timer: 19:44:57 GMT Oct 14 2006
 CRL NextUpdate timer: 19:45:25 GMT Oct 22 2003
 Current storage dir: nvram:
 Database Level: Complete - all issued certs written as <serialnum>.cer
```

The following example shows how to enable automated CA certificate rollover on the server mycs with the **auto-rollover** command. The **show crypto pki server** command shows that the automatic rollover has been configured on the server mycs with an overlap period of 25 days.

```
Router(config)# crypto pki server mycs
Router(cs-server)# auto-rollover 25
Router(cs-server)# no shut

%Some server settings cannot be changed after CA certificate generation.
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
% Exporting Certificate Server signing certificate and keys...

% Certificate Server enabled.
Router(cs-server)#

Router# show crypto pki server

Certificate Server mycs:
 Status:enabled
 Server's configuration is locked (enter "shut" to unlock it)
 Issuer name:CN=mycs
 CA cert fingerprint:70AFECA9 211CDDCC 6AA9D7FF 3ADB03AE
 Granting mode is:manual
 Last certificate issued serial number:0x1
 CA certificate expiration timer:00:49:26 PDT Jun 20 2008
 CRL NextUpdate timer:00:49:29 PDT Jun 28 2005
 Current storage dir:nvram:
 Database Level:Minimum - no cert data written to storage
 Auto-Rollover configured, overlap period 25 days
 Autorollover timer:00:49:26 PDT May 26 2008
```

## Configuring a Subordinate Certificate Server

Perform this task to configure a subordinate certificate server to grant all or certain SCEP or manual certificate requests and to enable automatic rollover.

### Restrictions

- You must be running Cisco IOS Release 12.3(14)T or a later release. (Versions prior to Cisco IOS software Release 12.3(14)T support only one certificate server and no hierarchy; that is, subordinate certificate servers are not supported.)
- The root certificate server should be a Cisco IOS certificate server.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment url** *url*
5. **exit**
6. **crypto pki server** *cs-label*
7. **issuer name** *DN-string*
8. **mode sub-cs**
9. **auto-rollover** [*time-period*]
10. **grant auto rollover** {*ca-cert* | *ra-cert*}
11. **no shutdown**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto pki trustpoint</b> <i>name</i>  <b>Example:</b> Router (config)# crypto pki trustpoint sub	Declares the trustpoint that your subordinate certificate server should use and enters ca-trustpoint configuration mode.
Step 4	<b>enrollment url</b> <i>url</i>  <b>Example:</b> Router (ca-trustpoint)# enrollment url http://192.0.2.6	Specifies the enrollment URL of the issuing CA certificate server (root certificate server).
Step 5	<b>exit</b>  <b>Example:</b> Router (ca-trustpoint)# exit	Exits ca-trustpoint configuration mode.
Step 6	<b>crypto pki server</b> <i>cs-label</i>  <b>Example:</b> Router(config)# crypto pki server sub	Enables a Cisco IOS certificate server and enters cs-server configuration mode.  <b>Note</b> The subordinate server must have the same name as the trustpoint that was created in Step 3 above.

	Command or Action	Purpose
Step 7	<b>issuer name</b> <i>DN-string</i>  <b>Example:</b> Router(cs-server)# issuer-name CN=sub CA, O=Cisco, C=us	(Optional) Specifies the DN as the CA issuer name for the certificate server.
Step 8	<b>mode sub-cs</b>  <b>Example:</b> Router(cs-server)# mode sub-cs	Places the PKI server into sub-certificate server mode.
Step 9	<b>auto-rollover</b> [ <i>time-period</i> ]  <b>Example:</b> Router(cs-server)# auto-rollover 90	(Optional) Enables the automated CA certificate rollover functionality. <ul style="list-style-type: none"> <li><i>time-period</i>—default is 30 days.</li> </ul>
Step 10	<b>grant auto rollover</b> { <b>ca-cert</b>   <b>ra-cert</b> }  <b>Example:</b> Router(cs-server)# grant auto rollover ca-cert	(Optional) Automatically grants reenrollment requests for subordinate CAs and RA-mode CAs without operator intervention. <ul style="list-style-type: none"> <li><b>ca-cert</b>—Specifies that the subordinate CA rollover certificate will be automatically granted.</li> <li><b>ra-cert</b>—Specifies that the RA-mode CA rollover certificate will be automatically granted.</li> </ul> <b>Note</b> If this is the first time that a subordinate certificate server is enabled and enrolled, the certificate request must be manually granted.
Step 11	<b>no shutdown</b>  <b>Example:</b> Router(cs-server)# no shutdown	Enables or reenables the certificate server.  If this is the first time that a subordinate certificate server is enabled, the certificate server will generate the key and obtain its signing certificate from the root certificate server.

## Examples

If the certificate server fails to enable or if the certificate server has trouble handling the request that has been configured, you can use the **debug crypto pki server** command to troubleshoot your configuration as shown in the following examples (Clock Not Set and Trustpoint Not Configured):

```
Router# debug crypto pki server
```

### Clock Not Set

```
Router (config)# crypto pki server sub
Router (cs-server)# mode sub-cs
Router (cs-server)# no shutdown
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key % or type Return to exit
Password:
*Jan 6 20:57:37.667: CRYPTO_CS: enter FSM: input state initial, input signal no shut

Re-enter password:
% Generating 1024 bit RSA keys ...
```

```
*Jan 6 20:57:45.303: CRYPTO_CS: starting enabling checks
*Jan 6 20:57:45.303: CRYPTO_CS: key 'sub' does not exist; generated automatically[OK]
% Time has not been set. Cannot start the Certificate server
```

### Trustpoint Not Configured

```
Router (config)# crypto pki server sub
Router (cs-server)# mode sub-cs
Router (cs-server)# no shutdown

%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key or type Return to exit
Password:
Jan 6 21:00:15.961: CRYPTO_CS: enter FSM: input state initial, input signal no shut.
Jan 6 21:03:34.309: CRYPTO_CS: enter FSM: input state initial, input signal time set.
Jan 6 21:03:34.313: CRYPTO_CS: exit FSM: new state initial.
Jan 6 21:03:34.313: CRYPTO_CS: cs config has been unlocked
Re-enter password:
% Generating 1024 bit RSA keys ...
Jan 6 21:03:44.413: CRYPTO_CS: starting enabling checks
Jan 6 21:03:44.413: CRYPTO_CS: associated trust point 'sub' does not exist; generated
automatically
Jan 6 21:03:44.417: CRYPTO_CS: key 'sub' does not exist; generated automatically[OK]

Jan 6 21:04:03.993: CRYPTO_CS: nvram filesystem
Jan 6 21:04:04.077: CRYPTO_CS: serial number 0x1 written.
You must specify an enrollment URL for this CA before you can authenticate it.
% Failed to authenticate the Certificate Authority
```

If the certificate server fails to obtain its signing certificate from the root certificate server, you can use the **debug crypto pki transactions** command to troubleshoot your configuration as shown in the following example:

```
Router# debug crypto pki transactions

Jan 6 21:07:00.311: CRYPTO_CS: enter FSM: input state initial, input signal time set
Jan 6 21:07:00.311: CRYPTO_CS: exit FSM: new state initial
Jan 6 21:07:00.311: CRYPTO_CS: cs config has been unlocked no sh
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key % or type Return to exit
Password:
Jan 6 21:07:03.535: CRYPTO_CS: enter FSM: input state initial, input signal no shut
Re-enter password:
% Generating 1024 bit RSA keys ...
Jan 6 21:07:10.619: CRYPTO_CS: starting enabling checks
Jan 6 21:07:10.619: CRYPTO_CS: key 'sub' does not exist; generated automatically[OK]

Jan 6 21:07:20.535: %SSH-5-ENABLED: SSH 1.99 has been enabled
Jan 6 21:07:25.883: CRYPTO_CS: nvram filesystem
Jan 6 21:07:25.991: CRYPTO_CS: serial number 0x1 written.
Jan 6 21:07:27.863: CRYPTO_CS: created a new serial file.
Jan 6 21:07:27.863: CRYPTO_CS: authenticating the CA 'sub'
Jan 6 21:07:27.867: CRYPTO_PKI: Sending CA Certificate Request:
GET /cgi-bin/pkiclient.exe?operation=GetCACert&message=sub HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI)

Jan 6 21:07:27.867: CRYPTO_PKI: can not resolve server name/IP address
Jan 6 21:07:27.871: CRYPTO_PKI: Using unresolved IP Address 192.0.2.6 Certificate has the
following attributes:
 Fingerprint MD5: 328ACC02 52B25DB8 22F8F104 B6055B5B
 Fingerprint SHA1: 02FD799D DD40C7A8 61DC53AB 1E89A3EA 2A729EE2

% Do you accept this certificate? [yes/no]:
Jan 6 21:07:30.879: CRYPTO_PKI: http connection opened
```



```
Jan 6 21:07:30.903: CRYPTO_PKI: HTTP response header:
 HTTP/1.1 200 OK
Date: Thu, 06 Jan 2005 21:07:30 GMT
Server: server-IOS
Content-Type: application/x-x509-ca-cert
Expires: Thu, 06 Jan 2005 21:07:30 GMT
Last-Modified: Thu, 06 Jan 2005 21:07:30 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Accept-Ranges: none

Content-Type indicates we have received a CA certificate.

Jan 6 21:07:30.903: Received 507 bytes from server as CA certificate:
Jan 6 21:07:30.907: CRYPTO_PKI: transaction GetCACert completed
Jan 6 21:07:30.907: CRYPTO_PKI: CA certificate received.
Jan 6 21:07:30.907: CRYPTO_PKI: CA certificate received.
Jan 6 21:07:30.927: CRYPTO_PKI: crypto_pki_authenticate_tp_cert()

Jan 6 21:07:30.927: CRYPTO_PKI: trustpoint sub authentication status = 0 y Trustpoint CA
certificate accepted.%

% Certificate request sent to Certificate Authority

% Enrollment in progress...
Router (cs-server)#
Jan 6 21:07:51.772: CRYPTO_CA: certificate not found
Jan 6 21:07:51.772: CRYPTO_CA: certificate not found
Jan 6 21:07:52.460: CRYPTO_CS: Publishing 213 bytes to crl file nvram:sub.crl
Jan 6 21:07:54.348: CRYPTO_CS: enrolling the server's trustpoint 'sub'
Jan 6 21:07:54.352: CRYPTO_CS: exit FSM: new state check failed
Jan 6 21:07:54.352: CRYPTO_CS: cs config has been locked
Jan 6 21:07:54.356: CRYPTO_PKI: transaction PKCSReq completed
Jan 6 21:07:54.356: CRYPTO_PKI: status:
Jan 6 21:07:55.016: CRYPTO_PKI: Certificate Request Fingerprint MD5: 1BA027DB 1C7860C7
EC188F65 64356C80
Jan 6 21:07:55.016: CRYPTO_PKI: Certificate Request Fingerprint SHA1: 840DB52C E17614CB
0C7BE187 0DFC884D D32CAA75
Jan 6 21:07:56.508: CRYPTO_PKI: can not resolve server name/IP address
Jan 6 21:07:56.508: CRYPTO_PKI: Using unresolved IP Address 192.0.2.6
Jan 6 21:07:56.516: CRYPTO_PKI: http connection opened
Jan 6 21:07:59.136: CRYPTO_PKI: received msg of 776 bytes
Jan 6 21:07:59.136: CRYPTO_PKI: HTTP response header:
 HTTP/1.1 200 OK
Date: Thu, 06 Jan 2005 21:07:57 GMT
Server: server-IOS
Content-Type: application/x-pki-message
Expires: Thu, 06 Jan 2005 21:07:57 GMT
Last-Modified: Thu, 06 Jan 2005 21:07:57 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Accept-Ranges: none

Jan 6 21:07:59.324: The PKCS #7 message has 1 verified signers.
Jan 6 21:07:59.324: signing cert: issuer=cn=root1
Jan 6 21:07:59.324: Signed Attributes:

Jan 6 21:07:59.328: CRYPTO_PKI: status = 102: certificate request pending
Jan 6 21:08:00.788: CRYPTO_PKI: can not resolve server name/IP address
Jan 6 21:08:00.788: CRYPTO_PKI: Using unresolved IP Address 192.0.2.6
Jan 6 21:08:00.796: CRYPTO_PKI: http connection opened
Jan 6 21:08:11.804: CRYPTO_PKI: received msg of 776 bytes
Jan 6 21:08:11.804: CRYPTO_PKI: HTTP response header: HTTP/1.1 200 OK
```

```

Date: Thu, 06 Jan 2005 21:08:01 GMT
Server: server-IOS
Content-Type: application/x-pki-message
Expires: Thu, 06 Jan 2005 21:08:01 GMT
Last-Modified: Thu, 06 Jan 2005 21:08:01 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Accept-Ranges: none

```

```

Jan 6 21:08:11.992: The PKCS #7 message has 1 verified signers.
Jan 6 21:08:11.992: signing cert: issuer=cn=root1
Jan 6 21:08:11.996: Signed Attributes:

```

```

Jan 6 21:08:11.996: CRYPTO_PKI: status = 102: certificate request pending
Jan 6 21:08:21.996: CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan 6 21:08:31.996: CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan 6 21:08:41.996: CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan 6 21:08:51.996: CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan 6 21:09:01.996: CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan 6 21:09:11.996: CRYPTO_PKI: resend GetCertInitial, 1
Jan 6 21:09:11.996: CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan 6 21:09:11.996: CRYPTO_PKI: resend GetCertInitial for session: 0
Jan 6 21:09:11.996: CRYPTO_PKI: can not resolve server name/IP address
Jan 6 21:09:11.996: CRYPTO_PKI: Using unresolved IP Address 192.0.2.6
Jan 6 21:09:12.024: CRYPTO_PKI: http connection opened% Exporting Certificate Server
signing certificate and keys...

```

```

Jan 6 21:09:14.784: CRYPTO_PKI: received msg of 1611 bytes
Jan 6 21:09:14.784: CRYPTO_PKI: HTTP response header:
HTTP/1.1 200 OK
Date: Thu, 06 Jan 2005 21:09:13 GMT
Server: server-IOS
Content-Type: application/x-pki-message
Expires: Thu, 06 Jan 2005 21:09:13 GMT
Last-Modified: Thu, 06 Jan 2005 21:09:13 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Accept-Ranges: none

```

```

Jan 6 21:09:14.972: The PKCS #7 message has 1 verified signers.
Jan 6 21:09:14.972: signing cert: issuer=cn=root1
Jan 6 21:09:14.972: Signed Attributes:

```

```

Jan 6 21:09:14.976: CRYPTO_PKI: status = 100: certificate is granted
Jan 6 21:09:15.668: The PKCS #7 message contains 1 certs and 0 crls.
Jan 6 21:09:15.688: Newly-issued Router Cert: issuer=cn=root serial=2
Jan 6 21:09:15.688: start date: 21:08:03 GMT Jan 6 2005
Jan 6 21:09:15.688: end date: 21:08:03 GMT Jan 6 2006
Jan 6 21:09:15.688: Router date: 21:09:15 GMT Jan 6 2005
Jan 6 21:09:15.692: Received router cert from CA
Jan 6 21:09:15.740: CRYPTO_CA: certificate not found
Jan 6 21:09:15.744: CRYPTO_PKI: All enrollment requests completed for trustpoint sub.
Jan 6 21:09:15.744: %PKI-6-CERTRET: Certificate received from Certificate Authority
Jan 6 21:09:15.744: CRYPTO_PKI: All enrollment requests completed for trustpoint sub.
Jan 6 21:09:15.744: CRYPTO_PKI: All enrollment requests completed for trustpoint sub.
Jan 6 21:09:15.748: CRYPTO_CS: enter FSM: input state check failed, input signal cert
configured
Jan 6 21:09:15.748: CRYPTO_CS: starting enabling checks
Jan 6 21:09:15.748: CRYPTO_CS: nvram filesystem
Jan 6 21:09:15.796: CRYPTO_CS: found existing serial file.
Jan 6 21:09:15.820: CRYPTO_CS: old router cert flag 0x4
Jan 6 21:09:15.820: CRYPTO_CS: new router cert flag 0x44

```

```

Jan 6 21:09:18.432: CRYPTO_CS: DB version 1
Jan 6 21:09:18.432: CRYPTO_CS: last issued serial number is 0x1
Jan 6 21:09:18.480: CRYPTO_CS: CRL file sub.crl exists.
Jan 6 21:09:18.480: CRYPTO_CS: Read 213 bytes from crl file sub.crl.
Jan 6 21:09:18.532: CRYPTO_CS: SCEP server started
Jan 6 21:09:18.532: CRYPTO_CS: exit FSM: new state enabled
Jan 6 21:09:18.536: CRYPTO_CS: cs config has been locked
Jan 6 21:09:18.536: CRYPTO_PKI: All enrollment requests completed for trustpoint sub.

```

If the certificate server fails to enable or if the certificate server has trouble handling the request that has been configured, you can use the **debug crypto pki server** command to troubleshoot the progress of an enrollment. This command can also be used to debug the root CA (turn it on at the root CA).

## Configuring a Certificate Server to Run in RA Mode

### Restrictions for Configuring a Certificate Server for RA Mode

When the Cisco IOS certificate server is acting as an RA, the issuing CA should be a Cisco IOS certificate server.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment url** *url*
5. **subject-name** *x.500-name*
6. **exit**
7. **crypto pki server** *cs-label*
8. **mode ra**
9. **auto-rollover** [*time-period*]
10. **grant auto rollover** {*ca-cert* | *ra-cert*}
11. **no shutdown**
12. **no shutdown**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<b>crypto pki trustpoint</b> <i>name</i>  <b>Example:</b> Router (config)# crypto pki trustpoint ra-server	Declares the trustpoint that your RA mode certificate server should use and enters ca-trustpoint configuration mode.
Step 4	<b>enrollment url</b> <i>url</i>  <b>Example:</b> Router (ca-trustpoint)# enrollment url http://ca-server.company.com	Specifies the enrollment URL of the issuing CA certificate server (root certificate server).
Step 5	<b>subject-name</b> <i>x.500-name</i>  <b>Example:</b> Router (ca-trustpoint)# subject-name cn=ioscs RA	(Optional) Specifies the subject name the RA will use.  <b>Note</b> Include “cn=ioscs RA” or “ou=ioscs RA” in the subject name so that the issuing CA certificate server can recognize the RA (see Step 7 below).
Step 6	<b>exit</b>  <b>Example:</b> Router (ca-trustpoint)# exit	Exits ca-trustpoint configuration mode.
Step 7	<b>crypto pki server</b> <i>cs-label</i>  <b>Example:</b> Router(config)# crypto pki server ra-server	Enables a Cisco IOS certificate server and enters cs-server configuration mode.  <b>Note</b> The certificate server must have the same name as the trustpoint that was created in Step 3 above.
Step 8	<b>mode ra</b>  <b>Example:</b> Router(cs-server)# mode ra	Places the PKI server into RA certificate server mode.
Step 9	<b>auto-rollover</b> [ <i>time-period</i> ]  <b>Example:</b> Router(cs-server)# auto-rollover 90	(Optional) Enables the automatic CA certificate rollover functionality. <ul style="list-style-type: none"> <li><i>time-period</i>—default is 30 days.</li> </ul>
Step 10	<b>grant auto rollover</b> { <b>ca-cert</b>   <b>ra-cert</b> }  <b>Example:</b> Router(cs-server)# grant auto rollover ra-cert	(Optional) Automatically grants reenrollment requests for subordinate CAs and RA-mode CAs without operator intervention. <ul style="list-style-type: none"> <li><b>ca-cert</b>—Specifies that the subordinate CA rollover certificate will be automatically granted.</li> <li><b>ra-cert</b>—Specifies that the RA-mode CA rollover certificate will be automatically granted.</li> </ul> If this is the first time that a subordinate certificate server is enabled and enrolled, the certificate request must be manually granted.

	Command or Action	Purpose
Step 11	<b>no shutdown</b>  <b>Example:</b> Router(cs-server)# no shutdown	Enables the certificate server.  <b>Note</b> After this command is issued, the RA will automatically enroll with the root certificate server.  After the RA certificate has been successfully received, you must issue the <b>no shutdown</b> command again, which reenables the certificate server.
Step 12	<b>no shutdown</b>  <b>Example:</b> Router(cs-server)# no shutdown	Reenables the certificate server.

## Configuring the Root Certificate Server to Delegate Enrollment Tasks to the RA Mode Certificate Server

Perform the following steps on the router that is running the issuing certificate server; that is, configure the root certificate server that is delegating enrollment tasks to the RA mode certificate server.



### Note

Granting enrollment requests for an RA is essentially the same process as granting enrollment requests for client devices—except that enrollment requests for an RA are displayed in the section “RA certificate requests” of the command output for the **crypto pki server info-requests** command.

## SUMMARY STEPS

1. **enable**
2. **crypto pki server** *cs-label* **info requests**
3. **crypto pki server** *cs-label* **grant req-id**
4. **configure terminal**
5. **crypto pki server** *cs-label*
6. **grant ra-auto**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>crypto pki server</b> <i>cs-label</i> <b>info requests</b>  <b>Example:</b> Router# crypto pki server root-server info requests	Displays the outstanding RA certificate request.  <b>Note</b> This command is issued on the router that is running the issuing certificate server.

	Command or Action	Purpose
Step 3	<b>crypto pki server</b> <i>cs-label</i> <b>grant</b> <i>req-id</i>  <b>Example:</b> Router# <b>crypto pki server</b> root-server <b>grant</b> 9	Grants the pending RA certificate request.  <b>Note</b> Because the issuing certificate server will delegate the enrollment request verification task to the RA, you must pay extra attention to the RA certificate request before granting it.
Step 4	<b>configure terminal</b>  <b>Example:</b> Router# <b>configure terminal</b>	Enters global configuration mode.
Step 5	<b>crypto pki server</b> <i>cs-label</i>  <b>Example:</b> Router (config)# <b>crypto pki server</b> root-server	Enables a Cisco IOS certificate server and enters cs-server configuration mode.
Step 6	<b>grant ra-auto</b>  <b>Example:</b> Router(cs-server)# <b>grant ra-auto</b>	(Optional) Specifies that all enrollment requests from an RA are to be granted automatically.  <b>Note</b> For the <b>grant ra-auto</b> command to work, you have to include “cn=ioscs RA” or “ou=ioscs RA” in the subject name of the RA certificate. (See Step 2 above.)

## What to Do Next

After you have configured a certificate server, you can use the preconfigured default values or specify values via the CLI for the functionality of the certificate server. If you choose to specify values other than the defaults, see the following section, “[Configuring Certificate Server Functionality](#).”

## Configuring Certificate Server Functionality

After you have enabled a certificate server and are in certificate server configuration mode, use any of the steps in this task to configure basic certificate server functionality values other than the default values.

### Certificate Server Default Values and Recommended Values

The default values for a certificate server are intended to address a relatively small network (of about ten devices). For example, the database settings are minimal (via the **database level minimal** command) and the certificate server handles all CRL requests via SCEP. For larger networks, it is recommended that you use either the database setting “names” or “complete” (as described in the **database level** command) for possible audit and revocation purposes. Depending on the CRL checking policy, you should also use an external CDP in a larger network.

## Certificate Server File Storage and Publication Locations

You have the flexibility to store file types to different storage and publication locations.

### SUMMARY STEPS

1. **database url** *root-url*
2. **database url** {*cnm* | *crl* | *crt* | **p12** | **pem** | **ser**} *root-url*
3. **database url** {*cnm* | *crl* | *crt*} **publish** *root-url*
4. **database level** {*minimal* | *names* | **complete**}
5. **database username** *username* [**password** [*encr-type*] *password*]
6. **database archive** {**pkcs12** | **pem**} [**password** [*encr-type*] *password*]
7. **issuer-name** *DN-string*
8. **lifetime** {*ca-certificate* | *certificate*} *time*
9. **lifetime crl** *time*
10. **lifetime enrollment-request** *time*
11. **cdp-url** *url*
12. **no shutdown**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>database url</b> <i>root-url</i>  <b>Example:</b> Router (cs-server)# database url tftp://cert-svr-db.company.com	Specifies the primary location where database entries for the certificate server will be written out.  If this command is not specified, all database entries will be written to NVRAM.
Step 2	<b>database url</b> { <i>cnm</i>   <i>crl</i>   <i>crt</i>   <b>p12</b>   <b>pem</b>   <b>ser</b> } <i>root-url</i>  <b>Example:</b> Router (cs-server)# database url ser nvram:	Specifies certificate server critical file storage location by file type.  <b>Note</b> If this command is not specified, all critical files will be stored to the primary location if specified. If the primary location is not specified, all critical files will be stored to NVRAM.
Step 3	<b>database url</b> { <i>cnm</i>   <i>crl</i>   <i>crt</i> } <b>publish</b> <i>root-url</i>  <b>Example:</b> Router (cs-server)# database url crl publish tftp://csdb_specific_crl_files.company.com	Specifies certificate server publish location by file type.  <b>Note</b> If this command is not specified, all publish files will be stored to the primary location if specified. If the primary location is not specified, all publish files will be stored to NVRAM.

	Command or Action	Purpose
Step 4	<p><b>database level</b> {<b>minimal</b>   <b>names</b>   <b>complete</b>}</p> <p><b>Example:</b> Router (cs-server)# database level complete</p>	<p>Controls what type of data is stored in the certificate enrollment database.</p> <ul style="list-style-type: none"> <li><b>minimal</b>—Enough information is stored only to continue issuing new certificates without conflict; the default value.</li> <li><b>names</b>—In addition to the information given in the minimal level, the serial number and subject name of each certificate.</li> <li><b>complete</b>—In addition to the information given in the minimal and names levels, each issued certificate is written to the database.</li> </ul> <p><b>Note</b> The <b>complete</b> keyword produces a large amount of information; if it is issued, you should also specify an external TFTP server in which to store the data via the <b>database url</b> command.</p>
Step 5	<p><b>database username</b> <i>username</i> [<b>password</b> [<i>encr-type</i>] <i>password</i>]</p> <p><b>Example:</b> Router (cs-server)# database username user password PASSWORD</p>	<p>(Optional) Sets a username and password when a user is required to access a primary certificate enrollment database storage location.</p>
Step 6	<p><b>database archive</b> {<b>pkcs12</b>   <b>pem</b>} [<b>password</b> [<i>encr-type</i>] <i>password</i>]</p> <p><b>Example:</b> Router (cs-server)# database archive pem</p>	<p>(Optional) Sets the CA key and CA certificate archive format and password to encrypt the file.</p> <p>The default value is <b>pkcs12</b>, so if this subcommand is not configured, autoarchiving will still be done, and the PKCS12 format will be used.</p> <ul style="list-style-type: none"> <li>The password is optional. If it is not configured, you will be prompted for the password when the server is turned on for the first time.</li> </ul> <p><b>Note</b> It is recommended that you remove the password from the configuration after the archive is finished.</p>
Step 7	<p><b>issuer-name</b> <i>DN-string</i></p> <p><b>Example:</b> Router (cs-server)# issuer-name my-server</p>	<p>(Optional) Sets the CA issuer name to the specified distinguished name (<i>DN-string</i>). The default value is as follows: <b>issuer-name cn={cs-label}</b>.</p>
Step 8	<p><b>lifetime</b> {<b>ca-certificate</b>   <b>certificate</b>} <i>time</i></p> <p><b>Example:</b> Router (cs-server)# lifetime certificate 888</p>	<p>(Optional) Specifies the lifetime, in days, of a CA certificate or a certificate.</p> <p>Valid values range from 1 day to 1825 days. The default CA certificate lifetime is 3 years; the default certificate lifetime is 1 year. The maximum certificate lifetime is 1 month less than the lifetime of the CA certificate.</p>
Step 9	<p><b>lifetime crl</b> <i>time</i></p> <p><b>Example:</b> Router (cs-server)# lifetime crl 333</p>	<p>(Optional) Defines the lifetime, in hours, of the CRL that is used by the certificate server.</p> <p>Maximum lifetime value is 336 hours (2 weeks). The default value is 168 hours (1 week).</p>



	Command or Action	Purpose
Step 10	<b>lifetime enrollment-request</b> <i>time</i>  <b>Example:</b> Router (cs-server)# lifetime enrollment-request 888	(Optional) Specifies how long an enrollment request should stay in the enrollment database before being removed.  Maximum lifetime is 1000 hours.
Step 11	<b>cdp-url</b> <i>url</i>  <b>Example:</b> Router (cs-server)# cdp-url http://my-cdp.company.com	(Optional) Defines the CDP location to be used in the certificates that are issued by the certificate server. <ul style="list-style-type: none"> <li>The URL must be an HTTP URL.</li> </ul> If you have PKI clients that are not running Cisco IOS software and that do not support a SCEP GetCRL request, use the following URL format: http://server.company.com/certEnroll/filename.crl Or, if your Cisco IOS certificate server is also configured as your CDP, use the following URL format http://cs-addr/cgi-bin/pkiclient.exe?operation=GetCRL where <i>cs-addr</i> is the location of the certificate server.  <b>Note</b> Although this command is optional, it is strongly recommended for any deployment scenario.
Step 12	<b>no shutdown</b>  <b>Example:</b> Router (cs-server)# no shutdown	Enables the certificate server.  You should issue this command only after you have completely configured your certificate server.

## Examples

The following example shows how to configure a CDP location where the PKI clients do not support SCEP GetCRL requests:

```
Router(config)# crypto pki server aaa
Router(cs-server)# database level minimum
Router(cs-server)# database url tftp://10.1.1.1/username1/
Router(cs-server)# issuer-name CN=aaa
Router(cs-server)# cdp-url http://server.company.com/certEnroll/aaa.crl
```

After a certificate server has been enabled on a router, the **show crypto pki server** command displays the following output:

```
Router# show crypto pki server

Certificate Server status:enabled, configured
Granting mode is:manual
Last certificate issued serial number:0x1
CA certificate expiration timer:19:31:15 PST Nov 17 2006
CRL NextUpdate timer:19:31:15 PST Nov 25 2003
Current storage dir:nvram:
Database Level:Minimum - no cert data written to storage
```

## Working with Automatic CA Certificate Rollover

This section describes different methods of initiating automatic CA certificate rollover on the server and obtaining rollover certificates. Use the following tasks as appropriate:

- [Starting Automated CA Certificate Rollover Immediately, page 28](#)
- [Requesting a Certificate Server Client's Rollover Certificate, page 28](#)
- [Exporting a CA Rollover Certificate, page 29](#)

### Starting Automated CA Certificate Rollover Immediately

Use this task to initiate the automated CA certificate rollover process immediately on your root CA server.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki server *cs-label* [rollover [cancel]]**

#### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto pki server <i>cs-label</i> [rollover [cancel]]</b>  <b>Example:</b> Router(config)# crypto pki server mycs rollover	Immediately starts the CA certificate rollover process by generating a shadow CA certificate.  To delete the CA certificate rollover certificate and keys, use the <b>cancel</b> keyword.

### Requesting a Certificate Server Client's Rollover Certificate

Use this task to request a certificate server client's rollover certificate.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki server *cs-label* [rollover request pkcs10 terminal]**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto pki server cs-label [rollover request pkcs10 terminal]</b>  <b>Example:</b> Router(config)# crypto pki server mycs rollover request pkcs10 terminal	Requests a client rollover certificate from the server.

## Examples

The following example shows a rollover certificate request being inputted into the server:

```
Router# crypto pki server mycs rollover request pkcs10 terminal

% Enter Base64 encoded or PEM formatted PKCS10 enrollment request.

% End with a blank line or "quit" on a line by itself.

-----BEGIN CERTIFICATE REQUEST-----

MIIBUTCBuwIBADASMRawDgYDVQQDEwdOZXdsb290MIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDMHeev1ERSs320zbLQQk+3lhV/R2HpYQ/im6uT1jkJf5iy0UPR
wF/Xl6yUNmG+ObiGiW9fsASF0nxZw+f07d2X2yh1PakfvF2wbP27C/sgJNOw9uPf
sBxEc40Xe0d5FMh0YKOSASHfZYKOflnyQR2Drmm2x/33QGo15QyRvjkeWQIDAQAB
oAAwDQYJKoZIhvcNAQEEBQADgYEALM90r4d79X6vxhD0qjuYJXfBCOvv4FNyFsjr
aBS/y6CnNVYySF8UBUohXYIGTWf4I4+s6i8gYfoFUW1/L82djS18TLrUr6wpCOs
RqfAfps7HW1e4cizOfjAUU+C7lNcobCAhwF1o6q2nIEjpQ/2yfk907sb3SCJZBfe
eW3tyCo=

-----END CERTIFICATE REQUEST-----
```

## Exporting a CA Rollover Certificate

Use this task to export a CA rollover certificate.

## SUMMARY STEPS

- enable
- configure terminal
- crypto pki export trustpoint pem {terminal | url url} [rollover]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto pki export trustpoint pem {terminal   url url} [rollover]</b>  <b>Example:</b> Router(config)# crypto pki export mycs pem terminal rollover	Exports a CA shadow certificate.

## Maintaining, Verifying, and Troubleshooting the Certificate Server, Certificates, and the CA

Use the tasks in this section to help maintain, verify, and troubleshoot the certificate server, certificates and the CA as appropriate:

- [Managing the Enrollment Request Database, page 30](#)
- [Removing Enrollment Requests from the Enrollment Request Database: Examples, page 38](#)
- [Deleting a Certificate Server, page 33](#)
- [Verifying and Troubleshooting Certificate Server and CA Status, page 34](#)
- [Verifying CA Certificate Information, page 34](#)

### Managing the Enrollment Request Database

SCEP supports two client authentication mechanisms—manual and preshared key. Manual enrollment requires the administrator at the CA server to specifically authorize the enrollment requests; enrollment using preshared keys allows the administrator to preauthorize enrollment requests by generating a one-time password (OTP).

Use any of the optional steps within this task to help manage the enrollment request database by performing functions such as specifying enrollment processing parameters that are to be used by SCEP and by controlling the run-time behavior or the certificate server.

## SUMMARY STEPS

1. **enable**
2. **crypto pki server cs-label grant {all | req-id}**
3. **crypto pki server cs-label reject {all | req-id}**
4. **crypto pki server cs-label password generate [minutes]**

5. **crypto pki server** *cs-label* **revoke** *certificate-serial-number*
6. **crypto pki server** *cs-label* **request pkcs10** {*url* | **terminal**} [**base64** | **pem**]
7. **crypto pki server** *cs-label* **info** **crl**
8. **crypto pki server** *cs-label* **info** **requests**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>crypto pki server</b> <i>cs-label</i> <b>grant</b> { <b>all</b>   <i>req-id</i> }  <b>Example:</b> Router# crypto pki server mycs grant all	Grants all or specific SCEP requests.
Step 3	<b>crypto pki server</b> <i>cs-label</i> <b>reject</b> { <b>all</b>   <i>req-id</i> }  Router# crypto pki server mycs reject all	Rejects all or specific SCEP requests.
Step 4	<b>crypto pki server</b> <i>cs-label</i> <b>password generate</b> [ <i>minutes</i> ]  <b>Example:</b> Router# crypto pki server mycs password generate 75	Generates a OTP for SCEP requests. <ul style="list-style-type: none"> <li><i>minutes</i>—Length of time, in minutes, that the password is valid. Valid values range from 1 to 1440 minutes. The default is 60 minutes.</li> </ul> <b>Note</b> Only one OTP is valid at a time; if a second OTP is generated, the previous OTP is no longer valid.
Step 5	<b>crypto pki server</b> <i>cs-label</i> <b>revoke</b> <i>certificate-serial-number</i>  <b>Example:</b> Router# crypto pki server mycs revoke 3	Revokes a certificate on the basis of its serial number. <ul style="list-style-type: none"> <li><i>certificate-serial-number</i>—One of the following options: <ul style="list-style-type: none"> <li>A string with a leading 0x, which is treated as a hexadecimal value</li> <li>A string with a leading 0 and no x, which is treated as octal</li> <li>All other strings, which are treated as decimal</li> </ul> </li> </ul>

	Command or Action	Purpose
Step 6	<pre>crypto pki server cs-label request pkcs10 {url   terminal} [base64   pem]</pre> <p><b>Example:</b> Router# crypto pki server mycs request pkcs10 terminal pem</p>	<p>Manually adds either a base64-encoded or PEM-formatted PKCS10 certificate enrollment request to the request database.</p> <p>After the certificate is granted, it will be displayed on the console terminal using base64 encoding.</p> <ul style="list-style-type: none"> <li>• <b>pem</b>—Specifies the certificate will be returned <i>with</i> PEM headers automatically added to the certificate after the certificate is granted, regardless of whether PEM headers were used in the request.</li> <li>• <b>base64</b>—Specifies the certificate will be returned <i>without</i> privacy-enhanced mail (PEM) headers, regardless of whether PEM headers were used in the request.</li> </ul>
Step 7	<pre>crypto pki server cs-label info crl</pre> <p><b>Example:</b> Router# crypto pki server mycs info crl</p>	Displays information regarding the status of the current CRL.
Step 8	<pre>crypto pki server cs-label info requests</pre> <p><b>Example:</b> Router# crypto pki server mycs info requests</p>	Displays all outstanding certificate enrollment requests.

## Removing Requests from the Enrollment Request Database

After the certificate server receives an enrollment request, the server can leave the request in a pending state, reject it, or grant it. The request stays in the enrollment request database for 1 week until the client polls the certificate server for the result of the request. If the client exits and never polls the certificate server, you can remove either individual requests or all requests from the database.

Use this task to remove requests from the database and allow the server to be returned to a clean slate with respect to the keys and transaction IDs. Also, you can use this task to help troubleshoot a SCEP client that may not be behaving properly.

### SUMMARY STEPS

1. **enable**
2. **crypto pki server cs-label remove {all | req-id}**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>crypto pki server <i>cs-label</i> remove {all   <i>req-id</i>}</b>  <b>Example:</b> Router# <b>crypto pki server mycs remove 15</b>	Removes enrollment requests from the enrollment request database.

## Deleting a Certificate Server

Users can delete a certificate server from the PKI configuration if they no longer want it on the configuration. Typically, a subordinate certificate server or an RA is being deleted. However, users may delete a root certificate server if they are moving it to another device via the archived RSA keys.

Perform this task to delete a certificate server from your PKI configuration.



### Note

When a certificate server is deleted, the associated trustpoint and key are also deleted.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no crypto pki server *cs-label***

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>no crypto pki server <i>cs-label</i></b>  <b>Example:</b> Router (config)# no crypto pki server mycs	Deletes a certificate server and associated trustpoint and key.

## Verifying and Troubleshooting Certificate Server and CA Status

Use any of the following optional steps to verify the status of the certificate server or the CA.

### SUMMARY STEPS

1. **enable**
2. **debug crypto pki server**
3. **dir filesystem:**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>debug crypto pki server</b>  <b>Example:</b> Router# debug crypto pki server	Enables debugging for a crypto PKI certificate server. <ul style="list-style-type: none"><li>• This command can be used for monitoring the progress of an enrollment and for troubleshooting if the certificate server fails to respond or if the certificate server has trouble handling the request that has been configured.</li></ul>
Step 3	<b>dir filesystem:</b>  <b>Example:</b> Router# dir slot0:	Displays a list of files on a file system. <ul style="list-style-type: none"><li>• This command can be used to verify the certificate server autoarchived file if the <b>database url</b> command was entered to point to a local file system. You should be able to at least see “<i>cs-label.ser</i>” and “<i>cs-label.crl</i>” files in the database.</li></ul>

## Verifying CA Certificate Information

To obtain information relating to the CA certificates including the certificate server rollover process, rollover certificates, and timers, you may use any of the following commands.



#### Note

These commands are not exclusive to shadow certificate information. If no shadow certificate exists, the following commands will simply display the active certificate information.

### SUMMARY STEPS

1. **crypto pki certificate chain** *name*
2. **crypto pki server** *cs-label* **info requests**
3. **show crypto pki certificates**
4. **show crypto pki server**
5. **show crypto pki trustpoints**



## DETAILED STEPS

- Step 1** The **crypto pki certificate chain** command can be used to view the certificate chain details and to distinguish the current active certificate from the rollover certificate in the certificate chain. The following example shows a certificate chain with an active CA certificate and a shadow, or rollover, certificate:

```
Router(config)# crypto pki certificate chain mica

certificate 06
certificate ca 01
! This is the peer's shadow PKI certificate.
certificate rollover 0B
! This is the CA shadow PKI certificate
certificate rollover ca 0A
```

- Step 2** The **crypto pki server info requests** command displays all outstanding certificate enrollment requests. The following example shows the output for shadow PKI certificate information requests:

```
Router# crypto pki server myca info requests

Enrollment Request Database:
RA certificate requests:

 ReqID State Fingerprint SubjectName

RA rollover certificate requests:

 ReqID State Fingerprint SubjectName

Router certificates requests:

 ReqID State Fingerprint SubjectName

1 pending A426AF07FE3A4BB69062E0E47198E5BF hostname=client

Router rollover certificates requests:

 ReqID State Fingerprint SubjectName

2 pending B69062E0E47198E5BFA426AF07FE3A4B hostname=client
```

- Step 3** The **show crypto pki certificates** command displays information about your certificate, the certification authority certificate, shadow certificates, and any registration authority certificates. The following example displays the certificate of the router and the certificate of the CA. There is no shadow certificate available. A single, general-purpose RSA key pair was previously generated, and a certificate was requested but not received for that key pair. Note that the certificate status of the router shows “Pending.” After the router receives its certificate from the CA, the Status field changes to “Available” in the **show** output.

```
Router# show crypto pki certificates

Certificate
 Subject Name
 Name: myrouter.example.com
 IP Address: 192.0.2.1
 Serial Number: 04806682
 Status: Pending
 Key Usage: General Purpose
```

```

Fingerprint: 428125BD A3419600 3F6C7831 6CD8FA95 00000000
CA Certificate
Status: Available
Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
Key Usage: Not Set

```

- Step 4** The **show crypto pki server** command displays the current state and configuration of the certificate server. The following example shows that the certificate server “routercs” has rollover configured. The CA auto-rollover time has occurred and the rollover, or shadow, PKI certificate is available. The status shows the rollover certificate fingerprint and rollover CA certificate expiration timer information.

```

Router# show crypto pki server

Certificate Server routercs:
 Status: enabled, configured
 Issuer name: CN=walnutcs
 CA cert fingerprint: 800F5944 74337E5B C2DF6C52 9A7B1BDB
 Granting mode is: auto
 Last certificate issued serial number: 0x7
 CA certificate expiration timer: 22:10:29 GMT Jan 29 2007
 CRL NextUpdate timer: 21:50:56 GMT Mar 5 2004
 Current storage dir: nvram:
 Database Level: Minimum - no cert data written to storage
Rollover status: available for rollover
 Rollover CA cert fingerprint: 6AAF5944 74227A5B 23DF3E52 9A7F1FEF
 Rollover CA certificate expiration timer: 22:10:29 GMT Jan 29 2017

```

- Step 5** The **show crypto pki trustpoints** command displays the trustpoints that are configured in the router. The following output shows that a shadow CA certificate is available and shows the SCEP capabilities reported during the last enrollment operation:

```

Router# show crypto pki trustpoints

Trustpoint vpn:
 Subject Name:
 cn=Cisco SSL CA
 o=Cisco Systems
 Serial Number: 0FFEBBDC1B6F6D9D0EA7875875E4C695
 Certificate configured.
 Rollover certificate configured.
 Enrollment Protocol:
 SCEPv1, PKI Rollover

```

## Configuration Examples for Using a Certificate Server

This section contains the following configuration examples:

- [Configuring Specific Storage and Publication Locations: Examples, page 37](#)
- [Removing Enrollment Requests from the Enrollment Request Database: Examples, page 38](#)
- [Autoarchiving the Certificate Server Root Keys: Examples, page 39](#)
- [Restoring a Certificate Server from Certificate Server Backup Files: Examples, page 41](#)
- [Subordinate Certificate Server: Example, page 43](#)
- [RA Mode Certificate Server: Example, page 45](#)
- [Enabling CA Certificate Rollover to Start Immediately: Example, page 47](#)

## Configuring Specific Storage and Publication Locations: Examples

The following example shows the configuration of a minimal local file system, so that the certificate server can respond quickly to certificate requests. The .ser and .crl files are stored on the local Cisco IOS file system for fast access, and a copy of all of the .crt files are published to a remote location for long-term logging.

```
crypto pki server myserver
 !Pick your database level.
 database level minimum
 !Specify a location for the .crt files that is different than the default local
 !Cisco IOS file system.
 database url crt publish http://url username user1 password secret
```



### Note

Free space on the local file system should be monitored, in case the .crl file becomes too large.

The following example shows the configuration of a primary storage location for critical files, a specific storage location for the critical file serial number file, the main certificate server database file, and a password protected file publication location for the CRL file:

```
Router(config)# crypto pki server mycs
Router(cs-server)# database url ftp://cs-db.company.com
!
% Server database url was changed. You need to move the
% existing database to the new location.
!
Router(cs-server)# database url ser nvram:
Router(cs-server)# database url crt publish ftp://crl.company.com username myname password
mypassword
Router(cs-server)# end
```

The following output displays the specified primary storage location and critical file storage locations specified:

```
Router# show
```

```
Sep 3 20:19:34.216: %SYS-5-CONFIG_I: Configured from console by user on console
```

```
Router# show crypto pki server
```

```
Certificate Server mycs:
 Status: disabled
 Server's configuration is unlocked (enter "no shut" to lock it)
 Issuer name: CN=mycs
 CA cert fingerprint: -Not found-
 Granting mode is: manual
 Last certificate issued serial number: 0x0
 CA certificate expiration timer: 00:00:00 GMT Jan 1 1970
 CRL not present.
 Current primary storage dir: ftp://cs-db.company.com
 Current storage dir for .ser files: nvram:
 Database Level: Minimum - no cert data written to storage
The following output displays all storage and publication locations. The serial number file (.ser) is stored in NVRAM. The CRL file will be published to ftp://crl.company.com with a username and password. All other critical files will be stored to the primary location, ftp://cs-db.company.com.
```

```
Router# show running-config
```

```
section crypto pki server
crypto pki server mycs shutdown database url ftp://cs-db.company.com
```

```

database url crl publish ftp://crl.company.com username myname password 7
12141C0713181F13253920
database url ser nvram:
Router#

```

## Removing Enrollment Requests from the Enrollment Request Database: Examples

The following examples show both the enrollment requests that are currently in the enrollment request database and the result after one of the enrollment requests has been removed from the database.

### Enrollment Request Currently in the Enrollment Request Database

The following example shows that the **crypto pki server info requests** command has been used to display the enrollment requests that are currently in the Enrollment Request Database:

```
Router# crypto pki server myserver info requests
```

Enrollment Request Database:

```

RA certificate requests:
ReqID State Fingerprint SubjectName

```

```

Router certificates requests:
ReqID State Fingerprint SubjectName

2 pending 1B07F3021DAAB0F19F35DA25D01D8567 hostname=host1.company.com
1 denied 5322459D2DC70B3F8EF3D03A795CF636 hostname=host2.company.com

```

### crypto pki server remove Command Used to Remove One Enrollment Request

The following example shows that the **crypto pki server remove** command has been used to remove Enrollment Request 1:

```
Router# crypto pki server myserver remove 1
```

### Enrollment Request Database After the Removal of One Enrollment Request

The following example shows the result of the removal of Enrollment Request 1 from the Enrollment Request Database:

```
Router# crypto pki server mycs info requests
```

Enrollment Request Database:

```

RA certificate requests:
ReqID State Fingerprint SubjectName

```

```

Router certificates requests:
ReqID State Fingerprint SubjectName

2 pending 1B07F3021DAAB0F19F35DA25D01D8567 hostname=host1.company.com

```

## Autoarchiving the Certificate Server Root Keys: Examples

The following output configurations and examples show what you might see if the **database archive** command has not been configured (that is, configured using the default value); if the **database archive** command has been configured to set the CA certificate and CA key archive format as PEM, without configuring a password; and if the **database archive** command has been configured to set the CA certificate and CA key archive format as PKCS12, with a password configured. The last example is sample content of a PEM-formatted archive file.

### database archive Command Not Configured



#### Note

The default is PKCS12, and the prompt for the password appears after the **no shutdown** command has been issued.

```
Router (config)# crypto pki server myserver
Router (cs-server)# no shutdown

% Generating 1024 bit RSA keys ...[OK]
% Ready to generate the CA certificate.
%Some server settings cannot be changed after CA certificate generation.

Are you sure you want to do this? [yes/no]: y
% Exporting Certificate Server signing certificate and keys...
! Note the next two lines, which are asking for a password.
% Please enter a passphrase to protect the private key.
Password:
% Certificate Server enabled.
Router (cs-server)# end

Router# dir nvram:

Directory of nvram:/

 125 -rw- 1693 <no date> startup-config
 126 ---- 5 <no date> private-config
 1 -rw- 32 <no date> myserver.ser
 2 -rw- 214 <no date> myserver.crl
! Note the next line, which indicates PKCS12 format.
 3 -rw- 1499 <no date> myserver.p12
```

### database archive Command and pem Keyword Configured



#### Note

The prompt for the password appears after the **no shutdown** command has been issued.

```
Router (config)# crypto pki server myserver
Router (cs-server)# database archive pem
Router (cs-server)# no shutdown

% Generating 1024 bit RSA keys ...[OK]
% Ready to generate the CA certificate.
%Some server settings cannot be changed after CA certificate generation.

Are you sure you want to do this? [yes/no]: y
% Exporting Certificate Server signing certificate and keys...
!Note the next two lines, which are asking for a password.
% Please enter a passphrase to protect the private key.
Password:
```

```
% Certificate Server enabled.
Router (cs-server)# end

Router# dir nvram

Directory of nvram:/

 125 -rw- 1693 <no date> startup-config
 126 ---- 5 <no date> private-config
 1 -rw- 32 <no date> myserver.ser
 2 -rw- 214 <no date> myserver.crl
! Note the next line showing that the format is PEM.
 3 -rw- 1705 <no date> myserver.pem
```

### database archive Command and pkcs12 Keyword (and Password) Configured



#### Note

When the password is entered, it will be encrypted. However, it is recommended that you remove the password from the configuration after the archive has finished.

```
Router (config)# crypto pki server myserver
Router (cs-server)# database archive pkcs12 password cisco123
Router (cs-server)# no shutdown

% Generating 1024 bit RSA keys ...[OK]
% Ready to generate the CA certificate.
% Some server settings cannot be changed after CA certificate generation.

Are you sure you want to do this? [yes/no]: y
% Exporting Certificate Server signing certificate and keys...
! Note that you are not being prompted for a password.
% Certificate Server enabled.
Router (cs-server)# end
Router# dir nvram:
Directory of nvram:/

 125 -rw- 1693 <no date> startup-config
 126 ---- 5 <no date> private-config
 1 -rw- 32 <no date> myserver.ser
 2 -rw- 214 <no date> myserver.crl
! Note that the next line indicates that the format is PKCS12.
 3 -rw- 1499 <no date> myserver.p12
```

### PEM-Formatted Archive

The following sample output shows that autoarchiving has been configured in PEM file format. The archive consists of the CA certificate and the CA private key. To restore the certificate server using the backup, you would have to import the PEM-formatted CA certificate and CA key individually.



#### Note

In addition to the CA certificate and CA key archive files, you should also back up the serial file (.ser) and the CRL file (.crl) regularly. The serial file and the CRL file are both critical for CA operation if you need to restore your certificate server.

```
Router# more nvram:mycs.pem

-----BEGIN CERTIFICATE-----
MIIB9zCCAWCgAwIBAgIBATANBgkqhkiG9w0BAQQFADAPMQ0wCwYDVQQDEwRteWNz
MB4XDTA0MDgyNzAyMzI0N1oXDTA3MDgyNzAyMzI0N1owDzENMAAGAlUEAxMEbXlj
czCBNzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA1lZpKP4nGDJHgPkpYSkix7ld
nr23aMlZ9Kz5oo/qTBxeZ8mujpjYcZ0T8AZvoOiCuDnYMl796ZwpkMgjz1aZZbL+
```

```

BtuVvllsEOfhC+u/Ol/vxfGG5xpshoz/F5J3xdg5ZZuWwuIDAUYu9+QbI5feuG04
Z/BiPIb4AmGTP4B2MM0CAwEAAAnjMGEwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8B
Af8EBAMCAYYwHwYDVR0jBBgwFoAUKi/cuK6wkz+ZswVtb06vUJboEeEwHQYDVR0O
BBYEFcov3LiusJM/mbMFbW9Or1CW6BHhMA0GCSqGSIb3DQEBAUAA4GBAKLOmoE2
4+NeOKEXMCXG1jcohK7O2HrkFfl/vpK0+q92PTnMUFhxL0qI8pWIq5CCgC7heace
OrTv2zcUAoH4rzx3Rc2USIxkDokWWQMLujsMm/SLIeHit0G5uj//GCcbgK20MAW6
ymf7+Tmb1SFljWzstoUXC2hLnsJIMq/KffaD
-----END CERTIFICATE-----

!The private key is protected by the password that is
configured in "database archive pem password pwd" or that
is entered when you are prompted for the password.
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-EDE3-CBC,106CE91FFD0A075E

zyiFC8rKv8Cs+IKsQG2QpsVpVDBHqZqBSM4D528bvZv7jzr6WuHj8E6zO+6G8R/A
zjsfTALo+e+ZDg7KMzbryHARvjSkbqFdOMLlVIYBhCeSElKsskWB6chOuyPHJInW
JwC5YzZdZwOqcyLBP/xOYXcvjzzNfPAXZzN12VR8vWDNq/kHT+3Lplc8hY++ABMI
M+C9FB3dpNZu501BZCJg46bqbkuLaCCmScIDaVt0zDFZwWTSufiemmnXZBG4xS8
t5t+FEhmSfv8DAmwg4f/KVRFtm10phUArcLxQ038A10W5YHHORdACnuzVUvHgc07
VT4XUTj07qMhmJgFNWylpu49fbdS2NnOn5IoIyAq51k1KUPrz/WABWiCvLMylGnZ
kyMCWoaMtgS/vdx74BBCj09yRZJnLmLi6SDofjCNTDhfMFEVg4LsSWCd41P9OP8
0MghP1D5VIx6PbMnwKWW121pBbCCdesFRGHjZD2dOu96kHD7ItErX34CC8W04aG4
b7DLktUu6WNV6M8g3CAqJiC0V8ATlp+kvdHZVkJXovgND5IU00Jpsj0HhGzKAGpOY
KTGTUekUboISjVVkI6efp1v06temVL3Txg3KGhzWMJGrq1snghE0KnV8tkddv/9N
d/t1l+we9mrccTq50WNDnKEi/cwHI/0PKXg+NDNH3k3QGpAprsqGQmMPdqc5ut0P
86i4cF9078QwWg4Tpay3uqNH1Zz6UN0tcarVvNmDupFESUxYw10qJrrEYVRadu74
rKAU4Ey4xkAftB2kuqvr21Av/L+jne4kkGIozYdB+p/M98pQRgkYyg==
-----END RSA PRIVATE KEY-----

```

## Restoring a Certificate Server from Certificate Server Backup Files: Examples

The following example shows that restoration is from a PKCS12 archive and that the database URL is NVRAM (the default).

```

Router# copy tftp://192.0.2.71/backup.ser nvram:mycs.ser
Destination filename [mycs.ser]?

32 bytes copied in 1.320 secs (24 bytes/sec)
Router# copy tftp://192.0.2.71/backup.crl nvram:mycs.crl
Destination filename [mycs.crl]?

214 bytes copied in 1.324 secs (162 bytes/sec)
Router# configure terminal
Router (config)# crypto pki import mycs pkcs12 tftp://192.0.2.71/backup.p12 cisco123
Source filename [backup.p12]?
CRYPTO_PKI: Imported PKCS12 file successfully.
Router (config)# crypto pki server mycs
! fill in any certificate server configuration here
Router (cs-server)# no shutdown
% Certificate Server enabled.
Router (cs-server)# end
Router# show crypto pki server

Certificate Server mycs:
 Status: enabled
 Server's current state: enabled
 Issuer name: CN=mycs
 CA cert fingerprint: 34885330 B13EAD45 196DA461 B43E813F
 Granting mode is: manual
 Last certificate issued serial number: 0x1

```

```

CA certificate expiration timer: 01:49:13 GMT Aug 28 2007
CRL NextUpdate timer: 01:49:16 GMT Sep 4 2004
Current storage dir: nvram:
Database Level: Minimum - no cert data written to storage

```

The following example shows that restoration is from a PEM archive and that the database URL is flash:

```

Router# copy tftp://192.0.2.71/backup.ser flash:mycs.ser
Destination filename [mycs.ser]?
32 bytes copied in 1.320 secs (24 bytes/sec)
Router# copy tftp://192.0.2.71/backup.crl flash:mycs.crl
Destination filename [mycs.crl]?
214 bytes copied in 1.324 secs (162 bytes/sec)
Router# configure terminal
! Because CA cert has Digital Signature usage, you need to import using the "usage-keys"
keyword
Router (config)# crypto ca import mycs pem usage-keys terminal cisco123
% Enter PEM-formatted CA certificate.
% End with a blank line or "quit" on a line by itself.
! Paste the CA cert from .pem archive.
-----BEGIN CERTIFICATE-----
MIIB9zCCAwwGAgAwIBAgIBATANBgkqhkiG9w0BAQQFADAPMQ0wCwYDVQQDEwRteWNz
MB4XDTA0MDkwMjIxMDI1N1oXDTA3MDkwMjIxMDI1N1owDzENMAAGA1UEAxMEbXl1j
czCBnzANBgkqhkiG9w0BAQEFAAOBjQAwGykCgYEAuGnnDXJbpdDQwCuKGS5Zg2rc
K7ZJauSUotTmWYQvNx+ZmWrUs5/j9Ee5FV2YonirGBQ9mc6u163kNlrIPFck062L
GpahBhNmKdGod1o2PHTnRlZpEZNDIqU2D3hACgByxPjY4vUnccV36ewLnQnYpp8
szEu7PYTJr5dU5ltAekCAwEAAANjMGEwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8B
Af8EBAMCAAYwHwYDVR0jBBgwFoAUaEEQwYKCQ1dm9+wLYBKRTlZxaDIwHQYDVR0O
BBYEFGBBEMGCGkNXZvfcS2ASKU5c8WgyMA0GCSqGSIb3DQEBAUAA4GBAHyhiV2C
mH+vsWkbjRA1FzZk8ttu9s5kwqG0dXp25QRUWsgLr9nsKPNdVkt3P7p0A/KochHe
eNiygIv+hDQ3FVnzsNv983le605jvAPxc17RO1BbfNhhqEWMSXdnjHocUy7XerCo
+bdPcUf/eCizueH/BEy/SZhd7yovzn2cdzBN
-----END CERTIFICATE-----

% Enter PEM-formatted encrypted private SIGNATURE key.
% End with "quit" on a line by itself.
! Paste the CA private key from .pem archive.
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-EDE3-CBC, 5053DC842B04612A

1Cn1F5Pqvd0zp2NLZ7iosxzTy6nDeXPPNyJpXB5q+V29IuY8Apb6TlJCU7YrsEB/
nBTK7K76DCeGPlLpcuyEI171QmkQJ2gA0QhC0LrRo09WrINVH+b4So/y7nffZkVb
p2yDpZwqoJ8cmRH94Tie0YmzBtEh6ayOud1lZ53qbrsCnfSEwszt1xrWlMKrFZrk
/fTy6loHzGFz13BDj4r5gBecExwcPp74ldHO+Ld4Nc9egG8BYkeBCsZZOQNvHXLN
I0tODos6hP915zb6OrZFVYv0NK6grTBO9D8hjNZ3U79jJzsSP7UNzIYHNTzRjIAyu
i56Oy/iHvkCSNUIK6zeIJQnW4bSoM1BqrbVPwHU6QaXUqlNzZ8SDtw7ZRZ/rHuiD
RTJMPbKquAzeuBss1132OaAUJRStjPXgyZTUbc+cWb6zATNws2yijPDTR6sRHoQL
47wHMr2Yj80VZGgkCSLAKL88ACz9TfUiVFhtf16xMC2yuF1+WRk1XfF5VtWe5Zer
3Fn1DcBmlF7086XUkiSHP4EV0cI6n5ZMzVLx0XAUTdA1lgD94y1V+6p9PcQHLYQA
pGRmj51lSfw90aLafgCTbRbmC0ChIqHy91UFa1ub0130+yu7LsLGR1PmJ9NE61JR
bjRh1UXItRYWY7C4M3m/0wz6fmVQNSumJM08RHq61UB3olZigGIz1ZkoaESrLG0p
qq2AENFemCPF0uhyVS2humMHjWuRr+jedfc/IM17sLEgAdqCVCfV3RZVEaNXBud1
4QjkuTrwaTcRXVfbtrVioT/puyVULpA7+k7w+F5TZwUV08mwvUEqDw==
-----END RSA PRIVATE KEY-----
quit
% Enter PEM-formatted SIGNATURE certificate.
% End with a blank line or "quit" on a line by itself.
! Paste the CA cert from .pem archive again.
-----BEGIN CERTIFICATE-----
MIIB9zCCAwwGAgAwIBAgIBATANBgkqhkiG9w0BAQQFADAPMQ0wCwYDVQQDEwRteWNz
MB4XDTA0MDkwMjIxMDI1N1oXDTA3MDkwMjIxMDI1N1owDzENMAAGA1UEAxMEbXl1j
czCBnzANBgkqhkiG9w0BAQEFAAOBjQAwGykCgYEAuGnnDXJbpdDQwCuKGS5Zg2rc
K7ZJauSUotTmWYQvNx+ZmWrUs5/j9Ee5FV2YonirGBQ9mc6u163kNlrIPFck062L

```



```
GpahBhNmKDgod1o2PHTnRlZpEZNDIqU2D3hACgByxPjrY4vUnccV36ewLnQnYpp8
szEu7PYTJr5dU5ltAekCAwEAAANjMGEwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8B
Af8EBAMCAYYwHwYDVR0jBBgwFoAUaEEQwYKCQ1dm9+wLYBKRTlzxADIwHQYDVR0O
BBYEFghBEMGCgkNXZvfsC2ASkU5c8WgyMA0GCSqGSIb3DQEBAUAA4GBAHyhiV2C
mH+vswkBjRA1Fzzk8ttu9s5kwqG0dXp25QRUWsGlr9nsKPNdVkt3P7p0A/KochHe
eNiygiv+hDQ3FVnzsnv9831e605jvAPxc17R01BbfNhgqEWMsXdnjH0cUy7XerCo
+bdPcUf/eCiZueH/BEy/SzhD7yovzn2cdzBN
-----END CERTIFICATE-----

% Enter PEM-formatted encrypted private ENCRYPTION key.
% End with "quit" on a line by itself.
! Because the CA cert only has Digital Signature usage, skip the encryption part.
quit
% PEM files import succeeded.
Router (config)# crypto pki server mycs
Router (cs-server)# database url flash:
! Fill in any certificate server configuration here.
Router (cs-server)# no shutdown
% Certificate Server enabled.
Router (cs-server)# end

Router # show crypto pki server

Certificate Server mycs:
 Status: enabled
 Server's current state: enabled
 Issuer name: CN=mycs
 CA cert fingerprint: F04C2B75 E0243FBC 19806219 B1D77412
 Granting mode is: manual
 Last certificate issued serial number: 0x2
 CA certificate expiration timer: 21:02:55 GMT Sep 2 2007
 CRL NextUpdate timer: 21:02:58 GMT Sep 9 2004
 Current storage dir: flash:
 Database Level: Minimum - no cert data written to storage
```

## Subordinate Certificate Server: Example

The following configuration and output is typical of what you might see after configuring a subordinate certificate server:

```
Router (config)# crypto pki trustpoint sub
Router (ca-trustpoint)# enrollment url http://192.0.2.6
Router (ca-trustpoint)# exit

Router (config)# crypto pki server sub
Router (cs-server)# mode sub-cs
Router (ca-server)# no shutdown

%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password:
Jan 6 22:32:22.698: CRYPTO_CS: enter FSM: input state initial, input signal no shut

Re-enter password:
% Generating 1024 bit RSA keys ...
Jan 6 22:32:30.302: CRYPTO_CS: starting enabling checks
Jan 6 22:32:30.306: CRYPTO_CS: key 'sub' does not exist; generated automatically [OK]

Jan 6 22:32:39.810: %SSH-5-ENABLED: SSH 1.99 has been enabled
Certificate has the following attributes:
```

```

Fingerprint MD5: 328ACC02 52B25DB8 22F8F104 B6055B5B
Fingerprint SHA1: 02FD799D DD40C7A8 61DC53AB 1E89A3EA 2A729EE2

% Do you accept this certificate? [yes/no]:
Jan 6 22:32:44.830: CRYPTO_CS: nvram filesystem
Jan 6 22:32:44.922: CRYPTO_CS: serial number 0x1 written.
Jan 6 22:32:46.798: CRYPTO_CS: created a new serial file.
Jan 6 22:32:46.798: CRYPTO_CS: authenticating the CA 'sub'y
Trustpoint CA certificate accepted.%

% Certificate request sent to Certificate Authority

% Enrollment in progress...
Router (cs-server)#
Jan 6 22:33:30.562: CRYPTO_CS: Publishing 213 bytes to crl file nvram:sub.crl
Jan 6 22:33:32.450: CRYPTO_CS: enrolling the server's trustpoint 'sub'
Jan 6 22:33:32.454: CRYPTO_CS: exit FSM: new state check failed
Jan 6 22:33:32.454: CRYPTO_CS: cs config has been locked
Jan 6 22:33:33.118: CRYPTO_PKI: Certificate Request Fingerprint MD5: CED89E5F 53B9C60E
> AA123413 CDDAD964
Jan 6 22:33:33.118: CRYPTO_PKI: Certificate Request Fingerprint SHA1: 70787C76 ACD7E67F
7D2C8B23 98CB10E7 718E84B1
% Exporting Certificate Server signing certificate and keys...

Jan 6 22:34:53.839: %PKI-6-CERTRET: Certificate received from Certificate Authority
Jan 6 22:34:53.843: CRYPTO_CS: enter FSM: input state check failed, input signal cert
configured
Jan 6 22:34:53.843: CRYPTO_CS: starting enabling checks
Jan 6 22:34:53.843: CRYPTO_CS: nvram filesystem
Jan 6 22:34:53.883: CRYPTO_CS: found existing serial file.
Jan 6 22:34:53.907: CRYPTO_CS: old router cert flag 0x4
Jan 6 22:34:53.907: CRYPTO_CS: new router cert flag 0x44
Jan 6 22:34:56.511: CRYPTO_CS: DB version
Jan 6 22:34:56.511: CRYPTO_CS: last issued serial number is 0x1
Jan 6 22:34:56.551: CRYPTO_CS: CRL file sub.crl exists.
Jan 6 22:34:56.551: CRYPTO_CS: Read 213 bytes from crl file sub.crl.
Jan 6 22:34:56.603: CRYPTO_CS: SCEP server started
Jan 6 22:34:56.603: CRYPTO_CS: exit FSM: new state enabled
Jan 6 22:34:56.603: CRYPTO_CS: cs config has been locked
Jan 6 22:35:02.359: CRYPTO_CS: enter FSM: input state enabled, input signal time set
Jan 6 22:35:02.359: CRYPTO_CS: exit FSM: new state enabled
Jan 6 22:35:02.359: CRYPTO_CS: cs config has been locked

```

## Root Certificate Server Differentiation: Example

When issuing certificates, the root certificate server (or parent subordinate certificate server) will differentiate the certificate request from “Sub CA,” “RA,” and peer requests, as shown in the following sample output:

```

Router# crypto pki server server1 info req

Enrollment Request Database:
RA certificate requests:
ReqID State Fingerprint SubjectName

Subordinate CS certificate requests:
ReqID State Fingerprint SubjectName

1 pending CB9977AD8A73B146D3221749999B0F66 hostname=host-subcs.company.com

```

```

RA certificate requests:
ReqID State Fingerprint SubjectName

Router certificate requests:
ReqID State Fingerprint SubjectName

```

## Show Output for a Subordinate Certificate Server: Example

The following **show crypto pki server** command output indicates that a subordinate certificate server has been configured:

```

Router# show crypto pki server

Certificate Server sub:
 Status: enabled
 Server's configuration is locked (enter "shut" to unlock it)
 Issuer name: CN=sub
 CA cert fingerprint: 11B586EE 3B354F33 14A25DDD 7BD39187
 Server configured in subordinate server mode
 Upper CA cert fingerprint: 328ACC02 52B25DB8 22F8F104 B6055B5B
 Granting mode is: manual
 Last certificate issued serial number: 0x1
 CA certificate expiration timer: 22:33:44 GMT Jan 6 2006
 CRL NextUpdate timer: 22:33:29 GMT Jan 13 2005
 Current storage dir: nvram:
 Database Level: Minimum - no cert data written to storage

```

## RA Mode Certificate Server: Example

The following output is typical of what you might see after having configured an RA mode certificate server:

```

Router-ra (config)# crypto pki trustpoint myra
Router-ra (ca-trustpoint)# enrollment url http://192.0.2.17
! Include "cn=ioscs RA" or "ou=ioscs RA" in the subject-name.
Router-ra (ca-trustpoint)# subject-name cn=myra, ou=ioscs RA, o=company, c=us
Router-ra (ca-trustpoint)# exit
Router-ra (config)# crypto pki server myra
Router-ra (cs-server)# mode ra
Router-ra (cs-server)# no shutdown
% Generating 1024 bit RSA keys ...[OK]

Certificate has the following attributes:
Fingerprint MD5: 32661452 0DDA3CE5 8723B469 09AB9E85
Fingerprint SHA1: 9785BBCE 6C67D27C C950E8D0 718C7A14 C0FE9C38
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Ready to request the CA certificate.
%Some server settings cannot be changed after the CA certificate has been requested.

Are you sure you want to do this? [yes/no]: yes
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
 password to the CA administrator in order to revoke your certificate.
 For security reasons your password will not be saved in the configuration.
 Please make a note of it.

```

```

Password:
Re-enter password:

% The subject name in the certificate will include: cn=myra, ou=ioscs RA, o=company, c=us
% The subject name in the certificate will include: Router-ra.company.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificate' command will also show the fingerprint.

% Enrollment in progress...
Router-ra (cs-server)#
Sep 15 22:32:40.197: CRYPTO_PKI: Certificate Request Fingerprint MD5: 82B41A76 AF4EC87D
AAF093CD 07747D3A
Sep 15 22:32:40.201: CRYPTO_PKI: Certificate Request Fingerprint SHA1: 897CDF40 C6563EAA
0FED05F7 0115FD3A 4FFC5231
Sep 15 22:34:00.366: %PKI-6-CERTRET: Certificate received from Certificate Authority
Router-ra (cs-server)#
Router-ra(cs-server)# end

```

```
Router-ra# show crypto pki server
```

```

Certificate Server myra:
 Status: enabled
 Issuer name: CN=myra
 CA cert fingerprint: 32661452 0DDA3CE5 8723B469 09AB9E85
 ! Note that the certificate server is running in RA mode
 Server configured in RA mode
 RA cert fingerprint: C65F5724 0E63B3CC BE7AE016 BE0D34FE
 Granting mode is: manual
 Current storage dir: nvram:
 Database Level: Minimum - no cert data written to storage

```

The following output shows the enrollment request database of the issuing certificate server after the RA has been enabled:



#### Note

The RA certificate request is recognized by the issuing certificate server because "ou=ioscs RA" is listed in the subject name.

```

Router-ca# crypto pki server mycs info request
Enrollment Request Database:

Subordinate CA certificate requests:
ReqID State Fingerprint SubjectName

! The request is identified as RA certificate request.
RA certificate requests:
ReqID State Fingerprint SubjectName

12 pending 88F547A407FA0C90F97CDE8900A30CB0
hostname=Router-ra.company.com,cn=myra,ou=ioscs RA,o=company,c=us

```

```
Router certificates requests:
ReqID State Fingerprint SubjectName

```

```
! Issue the RA certificate.
Router-ca# crypto pki server mycs grant 12
```

The following output shows that the issuing certificate server is configured to issue a certificate automatically if the request comes from an RA:

```
Router-ca(config)# crypto pki server mycs
Router-ca (cs-server)# grant ra-auto
% This will cause all certificate requests already authorized by known RAs to be
automatically granted.

Are you sure you want to do this? [yes/no]: yes
Router-ca (cs-server)# end
Router-ca# show crypto pki server

Certificate Server mycs:
 Status: enabled
 Server's current state: enabled
 Issuer name: CN=mycs
 CA cert fingerprint: 32661452 0DDA3CE5 8723B469 09AB9E85
 ! Note that the certificate server will issue certificate for requests from the RA.
 Granting mode is: auto for RA-authorized requests, manual otherwise
 Last certificate issued serial number: 0x2
 CA certificate expiration timer: 22:29:37 GMT Sep 15 2007
 CRL NextUpdate timer: 22:29:39 GMT Sep 22 2004
 Current storage dir: nvram:
 Database Level: Minimum - no cert data written to storage
```

The following example shows the configuration of “myra”, an RA server, configured to support automatic rollover from “myca”, the CA. After the RA server is configured, automatic granting of certificate reenrollment requests is enabled:

```
crypto pki trustpoint myra
 enrollment url http://myca
 subject-name ou=iosca RA
 rsakeypair myra
crypto pki server myra
 mode ra
 auto-rollover

crypto pki server mycs
 grant auto rollover ra-cert
 auto-rollover 25
```

## Enabling CA Certificate Rollover to Start Immediately: Example

The following example shows how to enable automated CA certificate rollover on the server mycs with the **crypto pki server** command. The **show crypto pki server** command then shows the current state of the mycs server and that the rollover certificate is currently available for rollover.

```
Router(config)# crypto pki server mycs rollover

Jun 20 23:51:21.211:%PKI-4-NOSHADOWAUTOSAVE:Configuration was
modified. Issue "write memory" to save new IOS CA certificate

! The config has not been automatically saved because the config has been changed.
```

```
Router# show crypto pki server
```

```
Certificate Server mycs:
 Status:enabled
 Server's configuration is locked (enter "shut" to unlock it)
 Issuer name:CN=mycs
 CA cert fingerprint:E7A5FABA 5D7AA26C F2A9F7B3 03CE229A
 Granting mode is:manual
 Last certificate issued serial number:0x2
 CA certificate expiration timer:00:49:26 PDT Jun 20 2008
 CRL NextUpdate timer:00:49:29 PDT Jun 28 2005
 Current storage dir:nvram:
 Database Level:Minimum - no cert data written to storage
 Rollover status:available for rollover
 ! Rollover certificate is available for rollover.
 Rollover CA certificate fingerprint:9BD7A443 00A6DD74 E4D9ED5F B7931BE0
 Rollover CA certificate expiration time:00:49:26 PDT Jun 20 2011
 Auto-Rollover configured, overlap period 25 days
```

## Where to Go Next

After the certificate server is successfully running, you can either begin enrolling clients via manual mechanisms (as explained in the module “Configuring Certificate Enrollment for a PKI”) or begin configuring SDP, which is a web-based enrollment interface, (as explained in the module “Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI.”)

## Additional References

The following sections provide references related to Cisco IOS certificate server.

Related Topic	Document Title
USB Token RSA Operations: Using the RSA keys on a USB token for initial autoenrollment	<a href="#">“Configuring Certificate Enrollment for a PKI”</a> chapter in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4T. See the <a href="#">“Configuring Certificate Servers”</a> section.
USB Token RSA Operations: Benefits of using USB tokens	<a href="#">“Storing PKI Credentials”</a> module in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4T
Certificate server client certificate enrollment, autoenrollment, and automatic rollover	<a href="#">“Configuring Certificate Enrollment for a PKI”</a> module in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4T
Setting up and logging into a USB token	<a href="#">“Storing PKI Credentials”</a> module in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4T
Web-based certificate enrollment	<a href="#">“Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI”</a> module in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4T
RSA keys in PEM formatted files	<a href="#">“Deploying RSA Keys Within a PKI”</a> module in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4T
Choosing a certificate revocation mechanism	<a href="#">“Configuring Authorization and Revocation of Certificates in a PKI”</a> module in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4T

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

# Feature Information for the Cisco IOS Certificate Server

Table 4 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Implementing and Managing PKI Features Roadmap](#).”

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.


**Note**

Table 4 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 4** Feature Information for the Cisco IOS Certificate Server

Feature Name	Releases	Feature Information
Cisco IOS USB Token PKI Enhancements—Phase 2	12.4(11)T	<p>This feature enhances USB token functionality by using the USB token as a cryptographic device. USB tokens may be used for RSA operations such as key generation, signing, and authentication.</p> <p>The following sections in this document provide information about this feature:</p> <ul style="list-style-type: none"> <li><a href="#">RSA Key Pair and Certificate of the Certificate Server</a></li> <li><a href="#">Trustpoint of the Certificate Server</a></li> <li><a href="#">Generating a Certificate Server RSA Key Pair</a></li> </ul> <p><b>Note</b> This document covers the use of using USB tokens for RSA operations during certificate server configuration. For other documents on this topic, see the “<a href="#">The following sections provide references related to Cisco IOS certificate server.Related Documents</a>” section.</p>
IOS Certificate Server (CS) Split Database	12.4(4)T	<p>This feature allows the user to set storage locations and publish locations for specific certificate server file types.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li><a href="#">Certificate Server Database</a></li> <li><a href="#">Configuring Certificate Server Functionality</a></li> <li><a href="#">Configuring Specific Storage and Publication Locations: Examples</a></li> </ul> <p>The following command was modified by this feature: <b>database url</b></p>



**Table 4**      *Feature Information for the Cisco IOS Certificate Server (continued)*

Feature Name	Releases	Feature Information
Subordinate/RA Mode IOS Certificate Server (CS) Rollover	12.4(4)T	<p>This feature expands on Certificate Authority (CA) Key Rollover introduced in 12.4(2)T to allow CA certificate rollover for subordinate CAs and RA-mode CAs. This functionality allows the rollover expiring CA certificates and keys and to have these changes propagate through the PKI network without manual intervention.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Automatic CA Certificate and Key Rollover</a></li> <li>• <a href="#">Configuring Certificate Servers</a></li> <li>• <a href="#">RA Mode Certificate Server: Example</a></li> </ul> <p>The following command was modified by this feature: <b>grant auto rollover</b></p>
Certificate Authority (CA) Key Rollover	12.4(2)T	<p>This feature introduces the ability for root or subordinate CAs to roll over expiring CA certificates and keys and to have these changes propagate through the PKI network without manual intervention.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Automatic CA Certificate and Key Rollover</a></li> <li>• <a href="#">Configuring Certificate Servers</a></li> <li>• <a href="#">Working with Automatic CA Certificate Rollover</a></li> <li>• <a href="#">Enabling CA Certificate Rollover to Start Immediately: Example</a></li> </ul> <p>The following commands were introduced or modified by this feature: <b>auto-rollover</b>, <b>crypto pki certificate chain</b>, <b>crypto pki export pem</b>, <b>crypto pki server info request</b>, <b>crypto pki server</b>, <b>show crypto pki certificates</b>, <b>show crypto pki server</b>, and <b>show crypto pki trustpoint</b></p>
Cisco IOS Certificate Server	12.3(8)T	<p>This feature introduces support for the Cisco IOS certificate server, which offers users a CA that is directly integrated with Cisco IOS software to more easily deploy basic PKI networks.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Information About Cisco IOS Certificate Servers</a></li> <li>• <a href="#">How to Set Up and Deploy a Cisco IOS Certificate Server</a></li> </ul>

**Table 4** *Feature Information for the Cisco IOS Certificate Server (continued)*

Feature Name	Releases	Feature Information
The Certificate Server Auto Archive Enhancement <sup>1</sup>	12.3(11)T	<p>This enhancement enables the CA certificate and CA key to be backed up automatically just once after they are generated by the certificate server. As a result, it is not necessary to generate an exportable CA key if CA backup is desirable.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li><a href="#">Certificate Enrollment Using a Certificate Server</a></li> <li><a href="#">Configuring Certificate Server Functionality</a></li> </ul> <p>The following commands were introduced by this feature: <b>crypto pki server remote, database archive</b></p>
The Certificate Server Registration Authority (RA) Mode enhancement	12.3(7)T	<p>A certificate server can be configured to run in RA mode.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> <li><a href="#">Configuring a Certificate Server to Run in RA Mode</a></li> </ul> <p>The following commands were introduced by this feature: <b>grant ra-auto, lifetime enrollment-requests</b></p>
PKI Status <sup>1</sup>	12.3(11)T	<p>This enhancement provides a quick snapshot of current trustpoint status.</p> <p>The following section provides information about this enhancement:</p> <ul style="list-style-type: none"> <li><a href="#">Maintaining, Verifying, and Troubleshooting the Certificate Server, Certificates, and the CA</a></li> </ul> <p>The following command was modified by this enhancement: <b>show crypto pki trustpoints</b></p>
Subordinate Certificate Server <sup>1</sup>	12.3(14)T	<p>This enhancement allows you to configure a subordinate certificate server to grant all or certain SCEP or manual certificate requests.</p> <p>The following section provides information about this enhancement:</p> <ul style="list-style-type: none"> <li><a href="#">Configuring a Subordinate Certificate Server</a></li> </ul> <p>The following command was introduced by this enhancement: <b>mode sub-cs</b></p>
Cisco IOS Certificate Server	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
Trustpoint CLI	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

1. This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator.



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2005–2007 Cisco Systems, Inc. All rights reserved.





# Storing PKI Credentials

---

**First Published: May 2, 2005**

**Last Updated: August 21, 2007**

This module explains how to store public key infrastructure (PKI) credentials, such as Rivest, Shamir, and Adelman (RSA) keys and certificates in a specific location.

An example of a certificate storage location includes NVRAM, which is the default location, and other local storage locations, such as flash, as supported by your platform.

An example of an RSA key and certificate storage location includes a USB token. Selected Cisco platforms support smart card technology in a USB key form factor (such as an Aladdin USB eToken key). USB tokens provide secure configuration distribution, provide RSA operations such as on-token key generation, signing, and authentication, and allow users to store Virtual Private Network (VPN) credentials for deployment.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all of the features documented in this module.* To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Storing PKI Credentials](#)” section on [page 25](#).

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for Storing PKI Credentials, page 2](#)
- [Restrictions for Storing PKI Credentials, page 2](#)
- [Information About Storing PKI Credentials, page 3](#)
- [How to Configure PKI Storage, page 5](#)
- [Configuration Examples for PKI Storage, page 21](#)



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

- [Additional References, page 23](#)
- [Feature Information for Storing PKI Credentials, page 25](#)

## Prerequisites for Storing PKI Credentials

### Prerequisites for Specifying a Local Certificate Storage Location

Before you can specify the local certificate storage location, your system should meet the following requirements:

- A Cisco IOS Release 12.4(2)T PKI-enabled image or a later image
- A platform that supports storing PKI credentials as separate files
- A configuration that contains at least one certificate
- An accessible local file system

### Prerequisites for Specifying USB Token Storage for PKI Credentials

Before you can use a USB token, your system should meet the following requirements:

- A Cisco 871 router, Cisco 1800 series, Cisco 2800 series, a Cisco 3800 series router, or a Cisco 7200VXR NPE-G2 platform
- At least a Cisco IOS Release 12.3(14)T image running on any of the supported platforms
- A Cisco supported USB token
- A k9 image

## Restrictions for Storing PKI Credentials

### Restrictions for Specifying a Local Certificate Storage Location

When storing certificates to a local storage location, the following restrictions are applicable:

- Only local file systems may be used. An error message will be displayed if a remote file system is selected, and the command will not take effect.
- A subdirectory may be specified if supported by the local file system. NVRAM does not support subdirectories.

### Restrictions for Specifying USB Token Storage

When using a USB token to store PKI data, the following restrictions are applicable:

- USB token support requires a 3DES (k9) Cisco IOS software image, which provides secure file storage.
- You cannot boot an image from a USB token. (However, you can boot a configuration from a USB token.)
- USB hubs are currently not supported. Thus, the number of supported devices is limited to the number of available USB ports.

# Information About Storing PKI Credentials

To determine where to store PKI credentials, you should understand the following concepts:

- [Storing Certificates to a Local Storage Location, page 3](#)
- [PKI Credentials and USB Tokens, page 3](#)

## Storing Certificates to a Local Storage Location

Certificates are stored to NVRAM by default, however some routers do not have the required amount of NVRAM to successfully store certificates. Introduced in Cisco IOS Release 12.4(2)T is the ability to specify where certificates are stored on a local file system.

All Cisco platforms support NVRAM and flash local storage. Depending on your platform, you may have other supported local storage options including bootflash, slot, disk, USB flash, or USB token.

During run time, you can specify what active local storage device you would like to use to store certificates.

## PKI Credentials and USB Tokens

To use a secure USB token on your router, you should understand the following concepts:

- [How a USB Token Works, page 3](#)
- [Benefits of USB Tokens, page 4](#)

### How a USB Token Works

A smart card is a small plastic card, containing a microprocessor and memory that allows you to store and process data. A USB token is a smart card with a USB interface. The token can securely store any type of file within its available storage space (32 KB). Configuration files that are stored on the USB token can be encrypted and accessed only via a user PIN. The router will not load the configuration file unless the proper PIN has been configured for secure deployment of router configuration files.

After you plug the USB token into the router, you must log into the USB token; thereafter, you can change default settings, such as the user PIN (default: 1234567890) and the allowed number of failed login attempts (default: 15 attempts) before future logins are refused. For more information on accessing and configuring the USB token, see the section “[Logging Into and Setting Up the USB Token.](#)”

After you have successfully logged into the USB token, you can copy files from the router on to the USB token via the **copy** command. USB token RSA keys and associated IPsec tunnels remain available until the router is reloaded. To specify the length of time before the keys are removed and the IPsec tunnels are torn down, issue the **crypto pki token removal timeout** command.

[Table 1](#) highlights the capabilities of the USB token.

**Table 1**      **Functionality Highlights for USB Tokens**

Function	USB Token
Accessibility	Used to securely store and transfer digital certificates, preshared keys, and router configurations from the USB token to the router.
Storage Size	32 KB

**Table 1**      **Functionality Highlights for USB Tokens (continued)**

Function	USB Token
<b>File Types</b>	<ul style="list-style-type: none"> <li>Typically used to store digital certificates, preshared keys, and router configurations for IPsec VPNs.</li> <li>USB tokens cannot store Cisco IOS images.</li> </ul>
<b>Security</b>	<ul style="list-style-type: none"> <li>Files can be encrypted and accessed only with a user PIN.</li> <li>Files can also be stored in a nonsecure format.</li> </ul>
<b>Boot Configurations</b>	<ul style="list-style-type: none"> <li>The router can use the configuration stored in the USB token during boot time.</li> <li>The router can use the secondary configuration stored in the USB token during boot time. (A secondary configuration allows users to load their IPsec configuration.)</li> </ul>

## Benefits of USB Tokens

USB token support on a Cisco router provides the following application benefits:

### Removable Credentials: Provide or Store VPN Credentials on an External Device for Deployment

A USB token can use smart card technology to store a digital certificate and configuration for IPsec VPN deployment. This ability enhances the capability of the router to generate RSA public keys to authenticate at least one IPsec tunnel. (Because a router can initiate multiple IPsec tunnels, the USB token can contain several certificates, as appropriate.)

Storing VPN credentials on an external device reduces the threat of compromising secure data.

### PIN Configuration for Secure File Deployment

A USB token can store a configuration file that can be used for enabling encryption on the router via a user-configured PIN. (That is, no digital certificates, preshared keys, or VPNs are used.)

### Touchless or Low Touch Configuration

The USB token can provide remote software configuration and provisioning with little or no human interaction. Configuration is set up as an automated process. That is, the USB token can store a bootstrap configuration that the router can use to boot from after the USB token has been inserted into the router. The bootstrap configuration connects the router to a TFTP server, which contains a configuration that completely configures the router.

### RSA Operations

As of Cisco IOS Release 12.4(11)T and later releases, a USB token may be used as a cryptographic device in addition to a storage device. Using a USB token as a cryptographic device allows RSA operations such as key generation, signing, and authentication to be performed on the token.

General-purpose, special-usage, encryption, or signature RSA key pairs with a modulus of 2048 bits or less may be generated from credentials located on your token storage device. Private keys are not distributed and remain on the token by default, however you may configure the private key storage location.

Keys that reside on a USB token are saved to persistent token storage when they are generated. Key deletion will remove the keys stored on the token from persistent storage immediately. (Keys that do not reside on a token are saved to or deleted from nontoken storage locations when the **write memory** or a similar command is issued.)



Remote Device Configuration and Provisioning in a Secure Device Provisioning (SDP) Environment

As of Cisco IOS Release 12.4(15)T and later releases, SDP may be used to configure a USB token. The configured USB token may be transported to provision a device at a remote location. That is, a USB token may be used to transfer cryptographic information from one network device to another remote network device providing a solution for a staged USB token deployment.

For information about using USB tokens with SDP, see document titles in the “[Related Documents](#)” section.

## How to Configure PKI Storage

This section contains the following configuration tasks:

- [Specifying a Local Storage Location for Certificates, page 5](#)
- [Setting Up and Using USB Tokens on Cisco Routers, page 6](#)
- [Troubleshooting USB Tokens, page 16](#)

### Specifying a Local Storage Location for Certificates

The following procedure allows you to specify the local storage location for certificates.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. `crypto pki certificate storage location-name`
4. `exit`
5. **copy** *source-url destination-url*
6. `show crypto pki certificates storage`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto pki certificate storage</b> <i>location-name</i>  <b>Example:</b> Router(config)# crypto pki certificate storage flash:/certs	Specifies the local storage location for certificates.
Step 4	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits global configuration mode.
Step 5	<b>copy</b> <i>source-url destination-url</i>  <b>Example:</b> Router# copy system:running-config nvram:startup-config	(Optional) Saves the running configuration to the startup configuration.  <b>Note</b> Settings will only take effect when the running configuration is saved to the startup configuration.
Step 6	<b>show crypto pki certificates storage</b>  <b>Example:</b> Router# show crypto pki certificates storage	(Optional) Displays the current setting for the PKI certificate storage location.

## Examples

The following is sample output for the **show crypto pki certificates storage** command where the certificates are stored in the certs subdirectory of disk0:

```
Router# show crypto pki certificates storage
```

```
Certificates will be stored in disk0:/certs/
```

## Setting Up and Using USB Tokens on Cisco Routers

This section contains the following procedures that allow you to configure a router to support USB tokens:

- [Storing the Configuration on a USB Token, page 7](#)
- [Logging Into and Setting Up the USB Token, page 7](#)
- [Configuring the USB Token, page 10](#)
- [Setting Administrative Functions on the USB Token, page 13](#)

## Storing the Configuration on a USB Token

Perform this task to store the configuration file in a USB token.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **boot config usbtoken[0-9]:filename**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>boot config usbtoken[0-9]:filename</b>  <b>Example:</b> Router(config)# boot config usbtoken0:file	Specifies that the startup configuration file is stored in a secure USB token.

## Logging Into and Setting Up the USB Token

Perform this task to log into and to perform the initial set up of a USB token.

### Use of RSA Keys with a USB Token

- RSA keys are loaded after the USB token is successfully logged into the router.
- By default, newly generated RSA keys are stored on the most recently inserted USB token. Regenerated keys should be stored in the same location where the original RSA key was generated.

### Automatic Login

Automatic login allows the router to completely come back up without any user or operator intervention. The PIN is stored in the private NVRAM, so it is not visible in the startup or running configuration.



#### Note

A hand-generated startup configuration can contain the automatic login command for deployment purposes, but the **copy system:running-config nvram: startup-config** command must be issued to put the hand-generated configuration in the private configuration.

### Manual Login

Unlike automatic login, manual login requires that the user know the actual USB token PIN.

Manual login can be used when storing a PIN on the router is not desirable. Manual login may also be suitable for some initial deployment or hardware replacement scenarios for which the router is obtained from the local supplier or drop-shipped to the remote site. Manual login can be executed with or without privileges, and it will make files and RSA keys on the USB token available to the Cisco IOS software. If a secondary configuration file is configured, it will be executed only with the privileges of the user who is performing the login. Thus, if you want to use manual login and set up the secondary configuration on the USB token to perform anything useful, you need to enable privileges.

Manual login can also be used in recovery scenarios for which the router configuration has been lost. If the scenario contains a remote site that normally connects to the core network with a VPN, the loss of the configuration and RSA keys requires out-of-band services that the USB token can provide. The USB token can contain a boot configuration, a secondary configuration, or both, and RSA keys to authenticate the connection.

## SUMMARY STEPS

1. **enable**
2. **crypto pki token** *token-name* [**admin**] **login** [*pin*]  
or  
**configure terminal**
3. **crypto pki token** *token-name* **user-pin** [*pin*]
4. **exit**
5. **show usbtoken**[0-9]:*filename*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>crypto pki token token-name [admin] login [pin]</b>  <b>Example:</b> Router# crypto pki token usbtokens0 admin login 5678  or <b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Manually logs into the USB token.  You must specify the <b>admin</b> keyword if later you want to change the user PIN.  or  Puts the router in global configuration mode, which allows you to configure automatic USB token login.
Step 3	<b>crypto pki token token-name user-pin [pin]</b>  <b>Example:</b> Router(config)# crypto pki token usbtokens0 user-pin 1234	(Optional) Configures the router to log into the token automatically, using the specified PIN at router startup or when the USB token is inserted into a USB slot.  The PIN is encrypted and stored in NVRAM.  <b>Note</b> You will be asked to enter your passphrase.
Step 4	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits global configuration mode.
Step 5	<b>show usbtokens[0-9]:filename</b>  <b>Example:</b> Router# show usbtokens0:usbfile	(Optional) Verifies whether the USB token has been logged onto the router.

## What to Do Next

After you have logged into the USB token, it is available for use.

- To further configure the USB token, see the “[Configuring the USB Token](#)” section.
- To perform USB token administrative tasks, such as changing the user PIN, copying files from the router to the USB token set key storage location, and changing USB tokens, see the “[Setting Administrative Functions on the USB Token](#)” section.
- To utilize the USB token as a cryptographic device to perform RSA operations, see the document titles in the “[Related Documents](#)” section.
- To specify that the USB token be used for RSA operations during initial autoenrollment, see the document titles in the “[Related Documents](#)” section.

## Configuring the USB Token

After you have set up automatic login, you may perform this task to further configure the USB token.

### PINs and Passphrases

For additional PIN security with automatic login, you may encrypt your PIN stored in NVRAM and set up a passphrase for your USB token. Establishing a passphrase allows you to keep your PIN secure; another user needs only to know the passphrase, not the PIN.

When the USB token is inserted into the router, the passphrase is needed to decrypt the PIN. Once the PIN is decrypted, the router can then use the PIN to login the USB token.

**Note**

The user has only the access they would normally have and needs only privilege level 1 to log in.

### Unlocking and Locking the USB Token

The USB token itself can be locked (encrypted) or unlocked (decrypted).

Unlocking the USB token allows it to be used. Once unlocked, Cisco IOS treats the token as if it were automatically logged in. Any keys on the USB token are loaded, and if a secondary configuration file is on the token, it is executed with full user privileges (privilege level 15) independent of the privilege level of the logged-in user.

Locking the token, unlike logging out of the token, deletes any RSA keys loaded from the token and runs the secondary unconfiguration file, if configured.

### Secondary Configuration and Unconfiguration Files

Configuration files that exist on a USB token are called secondary configuration files. If you create and configure a secondary configuration file, it is executed after the token is logged in. The existence of a secondary configuration file is determined by the presence of a secondary configuration file option in the Cisco IOS configuration stored in NVRAM. When the token is removed or logged out and the removal timer expires, a separate secondary unconfiguration file is processed to remove all secondary configuration elements from the running configuration. Secondary configuration and secondary unconfiguration files are executed at privilege level 15 and are not dependent on the level of the user logged in.

### SUMMARY STEPS

1. **enable**
2. **crypto pki token *token-name* unlock [*pin*]**
3. **configure terminal**
4. **crypto pki token *token-name* encrypted-user-pin [write]**
5. **crypto pki token *token-name* secondary unconfig *file***
6. **exit**
7. **crypto pki token *token-name* lock [*pin*]**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>crypto pki token token-name unlock [pin]</b>  <b>Example:</b> Router# crypto pki token mytoken unlock mypin	(Optional) Allows the token to be used if the USB token has been locked.  Once unlocked, Cisco IOS treats the token as if it has been automatically logged in. Any keys on the token are loaded and if a secondary configuration file exists, it is executed.
Step 3	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 4	<b>crypto pki token token-name encrypted-user-pin [write]</b>  <b>Example:</b> Router(config)# crypto pki token mytoken encrypted-user-pin write	(Optional) Encrypts the stored PIN in NVRAM.
Step 5	<b>crypto pki token token-name secondary unconfig file</b>  <b>Example:</b> Router(config)# crypto pki token mytoken secondary unconfig configs/myunconfigfile.cfg	(Optional) Specifies the secondary configuration file and its location.
Step 6	<b>exit</b>  <b>Example:</b> Router(config)# exit	Enters privileged EXEC mode.
Step 7	<b>crypto pki token token-name lock [pin]</b>  <b>Example:</b> Router# crypto pki token mytoken lock mypin	(Optional) Deletes any RSA keys loaded from the token and runs the secondary unconfiguration file, if it exists.

## Examples

The following example shows both the configuration and encryption of a user PIN and then the router reloading and the user PIN being unlocked:

```
! Configuring the user PIN
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)# crypto pki token usbtoken0: user-pin
```

```
Enter password:
```

```
! Encrypt the user PIN
```

```

Router (config)# crypto pki token usbtoken0: encrypted-user-pin
 Enter passphrase:
Router(config)# exit
Router#
Sep 20 21:51:38.076: %SYS-5-CONFIG_I: Configured from console by console
!

Router# show running config
.
.
.
crypto pki token usbtoken0 user-pin *encrypted*
.
.
.

! Reloading the router.
!
Router> enable
Password:
!
! Decrypting the user pin.
!
Router# crypto pki token usbtoken0: unlock
Token eToken is usbtoken0
!
Enter passphrase:
Token login to usbtoken0(eToken) successful
Router#
Sep 20 22:31:13.128: %CRYPTO-6-TOKENLOGIN: Cryptographic Token eToken
Login Successful

```

The following example shows how a secondary unconfiguration file might be used to remove secondary configuration elements from the running configuration. For example, a secondary configuration file might be used to set up a PKI trustpoint. A corresponding unconfiguration file, named `mysecondaryunconfigfile.cfg`, might contain this command line:

```
no crypto pki trustpoint token-tp
```

If the token were removed and the following commands executed, the trustpoint and associated certificates would be removed from the router's running configuration:

```

Router# configure terminal
Router(config)# no crypto pki token mytoken secondary unconfig mysecondaryunconfigfile.cfg

```

## What to Do Next

After you have logged into and configured the USB token, it is available for use.

- To perform USB token administrative tasks, such as changing the user PIN, copying files from the router to the USB token set key storage location, and changing USB tokens, see the “[Setting Administrative Functions on the USB Token](#)” section.
- To utilize the USB token as a cryptographic device to perform RSA operations, see the document titles in the “[Related Documents](#)” section.



- To specify that the USB token be used for RSA operations during initial autoenrollment, see the document titles in the “[Related Documents](#)” section.

## Setting Administrative Functions on the USB Token

Perform this task to change default settings, such as the user PIN, the maximum number of failed attempts on the USB token, or the credential storage location.

### SUMMARY STEPS

1. **enable**
2. **crypto pki token** *token-name* [**admin**] **change-pin** [*pin*]
3. **crypto pki token** *token-name* **device:** **label** *token-label*
4. **configure terminal**
5. **crypto key storage** *device:*
6. **crypto key generate rsa** [**general-keys** | **usage-keys** | **signature** | **encryption**] [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] [**storage** *devicename:*] [**on** *devicename:*]
7. **crypto key move rsa** *keylabel* [**non-exportable**] [**on** | **storage**] *location*
8. **crypto pki token** {*token-name* | **default**} **removal timeout** [*seconds*]
9. **crypto pki token** {*token-name* | **default**} **max-retries** [*number*]
10. **exit**
11. **copy usbflash**[0-9]:*filename* *destination-url*
12. **show usbtok**[0-9]:*filename*
13. **crypto pki token** *token-name* **logout**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>crypto pki token token-name [admin] change-pin [pin]</b>  <b>Example:</b> Router# crypto pki token usbtoken0 admin change-pin	(Optional) Changes the user PIN number on the USB token. <ul style="list-style-type: none"> <li>If the PIN is not changed, the default PIN—1234567890—will be used.</li> </ul> <b>Note</b> After the PIN has been changed, you must reset the login failure count to zero (via the <b>crypto pki token max-retries</b> command). The maximum number of allowable login failures is set (by default) to 15.
Step 3	<b>crypto pki token token-name device: label token-label</b>  <b>Example:</b> Router# crypto pki token my token usb0: label newlabel	(Optional) Sets or changes the name of the USB token. <ul style="list-style-type: none"> <li>The value of the <i>token-label</i> argument may be up to 31 alphanumeric characters in length including dashes and underscores.</li> </ul> <b>Tip</b> This command is useful when configuring multiple USB tokens for automatic login, secondary configuration files, or other token specific settings.
Step 4	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 5	<b>crypto key storage device:</b>  <b>Example:</b> Router(config)# crypto key storage usbtoken0:	(Optional) Sets the default RSA key storage location for newly created keys. <b>Note</b> Regardless of configuration settings, existing keys are stored on the device from where they were originally loaded.
Step 6	<b>crypto key generate rsa [general-keys   usage-keys   signature   encryption] [label key-label] [exportable] [modulus modulus-size] [storage devicename:] [on devicename:]</b>  <b>Example:</b> Router(config)# crypto key generate rsa label tokenkey1 storage usbtoken0:	(Optional) Generates the RSA key pair. <ul style="list-style-type: none"> <li>The <b>storage</b> keyword specifies the key storage location.</li> <li>The <b>on</b> keyword specifies that the keys will be generated on the designated device.</li> </ul>

	Command or Action	Purpose
Step 7	<p><b>crypto key move rsa</b> <i>keylabel</i> [<b>non-exportable</b>] [<b>on</b>   <b>storage</b>] <i>location</i></p> <p><b>Example:</b> Router(config)# crypto key move rsa keypairname non-exportable on token</p>	<p>(Optional) Moves existing Cisco IOS credentials from the current storage location to the specified storage location.</p> <p>By default, the RSA key pair remains stored on the current device.</p> <p>Generating the key on the router and moving it to the token takes less than a minute. Generating a key on the token, using the <b>on</b> keyword could take five to ten minutes, and is dependent on hardware key generation routines available on the USB token.</p> <p>When an existing RSA key pair is generated in Cisco IOS, stored on a USB token, and used for an enrollment, it may be necessary to move those existing RSA key pairs to an alternate location for permanent storage.</p> <p>This command is useful when using SDP with USB tokens to deploy credentials.</p>
Step 8	<p><b>crypto pki token</b> {<i>token-name</i>   <b>default</b>} <b>removal timeout</b> [<i>seconds</i>]</p> <p><b>Example:</b> Router(config)# crypto pki token usbtokens removal timeout 60</p>	<p>(Optional) Sets the time interval, in seconds, that the router will wait before removing the RSA keys that are stored in the USB token after the USB token has been removed from the router.</p> <p><b>Note</b> If this command is not issued, all RSA keys and IPsec tunnels associated with the USB token are torn down immediately after the USB token is removed from the router.</p>
Step 9	<p><b>crypto pki token</b> {<i>token-name</i>   <b>default</b>} <b>max-retries</b> [<i>number</i>]</p> <p><b>Example:</b> Router(config)# crypto pki token usbtokens max-retries 20</p>	<p>(Optional) Sets the maximum number of consecutive failed login attempts allowed before access to the USB token is denied.</p> <ul style="list-style-type: none"> <li>By default, the value is set at 15.</li> </ul>
Step 10	<p><b>exit</b></p> <p><b>Example:</b> Router(config)# exit</p>	Exits global configuration mode.
Step 11	<p><b>copy</b> usbflash[0-9]:<i>filename</i> <i>destination-url</i></p> <p><b>Example:</b> Router# copy usbflash0:file1 nvram:</p>	<p>Copies files from USB token to the router.</p> <ul style="list-style-type: none"> <li><i>destination-url</i>—See the <b>copy</b> command page documentation for a list of supported options.</li> </ul>
Step 12	<p><b>show usbtoken</b>[0-9]:<i>filename</i></p> <p><b>Example:</b> Router# show usbtoken:usbfile</p>	(Optional) Displays information about the USB token. You can use this command to verify whether the USB token has been logged onto the router.
Step 13	<p><b>crypto pki token</b> <i>token-name</i> <b>logout</b></p> <p><b>Example:</b> Router# crypto pki token usbtokens logout</p>	<p>Logs the router out of the USB token.</p> <p><b>Note</b> If you want to save any data to the USB token, you must log back into the token.</p>

## Troubleshooting USB Tokens

This section contains descriptions of the following Cisco IOS commands that can be used to help troubleshoot possible problems that may arise while using a USB token:

- [The show file systems Command, page 16](#)
- [The show usb device Command, page 17](#)
- [The show usb controllers Command, page 17](#)
- [The dir Command, page 19](#)

### The show file systems Command

Use the **show file systems** command to determine whether the router recognizes that there is a USB module plugged into a USB port. The USB module should appear on the list of file systems. If the module does not appear on the list, it can indicate any of the following problems:

- A connection problem with the USB module.
- The Cisco IOS image running on the router does not support a USB module.
- A hardware problem with the USB module itself.

### SUMMARY STEPS

1. **show file systems**

### DETAILED STEPS

- Step 1** Sample output from the **show file systems** command showing a USB token appears below. The USB module listing appears in the last line of the examples.

```
Router# show file systems
```

```
File Systems:
```

	Size(b)	Free(b)	Type	Flags	Prefixes
	-	-	opaque	rw	archive:
	-	-	opaque	rw	system:
	-	-	opaque	rw	null:
	-	-	network	rw	tftp:
*	129880064	69414912	disk	rw	flash:#
	491512	486395	nvr	rw	nvr
	-	-	opaque	wo	syslog:
	-	-	opaque	rw	xmodem:
	-	-	opaque	rw	ymodem:
	-	-	network	rw	rcp:
	-	-	network	rw	pram:
	-	-	network	rw	ftp:
	-	-	network	rw	http:
	-	-	network	rw	scp:
	-	-	network	rw	https:
	-	-	opaque	ro	cns:
	63158272	33037312	usbflash	rw	usbflash0:
	32768	858	usbtoken	rw	usbtoken1:

## The show usb device Command

Use the **show usb device** command to determine if a USB token is supported by Cisco.

### SUMMARY STEPS

1. **show usb device**

### DETAILED STEPS

- Step 1** The following sample output for the **show usb device** command indicates whether or not the module is supported is bold in the sample output below:

```
Router# show usb device

Host Controller:1
Address:0x11
Device Configured:YES
Device Supported:YES
Description:eToken Pro 4254
Manufacturer:AKS
Version:1.0
Serial Number:
Device Handle:0x1010000
USB Version Compliance:1.0
Class Code:0xFF
Subclass Code:0x0
Protocol:0x0
Vendor ID:0x529
Product ID:0x514
Max. Packet Size of Endpoint Zero:8
Number of Configurations:1
Speed:Low
Selected Configuration:1
Selected Interface:0

Configuration:
 Number:1
 Number of Interfaces:1
 Description:
 Attributes:None
 Max Power:60 mA

 Interface:
 Number:0
 Description:
 Class Code:255
 Subclass:0
 Protocol:0
 Number of Endpoints:0
```

## The show usb controllers Command

Use the **show usb controllers** command to determine if there is a hardware problem with a USB flash module. If the **show usb controllers** command displays an error, the error indicates a hardware problem in the USB module.

You can also use the **show usb controllers** command to verify that copy operations onto a USB flash module are occurring successfully. Issuing the **show usb controllers** command after performing a file copy should display successful data transfers.

## SUMMARY STEPS

### 1. show usb controllers

## DETAILED STEPS

- Step 1** The following sample output for the **show usb controllers** command displays a working USB flash module:

```
Router# show usb controllers

Name:1362HCD
Controller ID:1
Controller Specific Information:
 Revision:0x11
 Control:0x80
 Command Status:0x0
 Hardware Interrupt Status:0x24
 Hardware Interrupt Enable:0x80000040
 Hardware Interrupt Disable:0x80000040
 Frame Interval:0x27782EDF
 Frame Remaining:0x13C1
 Frame Number:0xDA4C
 LSThreshold:0x628
 RhDescriptorA:0x19000202
 RhDescriptorB:0x0
 RhStatus:0x0
 RhPort1Status:0x100103
 RhPort2Status:0x100303
 Hardware Configuration:0x3029
 DMA Configuration:0x0
 Transfer Counter:0x1
 Interrupt:0x9
 Interrupt Enable:0x196
 Chip ID:0x3630
 Buffer Status:0x0
 Direct Address Length:0x80A00
 ATL Buffer Size:0x600
 ATL Buffer Port:0x0
 ATL Block Size:0x100
 ATL PTD Skip Map:0xFFFFFFFF
 ATL PTD Last:0x20
 ATL Current Active PTD:0x0
 ATL Threshold Count:0x1
 ATL Threshold Timeout:0xFF

Int Level:1
Transfer Completion Codes:
 Success :920 CRC :0
 Bit Stuff :0 Stall :0
 No Response :0 Overrun :0
 Underrun :0 Other :0
 Buffer Overrun :0 Buffer Underrun:0

Transfer Errors:
 Canceled Transfers :2 Control Timeout :0

Transfer Failures:
 Interrupt Transfer :0 Bulk Transfer :0
```

```

 Isochronous Transfer :0
Transfer Successes:
 Interrupt Transfer :0
 Isochronous Transfer :0
 Control Transfer:0
 Bulk Transfer :26
 Control Transfer:894

USBD Failures:
 Enumeration Failures :0
 Power Budget Exceeded:0
 No Class Driver Found:0

USB MSCD SCSI Class Driver Counters:
 Good Status Failures :3
 Good Status Timed out:0
 Device Never Opened :0
 Illegal App Handle :0
 Invalid Unit Number :0
 Application Overflow :0
 Control Pipe Stall :0
 Device Stalled :0
 Device Detached :0
 Invalid Logic Unit Num:0
 Command Fail :0
 Device not Found:0
 Drive Init Fail :0
 Bad API Command :0
 Invalid Argument:0
 Device in use :0
 Malloc Error :0
 Bad Command Code:0
 Unknown Error :0

USB Aladdin Token Driver Counters:
 Token Inserted :1
 Send Insert Msg Fail :0
 Dev Entry Add Fail :0
 Dev Entry Remove Fail:0
 Response Txn Fail :0
 Txn Invalid Dev Handle:0
 Token Removed :0
 Response Txns :434
 Request Txns :434
 Request Txn Fail:0
 Command Txn Fail:0

USB Flash File System Counters:
 Flash Disconnected :0
 Flash Device Fail :0
 Flash startstop Fail :0
 Flash Connected :1
 Flash Ok :1
 Flash FS Fail :0

USB Secure Token File System Counters:
 Token Inserted :1
 Token FS success :1
 Token Max Inserted :0
 Token Event :0
 Watched Boolean Create Failures:0
 Token Detached :0
 Token FS Fail :0
 Create Talker Failures:0
 Destroy Talker Failures:0

```

---

## The dir Command

Use the **dir** command with the **filesystem** keyword option **usbtoken[0-9]:** to display all files, directories, and their permission strings on the USB token.

### SUMMARY STEPS

1. **dir [filesystem: ]**

## DETAILED STEPS

**Step 1** The following sample output displays directory information for the USB token:

```
Router# dir usbtoken1:
```

```
Directory of usbtoken1:/
```

```

 2 d--- 64 Dec 22 2032 05:23:40 +00:00 1000
 5 d--- 4096 Dec 22 2032 05:23:40 +00:00 1001
 8 d--- 0 Dec 22 2032 05:23:40 +00:00 1002
10 d--- 512 Dec 22 2032 05:23:42 +00:00 1003
12 d--- 0 Dec 22 2032 05:23:42 +00:00 5000
13 d--- 0 Dec 22 2032 05:23:42 +00:00 6000
14 d--- 0 Dec 22 2032 05:23:42 +00:00 7000
15 ---- 940 Jun 27 1992 12:50:42 +00:00 mystartup-config
16 ---- 1423 Jun 27 1992 12:51:14 +00:00 myrunning-config
```

```
32768 bytes total (858 bytes free)
```

The following sample output displays directory information for all devices the router is aware of:

```
Router# dir all-filesystems
```

```
Directory of archive:/
```

```
No files in directory
```

```
No space information available
```

```
Directory of system:/
```

```

 2 drwx 0 <no date> its
115 dr-x 0 <no date> lib
144 dr-x 0 <no date> memory
 1 -rw- 1906 <no date> running-config
114 dr-x 0 <no date> vfiles
```

```
No space information available
```

```
Directory of flash:/
```

```
 1 -rw- 30125020 Dec 22 2032 03:06:04 +00:00 c3825-entservicesk9-mz.123-14.T
```

```
129880064 bytes total (99753984 bytes free)
```

```
Directory of nvram:/
```

```

476 -rw- 1947 <no date> startup-config
477 ---- 46 <no date> private-config
478 -rw- 1947 <no date> underlying-config
 1 -rw- 0 <no date> ifIndex-table
 2 ---- 4 <no date> rf_cold_starts
 3 ---- 14 <no date> persistent-data
```

```
491512 bytes total (486395 bytes free)
```

```
Directory of usbflash0:/
```

```
 1 -rw- 30125020 Dec 22 2032 05:31:32 +00:00 c3825-entservicesk9-mz.123-14.T
```

```
63158272 bytes total (33033216 bytes free)
```

```
Directory of usbtoken1:/
```

```

 2 d--- 64 Dec 22 2032 05:23:40 +00:00 1000
 5 d--- 4096 Dec 22 2032 05:23:40 +00:00 1001
 8 d--- 0 Dec 22 2032 05:23:40 +00:00 1002
```



```

10 d--- 512 Dec 22 2032 05:23:42 +00:00 1003
12 d--- 0 Dec 22 2032 05:23:42 +00:00 5000
13 d--- 0 Dec 22 2032 05:23:42 +00:00 6000
14 d--- 0 Dec 22 2032 05:23:42 +00:00 7000
15 ---- 940 Jun 27 1992 12:50:42 +00:00 mystartup-config
16 ---- 1423 Jun 27 1992 12:51:14 +00:00 myrunning-config

```

32768 bytes total (858 bytes free)

## Configuration Examples for PKI Storage

This section contains the following configuration examples:

- [Storing Certificates to a Specific Local Storage Location: Example, page 21](#)
- [Logging Into a USB Token and Saving RSA Keys to the USB Token: Example, page 22](#)

### Storing Certificates to a Specific Local Storage Location: Example

The following configuration example shows how to store certificates to the certs subdirectory. The certs subdirectory does not exist and is automatically created.

Router# **dir nvram:**

```

114 -rw- 4687 <no date> startup-config
115 ---- 5545 <no date> private-config
116 -rw- 4687 <no date> underlying-config
 1 ---- 34 <no date> persistent-data
 3 -rw- 707 <no date> ioscaroot#7401CA.cer
 9 -rw- 863 <no date> msca-root#826E.cer
10 -rw- 759 <no date> msca-root#1BA8CA.cer
11 -rw- 863 <no date> msca-root#75B8.cer
24 -rw- 1149 <no date> storagename#6500CA.cer
26 -rw- 863 <no date> msca-root#83EE.cer

```

129016 bytes total (92108 bytes free)

Router# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# **crypto pki certificate storage disk0:/certs**

Requested directory does not exist -- created

Certificates will be stored in disk0:/certs/

Router(config)# **end**

Router# **write**

\*May 27 02:09:00:%SYS-5-CONFIG\_I:Configured from console by consolemem

Building configuration...

[OK]

Router# **directory disk0:/certs**

Directory of disk0:/certs/

```

14 -rw- 707 May 27 2005 02:09:02 +00:00 ioscaroot#7401CA.cer
15 -rw- 863 May 27 2005 02:09:02 +00:00 msca-root#826E.cer
16 -rw- 759 May 27 2005 02:09:02 +00:00 msca-root#1BA8CA.cer
17 -rw- 863 May 27 2005 02:09:02 +00:00 msca-root#75B8.cer
18 -rw- 1149 May 27 2005 02:09:02 +00:00 storagename#6500CA.cer

```

```

19 -rw- 863 May 27 2005 02:09:02 +00:00 msca-root#83EE.cer

47894528 bytes total (20934656 bytes free)

! The certificate files are now on disk0/certs:

```

## Logging Into a USB Token and Saving RSA Keys to the USB Token: Example

The following configuration example shows to how log into the USB token, generate RSA keys, and store the RSA keys onto the USB token:

```

! Configure the router to automatically log into the eToken
configure terminal
 crypto pki token default user-pin 0 1234567890
! Generate RSA keys and enroll certificates with the CA.
crypto pki trustpoint IOSCA
 enrollment url http://10.23.2.2
exit
crypto ca authenticate IOSCA
Certificate has the following attributes:
 Fingerprint MD5:23272BD4 37E3D9A4 236F7E1A F534444E
 Fingerprint SHA1:D1B4D9F8 D603249A 793B3CAF 8342E1FE 3934EB7A

% Do you accept this certificate? [yes/no]:yes
Trustpoint CA certificate accepted.
crypto pki enroll
crypto pki enroll IOSCA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will include:c2851-27.cisco.com
% Include the router serial number in the subject name? [yes/no]:no
% Include an IP address in the subject name? [no]:no
Request certificate from CA? [yes/no]:yes
% Certificate request sent to Certificate Authority
% The 'show crypto ca certificate IOSCA verbose' command will show the fingerprint.

*Jan 13 06:47:19.413:CRYPTO_PKI: Certificate Request Fingerprint MD5:E6DDAB1B
0E30EFE6 54529D8A DA787DBA
*Jan 13 06:47:19.413:CRYPTO_PKI: Certificate Request Fingerprint SHA1:3B0F33B
7 57C02A10 3935042B C4B6CD3D 61039251
*Jan 13 06:47:21.021:%PKI-6-CERTRET:Certificate received from Certificate Authority
! Issue the write memory command, which will automatically save the RSA keys to the eToken
! instead of private NVRAM.
Router# write memory
Building configuration...
[OK]

*Jan 13 06:47:29.481:%CRYPTO-6-TOKENSTOREKEY:Key c2851-27.cisco.com stored on
Cryptographic Token eToken Successfully

```

The following sample output from the **show crypto key mypubkey rsa** command displays stored credentials after they are successfully loaded from the USB token. Credentials that are stored on the USB token are in the protected area. When storing the credentials on the USB token, the files are stored in a directory called /keystore. However, the key files are hidden from the command-line interface (CLI).

```
Router# show crypto key mypubkey rsa

% Key pair was generated at:06:37:26 UTC Jan 13 2005
Key name:c2851-27.cisco.com
Usage:General Purpose Key
Key is not exportable.
Key Data:
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E3C644 43AA7DDD
 732E0F4E 3CA0CDAB 387ABF05 EB8F22F2 2431F1AE 5D51FEE3 FCDEA934 7FBD3603
 7C977854 B8E999BF 7FC93021 7F46ABF8 A4BA2ED6 172D3D09 B5020301 0001
% Key pair was generated at:06:37:27 UTC Jan 13 2005
Key name:c2851-27.cisco.com.server
Usage:Encryption Key
Key is not exportable.
Key Data:
 307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00DD96AE 4BF912EB
 2C261922 4784EF98 2E70E837 774B3778 7F7AEB2D 87F5669B BF5DDFBC F0D521A5
 56AB8FDC 9911968E DE347FB0 A514A856 B30EAFF4 D1F453E1 003CFE65 0CCC6DC7
 21FBE3AC 2F8DEA16 126754BC 1433DEF9 53266D33 E7338C95 BB020301 0001
```

## Additional References

The following sections provide references related to PKI storage support.

## Related Documents

Related Topic	Document Title
Connecting the USB modules to the router	<a href="#">Cisco Access Router USB Flash Module and USB eToken Hardware Installation Guide</a>
eToken and USB flash data sheet	<a href="#">USB eToken and USB Flash Features Support</a>
RSA keys	<a href="#">Deploying RSA Keys Within a PKI</a>
File management (loading, copying, and rebooting files)	<a href="#">Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.4</a>
USB Token RSA Operations: Certificate server configuration	<p>“Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment” chapter in the <a href="#">Cisco IOS Security Configuration Guide</a>, Release 12.4T.</p> <p>See the “Generating a Certificate Server RSA Key Pair” section, the “Configuring a Certificate Server Trustpoint” section, and related examples.</p>
USB Token RSA Operations: Using USB tokens for RSA operations upon initial autoenrollment	<p>“Configuring Certificate Enrollment for a PKI” chapter in the <a href="#">Cisco IOS Security Configuration Guide</a>, Release 12.4T.</p> <p>See the “Configuring Certificate Enrollment or Autoenrollment” section.</p>
SDP setup, configuration and use with USB tokens	<p>“Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI” chapter in the <a href="#">Cisco IOS Security Configuration Guide</a>, Release 12.4T.</p> <p>See the feature information section for the feature names on using SDP and USB tokens to deploy PKI credentials.</p>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Feature Information for Storing PKI Credentials

Table 2 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Implementing and Managing PKI Features Roadmap](#).”

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 2**      **Feature Information for Storing PKI Credentials**

Feature Name	Releases	Feature Information
USB Token and Secure Device Provisioning (SDP) Integration	12.4(15)T	<p>This feature provides the ability to provision remote devices with USB tokens using SDP.</p> <p>The following sections in this document provide information about this feature:</p> <ul style="list-style-type: none"><li>• <a href="#">Benefits of USB Tokens</a></li><li>• <a href="#">Setting Administrative Functions on the USB Token</a></li></ul> <p>The following commands were introduced by this feature: <b>binary file, crypto key move rsa, template file.</b></p> <p><b>Note</b> This document introduces the benefits of using USB tokens and SDP for a deployment solution. For other documentation on this topic, see the “<a href="#">Related Documents</a>” section.</p>

**Table 2** *Feature Information for Storing PKI Credentials (continued)*

Feature Name	Releases	Feature Information
Cisco IOS USB Token PKI Enhancements — Phase 2	12.4(11)T	<p>This feature enhances USB token functionality by using the USB token as a cryptographic device. USB tokens may be used for RSA operations such as key generation, signing, and authentication.</p> <p>The following sections in this document provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Benefits of USB Tokens</a></li> <li>• <a href="#">Logging Into and Setting Up the USB Token</a></li> <li>• <a href="#">Setting Administrative Functions on the USB Token</a></li> </ul> <p><b>Note</b> This document introduces the benefits of using USB tokens and the keys on the token for RSA operations. For other documentation on this topic, see the “<a href="#">Related Documents</a>” section.</p>
USB Storage PKI Enhancements	12.4(4)T 12.4(11)T	<p>This feature enhances the USB token PIN security for automatic login and increases the flexibility of USB token configuration and the RSA key storage.</p> <p>Cisco IOS Release 12.4(11)T introduced support for USB Storage on NPE-G2.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuring the USB Token</a></li> <li>• <a href="#">Setting Administrative Functions on the USB Token</a></li> </ul> <p>The following commands were introduced or modified by this feature: <b>crypto key storage</b>, <b>crypto pki generate rsa</b>, <b>crypto pki token encrypted-user-pin</b>, <b>crypto pki token label</b>, <b>crypto pki token lock</b>, <b>crypto pki token secondary unconfig</b>, <b>crypto pki token unlock</b></p>
Certificate — Storage Location Specification	12.2(33)SXH 12.2(33)SRA 12.4(2)T	<p>This feature allows you to specify the storage location of local certificates for platforms that support storing certificates as separate files. All Cisco platforms support NVRAM, which is the default location, and flash local storage. Depending on your platform, you may have other supported local storage options including bootflash, slot, disk, USB flash, or USB token.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Storing Certificates to a Local Storage Location</a></li> <li>• <a href="#">Specifying a Local Storage Location for Certificates</a></li> <li>• <a href="#">Storing Certificates to a Specific Local Storage Location: Example</a></li> </ul> <p>The following commands were introduced by this feature: <b>crypto pki certificate storage</b>, <b>show crypto pki certificates storage</b></p>

**Table 2**      **Feature Information for Storing PKI Credentials (continued)**

Feature Name	Releases	Feature Information
USB Storage	12.3(14)T 12.4(11)T	<p>This feature enables certain models of Cisco routers to support USB tokens. USB tokens provide secure configuration distribution and allow users to VPN credentials for deployment.</p> <p>Cisco IOS Release 12.4(11)T introduced support for USB Storage on NPE-G2.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">PKI Credentials and USB Tokens</a></li> <li>• <a href="#">Setting Up and Using USB Tokens on Cisco Routers</a></li> <li>• <a href="#">Troubleshooting USB Tokens</a></li> <li>• <a href="#">Logging Into a USB Token and Saving RSA Keys to the USB Token: Example</a></li> </ul> <p>The following commands were introduced or modified by this feature: <b>copy</b>, <b>crypto pki token change-pin</b>, <b>crypto pki token login</b>, <b>crypto pki token logout</b>, <b>crypto pki token max-retries</b>, <b>crypto pki token removal timeout</b>, <b>crypto pki token secondary config</b>, <b>crypto pki token user-pin</b>, <b>debug usb driver</b>, <b>dir</b>, <b>show usb controllers</b>, <b>show usb device</b>, <b>show usb driver</b>, <b>show usbtokn</b></p>
Certificate - Storage Location Specification	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.







## **Other Security Features**





# Neighbor Router Authentication: Overview and Guidelines

---

You can prevent your router from receiving fraudulent route updates by configuring neighbor router authentication.

This chapter describes neighbor router authentication as part of a total security plan. It describes what neighbor router authentication is, how it works, and why you should use it to increase your overall network security.

This chapter refers to neighbor router authentication as “neighbor authentication.” Neighbor router authentication is also sometimes called “route authentication.”

## In This Chapter

This chapter describes the following topics:

- [About Neighbor Authentication](#)
- [How Neighbor Authentication Works](#)
- [Key Management \(Key Chains\)](#)
- [Finding Neighbor Authentication Configuration Information](#)

## About Neighbor Authentication

This section contains the following sections:

- [Benefits of Neighbor Authentication](#)
- [Protocols That Use Neighbor Authentication](#)
- [When to Configure Neighbor Authentication](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

## Benefits of Neighbor Authentication

When configured, neighbor authentication occurs whenever routing updates are exchanged between neighbor routers. This authentication ensures that a router receives reliable routing information from a trusted source.

Without neighbor authentication, unauthorized or deliberately malicious routing updates could compromise the security of your network traffic. A security compromise could occur if an unfriendly party diverts or analyzes your network traffic. For example, an unauthorized router could send a fictitious routing update to convince your router to send traffic to an incorrect destination. This diverted traffic could be analyzed to learn confidential information of your organization, or merely used to disrupt your organization's ability to effectively communicate using the network.

Neighbor authentication prevents any such fraudulent route updates from being received by your router.

## Protocols That Use Neighbor Authentication

Neighbor authentication can be configured for the following routing protocols:

- Border Gateway Protocol (BGP)
- DRP Server Agent
- Intermediate System-to-Intermediate System (IS-IS)
- IP Enhanced Interior Gateway Routing Protocol (EIGRP)
- Open Shortest Path First (OSPF)
- Routing Information Protocol (RIP) version 2

## When to Configure Neighbor Authentication

You should configure any router for neighbor authentication if that router meets all of these conditions:

- The router uses any of the routing protocols previously mentioned.
- It is conceivable that the router might receive a false route update.
- If the router were to receive a false route update, your network might be compromised.
- If you configure a router for neighbor authentication, you also need to configure the neighbor router for neighbor authentication.

## How Neighbor Authentication Works

When neighbor authentication has been configured on a router, the router authenticates the source of each routing update packet that it receives. This is accomplished by the exchange of an authenticating key (sometimes referred to as a password) that is known to both the sending and the receiving router.

There are two types of neighbor authentication used: plain text authentication and Message Digest Algorithm Version 5 (MD5) authentication. Both forms work in the same way, with the exception that MD5 sends a "message digest" instead of the authenticating key itself. The message digest is created using the key and a message, but the key itself is not sent, preventing it from being read while it is being transmitted. Plain text authentication sends the authenticating key itself over the wire.

**Note**

Note that plain text authentication is not recommended for use as part of your security strategy. Its primary use is to avoid accidental changes to the routing infrastructure. Using MD5 authentication, however, is a recommended security practice.

**Caution**

As with all keys, passwords, and other security secrets, it is imperative that you closely guard authenticating keys used in neighbor authentication. The security benefits of this feature are reliant upon your keeping all authenticating keys confidential. Also, when performing router management tasks via Simple Network Management Protocol (SNMP), do not ignore the risk associated with sending keys using non-encrypted SNMP.

This section includes the following sections:

- [Plain Text Authentication](#)
- [MD5 Authentication](#)

## Plain Text Authentication

Each participating neighbor router must share an authenticating key. This key is specified at each router during configuration. Multiple keys can be specified with some protocols; each key must then be identified by a key number.

In general, when a routing update is sent, the following authentication sequence occurs:

- 
- Step 1** A router sends a routing update with a key and the corresponding key number to the neighbor router. In protocols that can have only one key, the key number is always zero.
  - Step 2** The receiving (neighbor) router checks the received key against the same key stored in its own memory.
  - Step 3** If the two keys match, the receiving router accepts the routing update packet. If the two keys do not match, the routing update packet is rejected.

These protocols use plain text authentication:

- DRP Server Agent
  - IS-IS
  - OSPF
  - RIP version 2
- 

## MD5 Authentication

MD5 authentication works similarly to plain text authentication, except that the key is never sent over the wire. Instead, the router uses the MD5 algorithm to produce a “message digest” of the key (also called a “hash”). The message digest is then sent instead of the key itself. This ensures that nobody can eavesdrop on the line and learn keys during transmission.

These protocols use MD5 authentication:

- OSPF

- RIP version 2
- BGP
- IP Enhanced IGRP

## Key Management (Key Chains)

You can configure key chains for these IP routing protocols:

- RIP version 2
- IP Enhanced IGRP
- DRP Server Agent

These routing protocols offer the additional function of managing keys by using key chains. When you configure a key chain, you specify a series of keys with lifetimes, and the Cisco IOS software rotates through each of these keys. This decreases the likelihood that keys will be compromised.

Each key definition within the key chain must specify a time interval for which that key will be activated (its “lifetime”). Then, during a given key’s lifetime, routing update packets are sent with this activated key. Keys cannot be used during time periods for which they are not activated. Therefore, it is recommended that for a given key chain, key activation times overlap to avoid any period of time for which no key is activated. If a time period occurs during which no key is activated, neighbor authentication cannot occur, and therefore routing updates will fail.

Multiple key chains can be specified.

Note that the router needs to know the time to be able to rotate through keys in synchronization with the other participating routers, so that all routers are using the same key at the same moment. Refer to the Network Time Protocol (NTP) and calendar commands in the “Performing Basic System Management” chapter of the *Cisco IOS Configuration Fundamentals Configuration Guide* for information about configuring time at your router.

## Finding Neighbor Authentication Configuration Information

To find complete configuration information for neighbor authentication, refer to the appropriate section and chapter in the *Cisco IOS IP Configuration Guide* as listed in [Table 66](#).

**Table 66** Location of Neighbor Authentication Information for Each Supported Protocol

Protocol	Chapter	Section
BGP	“Configuring BGP”	“Configuring Neighbor Options”
DRP Server Agent	“Configuring IP Services”	“Configuring a DRP Server Agent”
IP Enhanced IGRP	“Configuring IP Enhanced IGRP”	“Configuring Enhanced IGRP Route Authentication”
IS-IS	“Configuring Integrated IS-IS”	“Assigning a Password for an Interface” and “Configuring IS-IS Authentication Passwords”

**Table 66**      **Location of Neighbor Authentication Information for Each Supported Protocol**

Protocol	Chapter	Section
OSPF	“Configuring OSPF”	“Configuring OSPF Interface Parameters” and “Configuring OSPF Area Parameters” and “Creating Virtual Links”
RIP version 2	“Configuring RIP”	“Enabling RIP Authentication”

To find complete configuration information for key chains, refer to the “Managing Authentication Keys” section in the chapter “Configuring IP Routing Protocol-Independent Features” of the *Cisco IOS IP Configuration Guide*.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.







## Configuring IP Security Options

---

Cisco provides IP Security Option (IPSO) support as described in RFC 1108. Cisco's implementation is only minimally compliant with RFC 1108 because the Cisco IOS software only accepts and generates a 4-byte IPSO.

IPSO is generally used to comply with the U.S. government's Department of Defense security policy.

For a complete description of IPSO commands, refer to the chapter "IP Security Options Commands" of the *Cisco IOS Security Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the "Identifying Supported Platforms" section in the chapter "Using Cisco IOS Software."

## In This Chapter

This chapter describes how to configure IPSO for both the basic and extended security options described in RFC 1108. This chapter also describes how to configure auditing for IPSO. This chapter includes the following sections:

- [IPSO Configuration Task List](#)
- [IPSO Configuration Examples](#)

## IPSO Configuration Task List

This section describes the following configuration tasks:

- [Configuring Basic IP Security Options](#)
- [Configuring Extended IP Security Options](#)
- [Configuring the DNSIX Audit Trail Facility](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

## Configuring Basic IP Security Options

Cisco's basic IPSO support provides the following features:

- Defines security level on a per-interface basis
- Defines single-level or multilevel interfaces
- Provides a label for incoming packets
- Strips labels on a per-interface basis
- Reorders options to put any basic security options first

To configure basic IPSO, complete the tasks in the following sections:

- [Enabling IPSO and Setting the Security Classifications](#)
- [Specifying How IP Security Options Are Processed](#)

### Enabling IPSO and Setting the Security Classifications

To enable IPSO and set security classifications on an interface, use either of the following commands in interface configuration mode:

Command	Purpose
Router(config-if)# <b>ip security dedicated</b> <i>level</i> <i>authority [authority...]</i>	Sets an interface to the requested IPSO classification and authorities.
Router(config-if)# <b>ip security multilevel</b> <i>level1</i> <i>[authority1...] to level2 authority2</i> <i>[authority2...]</i>	Sets an interface to the requested IPSO range of classifications and authorities.

Use the **no ip security** command to reset an interface to its default state.

### Specifying How IP Security Options Are Processed

To specify how IP security options are processed, use any of the following optional commands in interface configuration mode:

Command	Purpose
Router(config-if)# <b>ip security ignore-authorities</b>	Enables an interface to ignore the authorities field of all incoming packets.
Router(config-if)# <b>ip security implicit-labelling</b> <i>[level authority [authority...]]</i>	Classifies packets that have no IPSO with an implicit security label.
Router(config-if)# <b>ip security extended-allowed</b>	Accepts packets on an interface that has an extended security option present.
Router(config-if)# <b>ip security ad</b>	Ensures that all packets leaving the router on an interface contain a basic security option.
Router(config-if)# <b>ip security strip</b>	Removes any basic security option that might be present on a packet leaving the router through an interface.

Command	Purpose
Router(config-if) # <b>ip security first</b>	Prioritizes security options on a packet.
Router(config-if) # <b>ip security reserved-allowed</b>	Treats as valid any packets that have Reserved1 through Reserved4 security levels.

### Default Values for Command Keywords

To fully comply with IPSO, the default values for the minor keywords have become complex. Default value usages include the following:

- The default for all of the minor keywords is *off*, with the exception of **implicit-labelling** and **add**.
- The default value of **implicit-labelling** is *on* if the interface is “unclassified Genser;” otherwise, it is *off*.
- The default value for **add** is *on* if the interface is not “unclassified Genser;” otherwise, it is *off*.

Table 67 provides a list of all default values.

**Table 67**      **Default Security Keyword Values**

Interface Type	Level	Authority	Implicit Labeling	Add IPSO
None	None	None	On	Off
Dedicated	Unclassified	Genser	On	Off
Dedicated	Any	Any	Off	On
Multilevel	Any	Any	Off	On

The default value for any interface is “dedicated, unclassified Genser.” Note that this implies implicit labeling. This might seem unusual, but it makes the system entirely transparent to packets without options. This is the setting generated when you specify the **no ip security** interface configuration command.

## Configuring Extended IP Security Options

Cisco’s extended IPSO support is compliant with the Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) specification documents. Extended IPSO functionality can unconditionally accept or reject Internet traffic that contains extended security options by comparing those options to configured allowable values. This support allows DNSIX networks to use additional security information to achieve a higher level of security than that achievable with basic IPSO.

Cisco also supports a subset of the security features defined in the DNSIX version 2.1 specification. Specifically, Cisco supports DNSIX definitions of the following:

- How extended IPSO is processed
- Audit trail facility

There are two kinds of extended IPSO fields defined by the DNSIX 2.1 specification and supported by Cisco’s implementation of extended IPSO—Network-level Extended Security Option (NLESO) and Auxiliary Extended Security Option (AESO) fields.

NLESO processing requires that security options be checked against configured allowable information, source, and compartment bit values, and requires that the router be capable of inserting extended security options in the IP header.

AESO is similar to NLESO, except that its contents are not checked and are assumed to be valid if its source is listed in the AESO table.

To configure extended IPSO, complete the tasks in the following sections:

- [Configuring Global Default Settings](#)
- [Attaching ESOs to an Interface](#)
- [Attaching AESOs to an Interface](#)

## Configuring Global Default Settings

To configure global default setting for extended IPSO, including AESOs, use the following command in global configuration mode:

Command	Purpose
Router(config)# <b>ip security eso-info</b> <i>source compartment-size default-bit</i>	Configures system-wide default settings.

## Attaching ESOs to an Interface

To specify the minimum and maximum sensitivity levels for an interface, use the following commands in interface configuration mode:

	Command	Purpose
<b>Step 1</b>	Router(config-if)# <b>ip security eso-min</b> <i>source compartment-bits</i>	Sets the minimum sensitivity level for an interface.
<b>Step 2</b>	Router(config-if)# <b>ip security eso-max</b> <i>source compartment-bits</i>	Sets the maximum sensitivity level for an interface.

## Attaching AESOs to an Interface

To specify the extended IPSO sources that are to be treated as AESO sources, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# <b>ip security aeso</b> <i>source compartment-bits</i>	Specifies AESO sources.

DNSIX version 2.1 causes slow-switching code.

See the “[IPSO Configuration Examples](#)” section at the end of this chapter.

## Configuring the DNSIX Audit Trail Facility

The audit trail facility is a UDP-based protocol that generates an audit trail of IPSO security violations. This facility allows the system to report security failures on incoming and outgoing packets. The Audit Trail Facility sends DNSIX audit trail messages when a datagram is rejected because of IPSO security violations. This feature allows you to configure organization-specific security information.

The DNSIX audit trail facility consists of two protocols:

- DNSIX Message Deliver Protocol (DMDP) provides a basic message-delivery mechanism for all DNSIX elements.
- Network Audit Trail Protocol provides a buffered logging facility for applications to use to generate auditing information. This information is then passed on to DMDP.

To configure the DNSIX auditing facility, complete the tasks in the following sections:

- [Enabling the DNSIX Audit Trail Facility](#)
- [Specifying Hosts to Receive Audit Trail Messages](#)
- [Specifying Transmission Parameters](#)

## Enabling the DNSIX Audit Trail Facility

To enable the DNSIX audit trail facility, use the following command in global configuration mode:

Command	Purpose
Router(config)# <b>dnsix-nat source</b> <i>ip-address</i>	Starts the audit writing module.

## Specifying Hosts to Receive Audit Trail Messages

To define and change primary and secondary addresses of the host to receive audit messages, use the following commands in global configuration mode:

	Command	Purpose
<b>Step 1</b>	Router(config)# <b>dnsix-nat primary</b> <i>ip-address</i>	Specifies the primary address for the audit trail.
<b>Step 2</b>	Router(config)# <b>dnsix-nat secondary</b> <i>ip-address</i>	Specifies the secondary address for the audit trail.
<b>Step 3</b>	Router(config)# <b>dnsix-nat authorized-redirection</b> <i>ip-address</i>	Specifies the address of a collection center that is authorized to change primary and secondary addresses. Specified hosts are authorized to change the destination of audit messages.

## Specifying Transmission Parameters

To specify transmission parameters, use the following commands in global configuration mode:

	Command	Purpose
<b>Step 1</b>	Router(config)# <b>dnsix-nat transmit-count</b> <i>count</i>	Specifies the number of records in a packet before it is sent to a collection center.
<b>Step 2</b>	Router(config)# <b>dnsix-dmdp retries</b> <i>count</i>	Specifies the number of transmit retries for DMDP.

# IPSO Configuration Examples

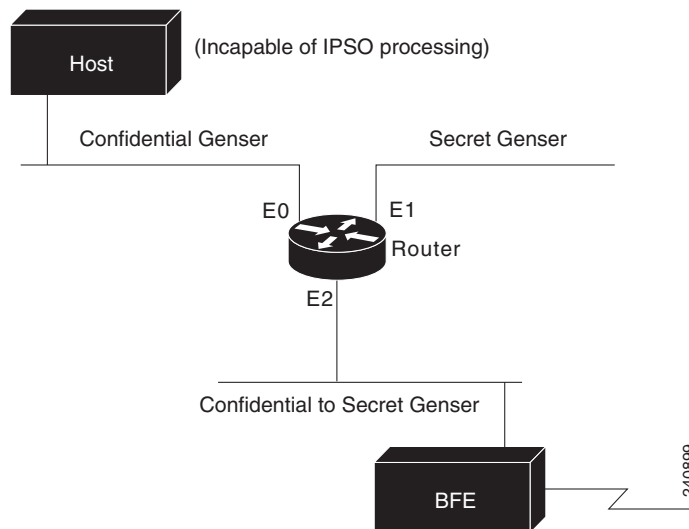
The following sections provide IPSO configuration examples:

- [Example 1](#)
- [Example 2](#)
- [Example 3](#)

## Example 1

In this example, three Ethernet interfaces are presented. These interfaces are running at security levels of Confidential Genser, Secret Genser, and Confidential to Secret Genser, as shown in [Figure 106](#).

**Figure 106** IPSO Security Levels



The following commands set up interfaces for the configuration in [Figure 106](#):

```

interface ethernet 0
 ip security dedicated confidential genser
interface ethernet 1
 ip security dedicated secret genser
interface ethernet 2
 ip security multilevel confidential genser to secret genser

```

It is possible for the setup to be much more complex.

## Example 2

In the following example, there are devices on Ethernet 0 that cannot generate a security option, and so must accept packets without a security option. These hosts do not understand security options; therefore, never place one on such interfaces. Furthermore, there are hosts on the other two networks that are using the extended security option to communicate information, so you must allow these to pass through the system. Finally, there also is a host (a Blacker Front End; see the “Configuring X.25 and LABP” chapter of the *Cisco IOS Wide-Area Networking Configuration Guide* for more information about Blacker emergency mode) on Ethernet 2 that requires the security option to be the first option present, and this condition also must be specified. The new configuration follows.

```

interface ethernet 0
 ip security dedicated confidential genser

```

```
ip security implicit-labelling
ip security strip
interface ethernet 1
ip security dedicated secret genser
ip security extended-allowed
!
interface ethernet 2
ip security multilevel confidential genser to secret genser
ip security extended-allowed
ip security first
```

## Example 3

This example shows how to configure a Cisco router with HP-UX CMW DNSIX hosts. The following commands should be configured on each LAN interface of the router for two DNSIX hosts to communicate:

```
ip security multilevel unclassified nsa to top secret nsa
ip security extended allowed
```

DNSIX hosts do not need to know the router's IP addresses, and DNSIX hosts do not need to set up M6RHDB entries for the routers.

---

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.







## **Unicast Reverse Path Forwarding**





# Configuring Unicast Reverse Path Forwarding

---

## Feature History

Release	Modification
Cisco IOS	For information about feature support in Cisco IOS software, use Cisco Feature Navigator.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

This chapter describes the Unicast Reverse Path Forwarding (Unicast RPF) feature. The Unicast RPF feature helps to mitigate problems that are caused by malformed or forged IP source addresses that are passing through a router.

For a complete description of the Unicast RPF commands in this chapter, refer to the chapter “Unicast Reverse Path Forwarding Commands” of the *Cisco IOS Security Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the “Identifying Supported Platforms” section in the chapter “Using Cisco IOS Software.”

## In This Chapter

This chapter has the following sections:

- [About Unicast Reverse Path Forwarding](#)
- [Unicast RPF Configuration Task List](#)
- [Troubleshooting Tips](#)
- [Monitoring and Maintaining Unicast RPF](#)
- [Unicast RPF Configuration Examples](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

# About Unicast Reverse Path Forwarding

The Unicast RPF feature helps to mitigate problems that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address. For example, a number of common types of denial-of-service (DoS) attacks, including Smurf and Tribal Flood Network (TFN), can take advantage of forged or rapidly changing source IP addresses to allow attackers to thwart efforts to locate or filter the attacks. For Internet service providers (ISPs) that provide public access, Unicast RPF deflects such attacks by forwarding only packets that have source addresses that are valid and consistent with the IP routing table. This action protects the network of the ISP, its customer, and the rest of the Internet.

This section covers the following information:

- [How Unicast RPF Works](#)
- [Implementing Unicast RPF](#)
- [Restrictions](#)
- [Related Features and Technologies](#)
- [Prerequisites to Configuring Unicast RPF](#)

## How Unicast RPF Works

When Unicast RPF is enabled on an interface, the router examines all packets received as input on that interface to make sure that the source address and source interface appear in the routing table and match the interface on which the packet was received. This “look backwards” ability is available only when Cisco express forwarding (CEF) is enabled on the router, because the lookup relies on the presence of the Forwarding Information Base (FIB). CEF generates the FIB as part of its operation.

**Note**

Unicast RPF is an input function and is applied only on the input interface of a router at the upstream end of a connection.

Unicast RPF checks to see if any packet received at a router interface arrives on the best return path (return route) to the source of the packet. Unicast RPF does this by doing a reverse lookup in the CEF table. If the packet was received from one of the best reverse path routes, the packet is forwarded as normal. If there is no reverse path route on the same interface from which the packet was received, it might mean that the source address was modified. If Unicast RPF does not find a reverse path for the packet, the packet is dropped or forwarded, depending on whether an access control list (ACL) is specified in the **ip verify unicast reverse-path** interface configuration command.

**Note**

With Unicast RPF, all equal-cost “best” return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on) and as long as the route is in the FIB. Unicast RPF also functions where EIGRP variants are being used and unequal candidate paths back to the source IP address exist.

When a packet is received at the interface where Unicast RPF and ACLs have been configured, the following actions occur:

**Step 1** Input ACLs configured on the inbound interface are checked.

- Step 2** Unicast RPF checks to see if the packet has arrived on the best return path to the source, which it does by doing a reverse lookup in the FIB table.
- Step 3** CEF table (FIB) lookup is carried out for packet forwarding.
- Step 4** Output ACLs are checked on the outbound interface.
- Step 5** The packet is forwarded.
- 

This section provides information about Unicast RPF enhancements:

- [Access Control Lists and Logging](#)
- [Per-Interface Statistics](#)

## Access Control Lists and Logging

If an ACL is specified in the command, then when (and only when) a packet fails the Unicast RPF check, the ACL is checked to see if the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the Unicast RPF command, the router drops the forged or malformed packet immediately and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

Unicast RPF events can be logged by specifying the logging option for the ACL entries used by the Unicast RPF command. Using the log information, administrators can see what source addresses are being used in the attack, the time the packets arrived at the interface, and so on.



### Caution

Logging requires CPU and memory resources. Logging Unicast RPF events for attacks having a high rate of forged packets can degrade the performance of the router.

---

## Per-Interface Statistics

Each time a packet is dropped or forwarded at an interface, that information is counted two ways: globally on the router and at each interface where you have applied Unicast RPF. Global statistics on dropped packets provide information about potential attacks on the network; however, these global statistics do not help to specify which interface is the source of the attack.

Per-interface statistics allow network administrators to track two types of information about malformed packets: Unicast RPF drops and Unicast RPF suppressed drops. Statistics on the number of packets that Unicast RPF drops help to identify the interface that is the entry point of the attack. The Unicast RPF drop count tracks the number of drops at the interface. The Unicast RPF suppressed drop count tracks the number of packets that failed the Unicast RPF check but were forwarded because of the permit permission set up in the ACL. Using the drop count and suppressed drop count statistics, a network administrator can take steps to isolate the attack at a specific interface.



### Note

Judicious use of ACL logging can further identify the address or addresses that are being dropped by Unicast RPF.

---

Figure 38 illustrates how Unicast RPF and CEF work together to validate IP source addresses by verifying packet return paths. In this example, a customer has sent a packet having a source address of 192.168.1.1 from interface FDDI 2/0/0. Unicast RPF checks the FIB to see if 192.168.1.1 has a path to FDDI 2/0/0. If there is a matching path, the packet is forwarded. If there is no matching path, the packet is dropped.

**Figure 38**      **Unicast RPF Validating IP Source Addresses**



Figure 39 illustrates how Unicast RPF drops packets that fail validation. In this example, a customer has sent a packet having a source address of 209.165.200.225, which is received at interface FDDI 2/0/0. Unicast RPF checks the FIB to see if 209.165.200.225 has a return path to FDDI 2/0/0. If there is a matching path, the packet is forwarded. In this case, there is no reverse entry in the routing table that routes the customer packet back to source address 209.165.200.225 on interface FDDI 2/0/0, and so the packet is dropped.

**Figure 39**      **Unicast RPF Dropping Packets That Fail Verification**



## Implementing Unicast RPF

Unicast RPF has several key implementation principles:

- The packet must be received at an interface that has the best return path (route) to the packet source (a process called *symmetric routing*). There must be a route in the FIB matching the route to the receiving interface. Adding a route in the FIB can be done via static route, network statement, or dynamic routing. (ACLs permit Unicast RPF to be used when packets are known to be arriving by specific, less optimal asymmetric input paths.)
- IP source addresses at the receiving interface must match the routing entry for the interface.
- Unicast RPF is an input function and is applied only on the input interface of a router at the upstream end of a connection.

Given these implementation principles, Unicast RPF becomes a tool that network administrators can use not only for their customers but also for their downstream network or ISP, even if the downstream network or ISP has other connections to the Internet.



### Caution

Using optional BGP attributes such as weight and local preference, the best path back to the source address can be modified. Modification would affect the operation of Unicast RPF.

This section provides information about the implementation of Unicast RPF:

- [Security Policy and Unicast RPF](#)
- [Where to Use Unicast RPF](#)
- [Routing Table Requirements](#)
- [Where Not to Use Unicast RPF](#)
- [Unicast RPF with BOOTP and DHCP](#)

## Security Policy and Unicast RPF

Consider the following points in determining your policy for deploying Unicast RPF:

- Unicast RPF must be applied at the interface downstream from the larger portion of the network, preferably at the edges of your network.
- The further downstream you apply Unicast RPF, the finer the granularity you have in mitigating address spoofing and in identifying the sources of spoofed addresses. For example, applying Unicast RPF on an aggregation router helps mitigate attacks from many downstream networks or clients and is simple to administer, but it does not help identify the source of the attack. Applying Unicast RPF at the network access server helps limit the scope of the attack and trace the source of the attack; however, deploying Unicast RPF across many sites does add to the administration cost of operating the network.
- The more entities that deploy Unicast RPF across Internet, intranet, and extranet resources, the better the chances of mitigating large-scale network disruptions throughout the Internet community, and the better the chances of tracing the source of an attack.
- Unicast RPF will not inspect IP packets encapsulated in tunnels, such as GRE, LT2P, or PPTP. Unicast RPF must be configured at a home gateway so that Unicast RPF processes network traffic only after the tunneling and encryption layers have been stripped off the packets.

## Where to Use Unicast RPF

Unicast RPF can be used in any “single-homed” environment where there is essentially only one access point out of the network; that is, one upstream connection. Networks having one access point offer the best example of symmetric routing, which means that the interface where a packet enters the network is also the best return path to the source of the IP packet. Unicast RPF is best used at the network perimeter for Internet, intranet, or extranet environments, or in ISP environments for customer network terminations.

The following sections provide a look at implementing Unicast RPF in two network environments:

- [Enterprise Networks with a Single Connection to an ISP](#)
- [Network Access Server Application \(Applying Unicast RPF in PSTN/ISDN PoP Aggregation Routers\)](#)

### Enterprise Networks with a Single Connection to an ISP

In enterprise networks, one objective of using Unicast RPF for filtering traffic at the input interface (a process called *ingress filtering*) is for protection from malformed packets arriving from the Internet. Traditionally, local networks that have one connection to the Internet would use ACLs at the receiving interface to prevent spoofed packets from the Internet from entering their local network.



ACLs work well for many single-homed customers; however, there are trade-offs when ACLs are used as ingress filters, including two commonly referenced limitations:

- Packet per second (PPS) performance at very high packet rates
- Maintenance of the ACL (whenever there are new addresses added to the network)

Unicast RPF is one tool that addresses both of these limitations. With Unicast RPF, ingress filtering is done at CEF PPS rates. This processing speed makes a difference when the link is more than 1 Mbps. Additionally, since Unicast RPF uses the FIB, no ACL maintenance is necessary, and thus the administration overhead of traditional ACLs is reduced. The following figure and example demonstrate how Unicast RPF is configured for ingress filtering.

[Figure 40](#) illustrates an enterprise network that has a single link to an upstream ISP. In this example, Unicast RPF is applied at interface S0 on the enterprise router for protection from malformed packets arriving from the Internet. Unicast RPF is also applied at interface S5/0 on the ISP router for protection from malformed packets arriving from the enterprise network.

**Figure 40**      *Enterprise Network Using Unicast RPF for Ingress Filtering*



Using the topography in [Figure 40](#), a typical configuration (assuming that CEF is turned on) on the ISP router would be as follows:

```
ip cef
interface loopback 0
 description Loopback interface on Gateway Router 2
 ip address 192.168.3.1 255.255.255.255
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
interface Serial 5/0
 description 128K HDLC link to ExampleCorp WT50314E R5-0
 bandwidth 128
 ip unnumbered loopback 0
 ip verify unicast reverse-path
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
ip route 192.168.10.0 255.255.252.0 Serial 5/0
```

The gateway router configuration of the enterprise network (assuming that CEF is turned on) would look similar to the following:

```
ip cef
interface Ethernet 0
 description ExampleCorp LAN
 ip address 192.168.10.1 255.255.252.0
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
interface Serial 0
```

```
description 128K HDLC link to ExampleCorp Internet Inc WT50314E C0
bandwidth 128
ip unnumbered ethernet 0
ip verify unicast reverse-path
no ip redirects
no ip directed-broadcast
no ip proxy-arp
ip route 0.0.0.0 0.0.0.0 Serial 0
```

Notice that Unicast RPF works with a single default route. There are no additional routes or routing protocols. Network 192.168.10.0/22 is a connected network. Hence, packets coming from the Internet with a source address in the range 192.168.10.0/22 will be dropped by Unicast RPF.

### Network Access Server Application (Applying Unicast RPF in PSTN/ISDN PoP Aggregation Routers)

Aggregation routers are ideal places to use Unicast RPF with single-homed clients. Unicast RPF works equally well on leased-line or PSTN/ISDN/xDSL customer connections into the Internet. In fact, dialup connections are reputed to be the greatest source of DoS attacks using forged IP addresses. As long as the network access server supports CEF, Unicast RPF will work. In this topology, the customer aggregation routers need not have the full Internet routing table. Aggregation routers need the routing prefixes information (IP address block); hence, information configured or redistributed in the Interior Gateway Protocol (IGP) or Internal Border Gateway Protocol (IBGP) (depending on the way that you add customer routes into your network) would be enough for Unicast RPF to do its job.

Figure 41 illustrates the application of Unicast RPF to the aggregation and access routers for an Internet service provider (ISP) point of presence (POP), with the ISP routers providing dialup customer connections. In this example, Unicast RPF is applied upstream from the customer dialup connection router on the receiving (input) interfaces of the ISP aggregation routers.

**Figure 41**      *Unicast RPF Applied to PSTN/ISDN Customer Connections*



## Routing Table Requirements

To work correctly, Unicast RPF needs proper information in the CEF tables. This requirement does not mean that the router must have the entire Internet routing table. The amount of routing information needed in the CEF tables depends on where Unicast RPF is configured and what functions the router performs in the network. For example, in an ISP environment, a router that is a leased-line aggregation router for customers needs only the information based on the static routes redistributed into the IGP or IBGP (depending on which technique is used in the network). Unicast RPF would be configured on the customer interfaces—hence the requirement for minimal routing information. In another scenario, a single-homed ISP could place Unicast RPF on the gateway link to the Internet. The full Internet routing table would be required. Requiring the full routing table would help protect the ISP from external DoS attacks that use addresses that are not in the Internet routing table.

## Where Not to Use Unicast RPF

Unicast RPF should not be used on interfaces that are internal to the network. Internal interfaces are likely to have routing asymmetry (see [Figure 42](#)), meaning multiple routes to the source of a packet. Unicast RPF should be applied only where there is natural or configured symmetry. As long as administrators carefully plan which interfaces they activate Unicast RPF on, routing asymmetry is not a serious problem.

For example, routers at the edge of the network of an ISP are more likely to have symmetrical reverse paths than routers that are in the core of the ISP network. Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router. Hence, it is not recommended that you apply Unicast RPF where there is a chance of asymmetric routing, unless you use ACLs to allow the router to accept incoming packets. ACLs permit Unicast RPF to be used when packets are known to be arriving by specific, less optimal asymmetric input paths. However, it is simplest to place Unicast RPF only at the edge of a network or, for an ISP, at the customer edge of the network.

[Figure 42](#) illustrates how Unicast RPF can block legitimate traffic in an asymmetrical routing environment.

**Figure 42**      *Unicast RPF Blocking Traffic in an Asymmetrical Routing Environment*



## Unicast RPF with BOOTP and DHCP

Unicast RPF will allow packets with 0.0.0.0 source and 255.255.255.255 destination to pass so that Bootstrap Protocol (BOOTP) and Dynamic Host Configuration Protocol (DHCP) functions work properly. This enhancement was added in Cisco IOS Release 12.0 and later, but it is not in Cisco IOS Release 11.1CC.

## Restrictions

There are some basic restrictions to applying Unicast RPF to multihomed clients:

- Clients should not be multihomed to the same router because multihoming defeats the purpose of building a redundant service for the client.
- Customers must ensure that the packets flowing up the link (out to the Internet) match the route advertised out the link. Otherwise, Unicast RPF filters those packets as malformed packets.
- Unicast RPF is available only for platform images that support CEF. Unicast RPF is supported in Cisco IOS Releases 11.1(17)CC and 12.0 and later. It is not available in Cisco IOS Release 11.2 or 11.3.

## Related Features and Technologies

For more information about Unicast RPF-related features and technologies, review the following:

- Unicast RPF requires Cisco express forwarding (CEF) to function properly on the router. For more information about CEF, refer to the *Cisco IOS Switching Services Configuration Guide*.
- Unicast RPF can be more effective at mitigating spoofing attacks when combined with a policy of *ingress* and *egress* filtering using Cisco IOS access control lists (ACLs).
  - Ingress filtering applies filters to traffic received at a network interface from either internal or external networks. With ingress filtering, packets that arrive from other networks or the Internet and that have a source address that matches a local network, private, or broadcast address are dropped. In ISP environments, for example, ingress filtering can apply to traffic received at the router from either the client (customer) or the Internet.
  - Egress filtering applies filters to traffic exiting a network interface (the sending interface). By filtering packets on routers that connect your network to the Internet or to other networks, you can permit only packets with valid source IP addresses to leave your network.

For more information on network filtering, refer to RFC 2267 and to the *Cisco IOS IP Configuration Guide*.

- Cisco IOS software provides additional features that can help mitigate DoS attacks:
  - Committed Access Rate (CAR). CAR allows you to enforce a bandwidth policy against network traffic that matches an access list. For example, CAR allows you to rate-limit what should be low-volume traffic, such as ICMP traffic. To find out more about CAR, refer to the *Cisco IOS Quality of Service Solutions Configuration Guide*.
  - Context-based Access Control (CBAC). CBAC selectively blocks any network traffic not originated by a protected network. CBAC uses timeout and threshold values to manage session state information, helping to determine when to drop sessions that do not become fully established. Setting timeout values for network sessions helps mitigate DoS attacks by freeing up system resources, dropping sessions after a specified amount of time. For more information on CBAC, refer to the *Cisco IOS Security Configuration Guide*.

- TCP Intercept. The TCP Intercept feature implements software to protect TCP servers from TCP SYN-flooding attacks, which are a type of DoS attack. A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection. Like CBAC, the TCP Intercept feature also uses timeout and threshold values to manage session state information, helping to determine when to drop sessions that do not become fully established. For more information on TCP Intercept, refer to the *Cisco IOS Security Configuration Guide*.

## Prerequisites to Configuring Unicast RPF

Prior to configuring Unicast RPF, configure ACLs:

- Configure standard or extended ACLs to mitigate transmission of invalid IP addresses (perform egress filtering). Permit only valid source addresses to leave your network and get onto the Internet. Prevent all other source addresses from leaving your network for the Internet.
- Configure standard or extended ACLs entries to drop (deny) packets that have invalid source IP addresses (perform ingress filtering). Invalid source IP addresses include the following types:
  - Reserved addresses
  - Loopback addresses
  - Private addresses (RFC 1918, *Address Allocation for Private Internets*)
  - Broadcast addresses (including multicast addresses)
  - Source addresses that fall outside the range of valid addresses associated with the protected network
- Configure standard or extended ACL entries to forward (permit) packets that fail the Unicast RPF checks to allow specific traffic from known asymmetric routed sources.
- Configure ACLs to track Unicast RPF events by adding the logging option into the ACL command. During network attacks, judicious logging of dropped or forwarded packets (suppressed drops) can provide additional information about network attacks.

## Unicast RPF Configuration Task List

The following sections describe the configuration tasks for Unicast RPF. Each task in the list is identified as either optional or required.

- [Configuring Unicast RPF](#) (Required)
- [Verifying Unicast RPF](#) (Optional)

See the section “[Unicast RPF Configuration Examples](#)” at the end of this chapter.

## Configuring Unicast RPF

To use Unicast RPF, you must configure the router for CEF switching or CEF distributed switching. There is no need to configure the input interface for CEF switching because Unicast RPF has been implemented as a search through the FIB using the source IP address. As long as CEF is running on the router, individual interfaces can be configured with other switching modes. Unicast RPF is an input-side function that is enabled on an interface or subinterface that supports any type of encapsulation and operates on IP packets received by the router. It is very important that CEF be turned on globally in the router—Unicast RPF will not work without CEF.

To configure Unicast RPF, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>ip cef</b>	Enables CEF or distributed CEF on the router. Distributed CEF is required for routers that use a Route Switch Processor (RSP) and Versatile Interface Processor (VIP), which includes Unicast RPF.
	or Router(config)# <b>ip cef distributed</b>	You might want to disable CEF or distributed CEF (dCEF) on a particular interface if that interface is configured with a feature that CEF or dCEF does not support. In this case, you would enable CEF globally, but disable CEF on a specific interface using the <b>no ip route-cache cef</b> interface command, which enables all but that specific interface to use express forwarding. If you have disabled CEF or dCEF operation on an interface and want to reenabling it, you can do so by using the <b>ip route-cache cef</b> command in interface configuration mode.
Step 2	Router(config-if)# <b>interface type</b>	Selects the input interface on which you want to apply Unicast RPF. This is the receiving interface, which allows Unicast RPF to verify the best return path before forwarding the packet on to the next destination.  The interface type is specific to your router and the types of interface cards installed on the router. To display a list of available interface types, enter the <b>interface ?</b> command.
Step 3	Router(config-if)# <b>ip verify unicast reverse-path list</b>	Enables Unicast RPF on the interface. Use the <i>list</i> option to identify an access list. If the access list denies network access, spoofed packets are dropped at the interface. If the access list permits network access, spoofed packets are forwarded to the destination address. Forwarded packets are counted in the interface statistics. If the access list includes the logging option, information about the spoofed packets is logged to the log server.  Repeat this step for each access list that you want specify.
Step 4	Router(config-if)# <b>exit</b>	Exits interface configuration mode. Repeat Steps 2 and 3 for each interface on which you want to apply Unicast RPF.

## Verifying Unicast RPF

To verify that Unicast RPF is operational, use the **show cef interface** command. The following example shows that Unicast RPF is enabled at interface serial2/0/0.

```
Router-3# show cef interface serial 2/0/0
```

```
Serial2/0/0 is up (if_number 8)
Internet address is 192.168.10.2/30
ICMP redirects are never sent
Per packet loadbalancing is disabled
!The next line displays Unicast RPF packet dropping information.
IP unicast RPF check is enabled
Inbound access list is not set
Outbound access list is not set
Interface is marked as point to point interface
Packets switched to this interface on linecard are dropped to next slow path
Hardware idb is Serial2/0/0
Fast switching type 4, interface type 6
!The next line displays Unicast RPF packet dropping information.
IP Distributed CEF switching enabled
IP LES Feature Fast switching turbo vector
IP Feature CEF switching turbo vector
Input fast flags 0x40, Output fast flags 0x0, ifindex 7(7)
Slot 2 Slot unit 0 VC -1
Transmit limit accumulator 0x48001A02 (0x48001A02)
IP MTU 1500
```

## Troubleshooting Tips

If you experience problems while using Unicast RPF, check the following items.

### HSRP Failure

Failure to disable Unicast RPF before disabling CEF can cause Hot Standby Router Protocol (HSRP) failure. If you want to disable CEF on the router, you must first disable Unicast RPF. To disable Unicast RPF, see the section “[Monitoring and Maintaining Unicast RPF](#).”

### Dropped Boot Requests

In Cisco IOS Release 11.1(17)CC, Unicast RPF can drop BOOTP request packets that have a source address of 0.0.0.0 due to source address verification at the interface. To enable boot requests to work on the interface, you must use ACLs instead of Unicast RPF.

# Monitoring and Maintaining Unicast RPF

This section describes commands used to monitor and maintain Unicast RPF.

Command	Purpose
Router# <b>show ip traffic</b>	Displays global router statistics about Unicast RPF drops and suppressed drops.
Router# <b>show ip interface type</b>	Displays per-interface statistics about Unicast RPF drops and suppressed drops.
Router# <b>show access-lists</b>	Displays the number of matches to a specific ACL.
Router(config-if)# <b>no ip verify unicast reverse-path list</b>	Disables Unicast RPF at the interface. Use the <i>list</i> option to disable Unicast RPF for a specific ACL at the interface.



## Caution

To disable CEF, you must first disable Unicast RPF. Failure to disable Unicast RPF before disabling CEF can cause HSRP failure. If you want to disable CEF on the router, you must first disable Unicast RPF.

Unicast RPF counts the number of packets dropped or suppressed because of malformed or forged source addresses. Unicast RPF counts dropped or forwarded packets that include the following global and per-interface information:

- Global Unicast RPF drops
- Per-interface Unicast RPF drops
- Per-interface Unicast RPF suppressed drops

The **show ip traffic** command shows the total number (global count) of dropped or suppressed packets for all interfaces on the router. The Unicast RPF drop count is included in the IP statistics section.

```
Router# show ip traffic
```

```
IP statistics:
```

```
Rcvd: 1471590 total, 887368 local destination
 0 format errors, 0 checksum errors, 301274 bad hop count
 0 unknown protocol, 0 not a gateway
 0 security failures, 0 bad options, 0 with options
Opts: 0 end, 0 nop, 0 basic security, 0 loose source route
 0 timestamp, 0 extended security, 0 record route
 0 stream ID, 0 strict source route, 0 alert, 0 other
Frgs: 0 reassembled, 0 timeouts, 0 couldn't reassemble
 0 fragmented, 0 couldn't fragment
Bcast: 205233 received, 0 sent
Mcast: 463292 received, 462118 sent
Sent: 990158 generated, 282938 forwarded
! The second line below ("0 unicast RPF") displays Unicast RPF packet dropping
information.
Drop: 3 encapsulation failed, 0 unresolved, 0 no adjacency
 0 no route, 0 unicast RPF, 0 forced drop
```

A nonzero value for the count of dropped or suppressed packets can mean one of two things:

- Unicast RPF is dropping or suppressing packets that have a bad source address (normal operation).



- Unicast RPF is dropping or suppressing legitimate packets because the route is misconfigured to use Unicast RPF in environments where asymmetric routing exists; that is, where multiple paths can exist as the best return path for a source address.

The **show ip interface** command shows the total of dropped or suppressed packets at a specific interface. If Unicast RPF is configured to use a specific ACL, that ACL information is displayed along with the drop statistics.

```
Router> show ip interface ethernet0/1/1
```

```
Unicast RPF ACL 197
1 unicast RPF drop
1 unicast RPF suppressed drop
```

The **show access-lists** command displays the number of matches found for a specific entry in a specific access list.

```
Router> show access-lists
```

```
Extended IP access list 197
deny ip 192.168.201.0 0.0.0.63 any log-input (1 match)
permit ip 192.168.201.64 0.0.0.63 any log-input (1 match)
deny ip 192.168.201.128 0.0.0.63 any log-input
permit ip 192.168.201.192 0.0.0.63 any log-input
```

## Unicast RPF Configuration Examples

This section provides the following configuration examples:

- [Unicast RPF on a Leased-Line Aggregation Router Example](#)
- [Unicast RPF on the Cisco AS5800 Using Dialup Ports Example](#)
- [Unicast RPF with Inbound and Outbound Filters Example](#)
- [Unicast RPF with ACLs and Logging Example](#)

### Unicast RPF on a Leased-Line Aggregation Router Example

The following commands enable Unicast RPF on a serial interface:

```
ip cef
! or "ip cef distributed" for RSP+VIP based routers
!
interface serial 5/0/0
ip verify unicast reverse-path
```

### Unicast RPF on the Cisco AS5800 Using Dialup Ports Example

The following example enables Unicast RPF on a Cisco AS5800. The **interface Group-Async** command makes it easy to apply Unicast RPF on all the dialup ports.

```
ip cef
!
interface Group-Async1
ip verify unicast reverse-path
```

## Unicast RPF with Inbound and Outbound Filters Example

The following example uses a very simple single-homed ISP to demonstrate the concepts of ingress and egress filters used in conjunction with Unicast RPF. The example illustrates an ISP-allocated classless interdomain routing (CIDR) block 209.165.202.128/28 that has both inbound and outbound filters on the upstream interface. Be aware that ISPs are usually not single-homed. Hence, provisions for asymmetrical flows (when outbound traffic goes out one link and returns via a different link) need to be designed into the filters on the border routers of the ISP.

```
ip cef distributed
!
interface Serial 5/0/0
 description Connection to Upstream ISP
 ip address 209.165.200.225 255.255.255.252
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
 ip verify unicast reverse-path
 ip access-group 111 in
 ip access-group 110 out
!
access-list 110 permit ip 209.165.202.128 0.0.0.31 any
access-list 110 deny ip any any log
access-list 111 deny ip host 0.0.0.0 any log
access-list 111 deny ip 127.0.0.0 0.255.255.255 any log
access-list 111 deny ip 10.0.0.0 0.255.255.255 any log
access-list 111 deny ip 172.16.0.0 0.15.255.255 any log
access-list 111 deny ip 192.168.0.0 0.0.255.255 any log
access-list 111 deny ip 209.165.202.128 0.0.0.31 any log
access-list 111 permit ip any any
```

## Unicast RPF with ACLs and Logging Example

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL 197 provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on interface Ethernet0 to check packets arriving at that interface.

For example, packets with a source address of 192.168.201.10 arriving at interface Ethernet0 are dropped because of the deny statement in ACL 197. In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per interface and globally. Packets with a source address of 192.168.201.100 arriving at interface Ethernet0 are forwarded because of the permit statement in ACL 197. ACL information about dropped or suppressed packets is logged (logging option turned on for the ACL entry) to the log server.

```
ip cef distributed
!
int eth0/1/1
 ip address 192.168.200.1 255.255.255.0
 ip verify unicast reverse-path 197
!
int eth0/1/2
 ip address 192.168.201.1 255.255.255.0
!
access-list 197 deny ip 192.168.201.0 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 0.0.0.63 any log-input
access-list 197 deny ip 192.168.201.128 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 0.0.0.63 any log-input
access-list 197 deny ip host 0.0.0.0 any log
```



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





# Unicast Reverse Path Forwarding Loose Mode

The Unicast Reverse Path Forwarding Loose Mode feature creates a new option for Unicast Reverse Path Forwarding (Unicast RPF), providing a scalable anti-spoofing mechanism suitable for use in multihome network scenarios. This mechanism is especially relevant for Internet Service Providers (ISPs), specifically on routers that have multiple links to multiple ISPs. In addition, Unicast RPF (strict or loose mode), when used in conjunction with a Border Gateway Protocol (BGP) “trigger,” provides an excellent quick reaction mechanism that allows network traffic to be dropped on the basis of either the source or destination IP address, giving network administrators an efficient tool for mitigating denial of service (DoS) and distributed denial of service (DDoS) attacks.

## History for the Unicast Reverse Path Forwarding Loose Mode Feature

Release	Modification
12.0(15)S	This feature was introduced.
12.1(8a)E	This feature was integrated into Cisco IOS Release 12.1(8a)E.
12.2(13)T	This feature was integrated into Cisco IOS Release 12.2(13)T.

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for Unicast Reverse Path Forwarding Loose Mode, page 2](#)
- [Information About Unicast Reverse Path Forwarding Loose Mode, page 2](#)
- [How to Configure Unicast Reverse Path Forwarding Loose Mode, page 3](#)
- [Configuration Examples for Unicast Reverse Path Forwarding Loose Mode, page 5](#)
- [Additional References, page 6](#)
- [Command Reference, page 7](#)



**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

## Prerequisites for Unicast Reverse Path Forwarding Loose Mode

- To use Unicast RPF, you must enable Cisco Express Forwarding (CEF) switching or distributed CEF (dCEF) switching in the router. There is no need to configure the input interface for CEF switching. As long as CEF is running on the router, individual interfaces can be configured for other switching modes.

## Information About Unicast Reverse Path Forwarding Loose Mode

Before configuring Unicast Reverse Path Forwarding Loose Check, you should understand the following concepts:

- [Unicast Reverse Path Forwarding: Background, page 2](#)
- [Loose Mode, page 3](#)

## Unicast Reverse Path Forwarding: Background

A number of common types of DoS attacks take advantage of forged or rapidly changing source IP addresses, allowing attackers to thwart efforts by ISPs to locate or filter these attacks. Unicast RPF was originally created to help mitigate such attacks by providing an automated, scalable mechanism to implement the Internet Engineering Task Force (IETF) Best Common Practices 38/Request for Comments 2827 (BCP 38/RFC 2827) anti-spoofing filtering on the customer-to-ISP network edge. By taking advantage of the information stored in the Forwarding Information Base (FIB) that is created by the CEF switching process, Unicast RPF can determine whether IP packets are spoofed or malformed by matching the IP source address and ingress interface against the FIB entry that reaches “back” to this source (a so-called “reverse lookup”). Packets that are received from one of the best reverse path routes back out of the same interface are forwarded as normal. If there is no reverse path route on the same interface from which the packet was received, it might mean that the source address was modified, and the packet is dropped (by default).

This original implementation of Unicast RPF, known as “strict mode,” required a match between the ingress interface and the reverse path FIB entry. With Unicast RPF, all equal-cost “best” return paths are considered valid, meaning that it works for cases in which multiple return paths exist, provided that each path is equal in routing cost to the others (number of hops, weights, and so on), and as long as the route is in the FIB. Unicast RPF also functions when Enhanced Interior Gateway Routing Protocol (EIGRP) variants are being used and unequal candidate paths back to the source IP address exist. The strict mode works well for customer-to-ISP network edge configurations that have symmetrical flows (including some multihomed configurations in which symmetrical flows can be enforced).

However, some customer-to-ISP network edges and nearly all ISP-to-ISP network edges use multihomed configurations in which routing asymmetry is typical. When traffic flows are asymmetrical, that is, those in which traffic from Network A to Network B would normally take a different path from traffic flowing from Network B to Network A, the Unicast RPF check will always fail the strict mode test. Because this type of asymmetric routing is common among ISPs and in the Internet core, the original implementation of Unicast RPF was not available for use by ISPs on their core routers and ISP-to-ISP links.

Over time and with an increase in DDoS attacks on the Internet, the functionality of Unicast RPF was reviewed as a tool that ISPs can use on the ISP-to-ISP network edge (an ISP router “peered” with another ISP router) to enable dynamic BGP, triggered black-hole filtering. To provide this functionality, however, the mechanisms used with Unicast RPF had to be modified to permit its deployment on the ISP-to-ISP network edge so that asymmetrical routing is not an issue.

## Loose Mode

To provide ISPs with a DDoS resistance tool on the ISP-to-ISP edge of a network, Unicast RPF was modified from its original strict mode implementation to check the source addresses of each ingress packet without regard for the specific interface on which it was received. This modification is known as “loose mode.” Loose mode allows Unicast RPF to automatically detect and drop packets such as the following:

- IETF RFC 1918 source addresses
- Other Documenting Special Use Addresses (DUSA) that should not appear in the source
- Unallocated addresses that have not been allocated by the Regional Internet Registries (RIRs)
- Source addresses that are routed to a null interface on the router

Loose mode removes the match requirement on the specific ingress interface, allowing Unicast RPF to loose-check packets. This packet checking allows the “peering” router of an ISP having multiple links to multiple ISPs to check the source IP address of ingress packets to determine whether they exist in the FIB. If they exist, the packets are forwarded. If they do not exist in the FIB, the packets fail and are dropped. This checking increases resistance against DoS and DDoS attacks that use spoofed source addresses and unallocated IP addresses.

## How to Configure Unicast Reverse Path Forwarding Loose Mode

This section contains the following procedure:

- [Configuring Unicast Reverse Path Forwarding Loose Mode, page 3](#)

### Configuring Unicast Reverse Path Forwarding Loose Mode

To configure Unicast RPF loose mode, perform the following steps.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef**
4. **interface** *type slot/port-adapter/port*
5. **ip verify unicast source reachable-via any**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip cef</b>  <b>Example:</b> Router (config)# ip cef	Enables CEF on the route processor card.
Step 4	<b>interface</b> <i>type slot/port-adapter/port</i>  <b>Example:</b> Router (config)# interface serial5/0/0	Configures an interface type and enters interface configuration mode.
Step 5	<b>ip verify unicast source reachable-via any</b> Router (config-if)# ip verify unicast source reachable-via any	Enables Unicast RPF using loose mode.

## Troubleshooting Tips

### CEF Not Enabled

If CEF is not enabled on your device and an attempt is made to deploy Unicast RPF, the following error message is generated:

```
Router(config-if)# ip verify unicast source reachable-via any
% CEF not enabled. Enable first.
```

### Dropped Packets

If it is believed that Unicast RPF is dropping packets that are deemed valid, it may be necessary to configure an access list within Unicast RPF to pass these specific packets.

- Check to see if Unicast RPF is dropping packets using the following **show** commands.

```
Router# show ip traffic | include unicast RPF
```

The above command output displays the global counter for packets dropped by Unicast RPF. If the packet drop counter is increasing, Unicast RPF is dropping packets.

```
Router# show ip interface {type/slot/port} | include verif
```

The above command output displays drop counters on a per-interface basis. If the packet drop counter is increasing, Unicast RPF is dropping packets on the referenced interface.

- Configure a “classification” access list (one that is used to identify traffic types) and add it to the Unicast RPF configuration on the interface or interfaces that are in question.



In this case, the most prudent classification access list would be one that includes a series of “deny” statements covering the traffic types in question (instead of the more traditional “permit” statements that would be used, for example, in a typical classification access list that would be applied directly to an interface). The **logging** keyword may be useful for this access list as well.

- Apply the above access list to Unicast RPF on the interface in question using the following command:

```
Router (config-if)# ip verify unicast source reachable-via any 199
```

- Periodically check the counters on the above access list using the following **show** command:

```
Router# show ip access-list 199
```

If the access list hit counters are increasing for the packet type in question, Unicast RPF is dropping the packets in question. To permit them, configure an access list using a “permit” statement for the packet type in question and apply it to Unicast RPF.

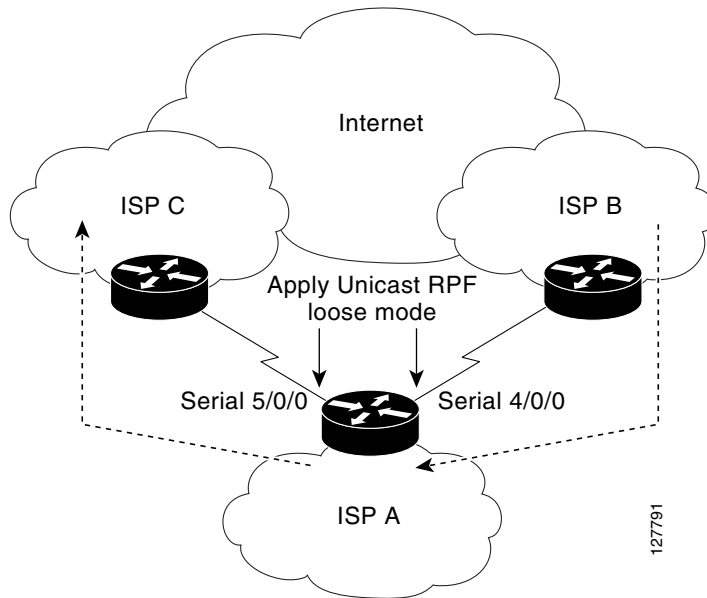
## Configuration Examples for Unicast Reverse Path Forwarding Loose Mode

This section includes the following configuration example:

- [Configuring Unicast RPF Using Loose Mode: Example, page 5](#)

### Configuring Unicast RPF Using Loose Mode: Example

The following example (see [Figure 1](#)) uses a simple dual-homed ISP to demonstrate the concept of Unicast RPF loose mode. The example illustrates an ISP (A) peering router that is connected to two different upstream ISPs (B and C) and shows that traffic flows into and out of ISP A may be asymmetric given this dual-homed configuration. Hence, provisions for asymmetrical flows (when outbound traffic goes out one link and returns via a different link) must be accounted for by the Unicast RPF deployment. In this case, it is appropriate to use the loose-mode configuration of Unicast RPF because this configuration alleviates the interface dependency of strict mode.

**Figure 1**      **Unicast RPF Loose Mode**

```

interface Serial4/0/0
description - link to ISP B
ip address 192.168.200.225 255.255.255.252
no ip redirects
no ip directed-broadcasts
no ip proxy-arp
ip verify unicast source reachable-via any
!
interface Serial5/0/0
description - link to ISP C
ip address 172.16.100.9 255.255.255.252
no ip redirects
no ip directed-broadcasts
no ip proxy-arp
ip verify unicast source reachable-via any
!

```

## Additional References

The following sections provide references related to Unicast Reverse Path Forwarding Loose Check.

## Related Documents

Related Topic	Document Title
Cisco IOS commands	<i>Cisco IOS Command Reference, Release 12.3T</i>
Best practices using Unicast RPF	<i>Internet Service Provider (ISP) Security Bootcamp/Best Practices—CPN—Summit—2004/Paris—Sept—04</i>

## Standards

Standards	Title
No new or modified standards are supported by this feature.	—

## MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	—

## Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log on from this page to access even more content.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html). For information

about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **ip verify unicast reverse-path**
- **ip verify unicast source reachable-via**

---

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



## **Secure Shell**





# Configuring Secure Shell

---

## Feature History

Release	Modification
Cisco IOS	For information about feature support in Cisco IOS software, use Cisco Feature Navigator.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

This chapter describes the Secure Shell (SSH) feature. The SSH feature consists of an application and a protocol.

For a complete description of the SSH commands in this chapter, refer to the chapter “Secure Shell Commands” of the *Cisco IOS Security Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the “Identifying Supported Platforms” section in the chapter “Using Cisco IOS Software.”

## In This Chapter

This chapter has the following sections:

- [About Secure Shell](#)
- [SSH Configuration Task List](#)
- [Troubleshooting Tips](#)
- [Monitoring and Maintaining SSH](#)
- [SSH Configuration Examples](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

# About Secure Shell

Secure Shell (SSH) is an application and a protocol that provide a secure replacement to the Berkeley r-tools. The protocol secures the sessions using standard cryptographic mechanisms, and the application can be used similarly to the Berkeley **rexec** and **rsh** tools. There are currently two versions of SSH available: SSH Version 1 and SSH Version 2. This document describes SSH Version 1. For information about SSH Version 2, see the document *Secure Shell Version 2 Support*.

**Note**

---

Hereafter, unless otherwise noted, the term “SSH” will denote “SSH Version 1” only.

---

This rest of this section covers the following information:

- [How SSH Works](#)
- [Restrictions](#)
- [Related Features and Technologies](#)
- [Prerequisites to Configuring SSH](#)

## How SSH Works

This section provides the following information about how SSH works:

- [SSH Server](#)
- [SSH Integrated Client](#)

### SSH Server

The SSH Server feature enables a SSH client to make a secure, encrypted connection to a Cisco router. This connection provides functionality that is similar to that of an inbound Telnet connection. Before SSH, security was limited to Telnet security. SSH allows a strong encryption to be used with the Cisco IOS software authentication. The SSH server in Cisco IOS software will work with publicly and commercially available SSH clients.

### SSH Integrated Client

The SSH Integrated Client feature is an application running over the SSH protocol to provide device authentication and encryption. The SSH client enables a Cisco router to make a secure, encrypted connection to another Cisco router or to any other device running the SSH server. This connection provides functionality that is similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.

The SSH client in the Cisco IOS software works with publicly and commercially available SSH servers. The SSH client supports the ciphers of Data Encryption Standard (DES), Triple DES (3DES), and password authentication. User authentication is performed like that in the Telnet session to the router. The user authentication mechanisms supported for SSH are RADIUS, TACACS+ and the use of locally stored user names and passwords.

**Note**

---

The SSH client functionality is available only when the SSH server is enabled.

---



## Restrictions

There following are some basic SSH restrictions:

- RSA authentication available in SSH clients is not supported in the SSH server for Cisco IOS software.
- SSH server and SSH client are supported on DES (56-bit) and 3DES (168-bit) data encryption software images only. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.
- Execution shell is the only application supported.
- The login banner is not supported in Secure Shell Version 1. It is supported in Secure Shell Version 2.

## Related Features and Technologies

For more information about SSH-related features and technologies, review the following:

- Authentication, Authorization, and Accounting (AAA) feature. AAA is a suite of network security services that provide the primary framework through which access control can be set up on your Cisco router or access server. For more information on AAA, refer to the Authentication, Authorization, and Accounting chapters earlier in this book and the *Cisco IOS Security Command Reference*.
- IP Security (IPSec) feature. IPSec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses Internet Key Exchange (IKE) to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host. For more information on IPSec, refer to the chapter “Configuring IPSec Network Security” and the *Cisco IOS Security Command Reference*.

## Prerequisites to Configuring SSH


Prior to configuring SSH, perform the following tasks:

- Download the required image on your router. (The SSH server requires you to have an IPSec (DES or 3DES) encryption software image from Cisco IOS Release 12.1(1)T downloaded on your router; the SSH client requires you to have an IPSec (DES or 3DES) encryption software image from Cisco IOS Release 12.1(3)T downloaded on your router.) For more information on downloading a software image, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*.
- Configure a host name and host domain for your router.

To configure a host name and host domain, enter the following commands beginning in global configuration mode:

Command	Purpose
Router(config)# <b>hostname</b> <i>hostname</i>	Configures a host name for your router.
Router(config)# <b>ip domain-name</b> <i>domainname</i>	Configures a host domain for your router.

- Generate an RSA key pair for your router, which automatically enables SSH.  
To generate an RSA key pair, enter the following global configuration command:

Command	Purpose
Router(config)# <b>crypto key generate rsa</b>	<p>Enables the SSH server for local and remote authentication on the router.</p> <p>The recommended minimum modulus size is 1024 bits.</p> <hr/> <p> <b>Note</b> To delete the RSA key-pair, use the <b>crypto key zeroize rsa</b> global configuration command. Once you delete the RSA key-pair, you automatically disable the SSH server.</p>

- Configure user authentication for local or remote access. You can configure authentication with or without AAA. For more information, refer to the “Authentication, Authorization, and Accounting (AAA)” chapters earlier in the book.

## SSH Configuration Task List

The following sections describe the configuration tasks for SSH. Each task in the list is identified as either optional or required.

- [Configuring SSH Server](#) (Required)
- [Verifying SSH](#) (Optional)

See the section “[SSH Configuration Examples](#)” at the end of this chapter.

## Configuring SSH Server



### Note

The SSH client feature runs in user EXEC mode and has no specific configuration on the router.



### Note

The SSH commands are optional and are disabled when the SSH server is disabled.

To enable and configure a Cisco Router for SSH, you can configure SSH parameters. If you do not configure SSH parameters, the the default values will be used.

To configure SSH server, use the following command in global configuration mode:

Command	Purpose
Router(config)# <b>ip ssh</b> {[timeout <i>seconds</i> ]   [authentication-retries <i>integer</i> ]}	<p>(Required) Configures SSH control variables on your router.</p> <ul style="list-style-type: none"> <li>You can specify the timeout in seconds, not to exceed 120 seconds. The default is 120. This setting applies to the SSH negotiation phase. Once the EXEC session starts, the standard timeouts configured for the vty apply.</li> </ul> <p>By default, there are 5 vtys defined (0–4), therefore 5 terminal sessions are possible. After the SSH executes a shell, the vty timeout starts. The vty timeout defaults to 10 minutes.</p> <ul style="list-style-type: none"> <li>You can also specify the number of authentication retries, not to exceed 5 authentication retries. The default is 3.</li> </ul>

## Verifying SSH

To verify that the SSH server is enabled and view the version and configuration data for your SSH connection, use the **show ip ssh** command. The following example shows that SSH is enabled:

```
Router# show ip ssh
```

```
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
```

The following example shows that SSH is disabled:

```
Router# show ip ssh
```

```
%SSH has not been enabled
```

To verify the status of your SSH server connections, use the **show ssh** command. The following example shows the SSH server connections on the router when SSH is enabled:

```
Router# show ssh
Connection Version EncryptionStateUsername
0 1.5 3DESSession Startedguest
```

The following example shows that SSH is disabled:

```
Router# show ssh
```

```
%No SSH server connections running.
```

## Troubleshooting Tips

- If your SSH configuration commands are rejected as illegal commands, you have not successfully generated a RSA key pair for your router. Make sure you have specified a host name and domain. Then use the **crypto key generate rsa** command to generate a RSA key pair and enable the SSH server.
- When configuring the RSA key pair, you might encounter the following error messages:

- No hostname specified  
You must configure a host name for the router using the **hostname** global configuration command. For more information, see [“Prerequisites to Configuring SSH.”](#)
- No domain specified  
You must configure a host domain for the router using the **ip domain-name** global configuration command. For more information, see [“Prerequisites to Configuring SSH.”](#)
- The number of allowable SSH connections is limited to the maximum number of vtys configured for the router. Each SSH connection will use a vty resource.
- SSH uses either local security or the security protocol that is configured through AAA on your router for user authentication. When configuring AAA, you must ensure that the console is not running under AAA by applying a keyword in the global configuration mode to disable AAA on the console.

## Monitoring and Maintaining SSH

To monitor and maintain your SSH connections, use the following commands in user EXEC mode:

Command	Purpose
Router# <b>show ip ssh</b>	Displays the version and configuration data for SSH.
Router# <b>show ssh</b>	Displays the status of SSH server connections.

## SSH Configuration Examples

This section provides the following configuration examples, which are output from the **show running configuration** EXEC command on a Cisco 7200, Cisco 7500, and Cisco 12000.

- [SSH on a Cisco 7200 Series Router Example](#)
- [SSH on a Cisco 7500 Series Router Example](#)
- [SSH on a Cisco 1200 Gigabit Switch Router Example](#)



**Note**

The **crypto key generate rsa** command is not displayed in the **show running configuration** output.

### SSH on a Cisco 7200 Series Router Example

In the following example, SSH is configured on a Cisco 7200 with a timeout that is not to exceed 60 seconds, and no more than 2 authentication retries. Also, before configuring the SSH server feature on the router, TACACS+ is specified as the method of authentication.

```
hostname Router72K
aaa new-model
aaa authentication login default tacacs+
aaa authentication login aaa7200kw none
enable password enable7200pw

username mcisco password 0 maryspw
username jcisco password 0 johnspw
```

```

ip subnet-zero
no ip domain-lookup
ip domain-name cisco.com
! Enter the ssh commands.
ip ssh time-out 60
ip ssh authentication-retries 2

controller E1 2/0

controller E1 2/1

interface Ethernet1/0
ip address 192.168.110.2 255.255.255.0 secondary
ip address 192.168.109.2 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no keepalive
no cdp enable

interface Ethernet1/1
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
no cdp enable

interface Ethernet1/2
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
no cdp enable

no ip classless
ip route 192.168.1.0 255.255.255.0 10.1.10.1
ip route 192.168.9.0 255.255.255.0 10.1.1.1
ip route 192.168.10.0 255.255.255.0 10.1.1.1

map-list atm
ip 10.1.10.1 atm-vc 7 broadcast
no cdp run

tacacs-server host 192.168.109.216 port 9000
tacacs-server key cisco
radius-server host 192.168.109.216 auth-port 1650 acct-port 1651
radius-server key cisco

line con 0
exec-timeout 0 0
login authentication aaa7200kw
transport input none
line aux 0
line vty 0 4
password enable7200pw

end

```

## SSH on a Cisco 7500 Series Router Example

In the following example, SSH is configured on a Cisco 7500 with a timeout that is not to exceed 60 seconds and no more than 5 authentication retries. Before the SSH Server feature is configured on the router, RADIUS is specified as the method of authentication.

```
hostname Router75K
aaa new-model
aaa authentication login default radius
aaa authentication login aaa7500kw none
enable password enable7500pw

username mcisco password 0 maryspw
username jcisco password 0 johnspw
ip subnet-zero
no ip cef
no ip domain-lookup
ip domain-name cisco.com
! Enter ssh commands.
ip ssh time-out 60
ip ssh authentication-retries 5

controller E1 3/0
channel-group 0 timeslots 1

controller E1 3/1
channel-group 0 timeslots 1
channel-group 1 timeslots 2

interface Ethernet0/0/0
no ip address
no ip directed-broadcast
no ip route-cache distributed
shutdown

interface Ethernet0/0/1
no ip address
no ip directed-broadcast
no ip route-cache distributed
shutdown
interface Ethernet0/0/2
no ip address
no ip directed-broadcast
no ip route-cache distributed
shutdown

interface Ethernet0/0/3
no ip address
no ip directed-broadcast
no ip route-cache distributed
shutdown

interface Ethernet1/0
ip address 192.168.110.2 255.255.255.0 secondary
ip address 192.168.109.2 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache

interface Ethernet1/1
ip address 192.168.109.2 255.255.255.0
no ip directed-broadcast
no ip route-cache
```

```
no ip mroute-cache
shutdown

interface Ethernet1/2
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache

interface Ethernet1/3
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown

interface Ethernet1/4
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
interface Ethernet1/5
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown

interface Serial2/0
ip address 10.1.1.2 255.0.0.0
no ip directed-broadcast
encapsulation ppp
no ip route-cache
no ip mroute-cache

ip classless
ip route 192.168.9.0 255.255.255.0 10.1.1.1
ip route 192.168.10.0 255.255.255.0 10.1.1.1

tacacs-server host 192.168.109.216 port 9000
tacacs-server key cisco
radius-server host 192.168.109.216 auth-port 1650 acct-port 1651
radius-server key cisco

line con 0
exec-timeout 0 0
login authentication aaa7500kw
transport input none
line aux 0
transport input all
line vty 0 4

end
```

## SSH on a Cisco 1200 Gigabit Switch Router Example

In the following example, SSH is configured on a Cisco 12000 with a timeout that is not to exceed 60 seconds and no more than 2 authentication retries. Before the SSH Server feature is configured on the router, TACACS+ is specified as the method of authentication.

```

hostname Router12K
aaa new-model
aaa authentication login default tacacs+ local
aaa authentication login aaa12000kw local
enable password enable12000pw

username mcisco password 0 maryspw
username jcisco password 0 johnspw
redundancy
main-cpu
 auto-sync startup-config
ip subnet-zero
no ip domain-lookup
ip domain-name cisco.com
! Enter ssh commands.
ip ssh time-out 60
ip ssh authentication-retries 2

interface ATM0/0
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown

interface POS1/0
ip address 10.100.100.2 255.255.255.0
no ip directed-broadcast
encapsulation ppp
no ip route-cache cef
no keepalive
crc 16
no cdp enable

interface POS1/1
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown
crc 32

interface POS1/2
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown
crc 32

interface POS1/3
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown
crc 32

interface POS2/0
ip address 10.1.1.1 255.255.255.0
no ip directed-broadcast
encapsulation ppp
no ip route-cache cef
crc 16

interface Ethernet0
ip address 172.17.110.91 255.255.255.224
no ip directed-broadcast

```



```
router ospf 1
network 0.0.0.0 255.255.255.255 area 0.0.0.0

ip classless
ip route 0.0.0.0 0.0.0.0 172.17.110.65

logging trap debugging
tacacs-server host 172.17.116.138
tacacs-server key cisco

radius-server host 172.17.116.138 auth-port 1650 acct-port 1651
radius-server key cisco

line con 0
exec-timeout 0 0
login authentication aaa12000kw
transport input none
line aux 0
line vty 0 4

no scheduler max-task-time
no exception linecard slot 0 sqe-registers
no exception linecard slot 1 sqe-registers
no exception linecard slot 2 sqe-registers
no exception linecard slot 3 sqe-registers
no exception linecard slot 4 sqe-registers
no exception linecard slot 5 sqe-registers
no exception linecard slot 6 sqe-registers
end
```

---

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0805R)

---

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.





## Reverse SSH Enhancements

---

The Reverse SSH Enhancements feature provides an alternative method of configuring reverse Secure Shell (SSH). Using this feature, you can configure reverse SSH without having to list separate lines for every terminal or auxiliary line on which SSH has to be enabled. This feature also eliminates the rotary-group limitation. This feature is supported for SSH Version 1 and SSH Version 2.

### Feature History for Reverse SSH Enhancements

Release	Modification
12.3(11)T	This feature was introduced.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for Reverse SSH Enhancements, page 2](#)
- [Restrictions for Reverse SSH Enhancements, page 2](#)
- [Information About Reverse SSH Enhancements, page 2](#)
- [How to Configure Reverse SSH Enhancements, page 2](#)
- [Configuration Examples for Reverse SSH Enhancements, page 7](#)
- [Additional References, page 8](#)
- [Command Reference, page 9](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

## Prerequisites for Reverse SSH Enhancements

- SSH must be enabled.
- The SSH client and server must be running the same version of SSH.

## Restrictions for Reverse SSH Enhancements

- The **-I** keyword and *userid* :{number} {ip-address} delimiter and arguments are mandatory when configuring the alternative method of Reverse SSH for console access.

## Information About Reverse SSH Enhancements

To configure Reverse SSH Enhancements, you should understand the following concepts:

- [Reverse Telnet, page 2](#)
- [Reverse SSH, page 2](#)

## Reverse Telnet

Cisco IOS software has for quite some time included a feature called Reverse Telnet, whereby you can telnet to a certain port range and connect to terminal or auxiliary lines. Reverse telnetting has often been used to connect a Cisco IOS router that has many terminal lines to the consoles of other Cisco IOS routers or to other devices. Telnetting makes it easy to reach the router console from anywhere simply by telnetting to the terminal server on a specific line. This telnetting approach can be used to configure a router even if all network connectivity to that router is disconnected. Reverse telnetting also allows modems that are attached to Cisco IOS routers to be used for dial-out (usually with a rotary device).

## Reverse SSH

Reverse telnetting can be accomplished using SSH. Unlike reverse telnetting, SSH provides for secure connections. The Reverse SSH Enhancements feature provides you with a simplified method of configuring SSH. Using this feature, you no longer have to configure a separate line for every terminal or auxiliary line on which you want to enable SSH. The previous method of configuring reverse SSH limited the number of ports that can be accessed to 100. The Reverse SSH Enhancements feature removes the port number limitation. For information on the alternative method of configuring reverse SSH, see the section “[How to Configure Reverse SSH Enhancements.](#)”

## How to Configure Reverse SSH Enhancements

This section contains the following procedures:

- [Configuring Reverse SSH for Console Access, page 3](#)
- [Configuring Reverse SSH for Modem Access, page 4](#)

- [Troubleshooting Reverse SSH on the Client, page 6](#)
- [Troubleshooting Reverse SSH on the Server, page 6](#)

## Configuring Reverse SSH for Console Access

To configure reverse SSH console access on the SSH server, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line** *line-number* [*ending-line-number*]
4. **no exec**
5. **login authentication** *listname*
6. **transport input ssh**
7. **exit**
8. **exit**
9. **ssh -l** *userid*:*{number}* *{ip-address}*

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>line</b> <i>line-number</i> [ <i>ending-line-number</i> ]  <b>Example:</b> Router# line 1 3	Identifies a line for configuration and enters line configuration mode.
Step 4	<b>no exec</b>  <b>Example:</b> Router (config-line)# no exec	Disables EXEC processing on a line.
Step 5	<b>login authentication</b> <i>listname</i>  <b>Example:</b> Router (config-line)# login authentication default	Defines a login authentication mechanism for the lines. <b>Note</b> The authentication method must use a username and password.

	Command or Action	Purpose
Step 6	<b>transport input ssh</b>  <b>Example:</b> Router (config-line)# transport input ssh	Defines which protocols to use to connect to a specific line of the router. <ul style="list-style-type: none"><li>The <b>ssh</b> keyword must be used for the Reverse SSH Enhancements feature.</li></ul>
Step 7	<b>exit</b>  <b>Example:</b> Router (config-line)# exit	Exits line configuration mode.
Step 8	<b>exit</b>  <b>Example:</b> Router (config)# exit	Exits global configuration mode.
Step 9	<b>ssh -l userid:{number} {ip-address}</b>  <b>Example:</b> Router# ssh -l lab:1 router.example.com	Specifies the user ID to use when logging in on the remote networking device that is running the SSH server. <ul style="list-style-type: none"><li><i>userid</i>—User ID.</li><li><b>:—Signifies that a port number and terminal IP address will follow the <i>userid</i> argument.</b></li><li><i>number</i>—Terminal or auxiliary line number.</li><li><i>ip-address</i>—Terminal server IP address.</li></ul> <b>Note</b> The <i>userid</i> argument and <b>:rotary{number}{ip-address}</b> delimiter and arguments are mandatory when configuring the alternative method of Reverse SSH for modem access.

## Configuring Reverse SSH for Modem Access

To configure Reverse SSH for modem access, perform the steps shown in the “SUMMARY STEPS” section below.

In this configuration, reverse SSH is being configured on a modem used for dial-out lines. To get any of the dial-out modems, you can use any SSH client and start a SSH session as shown (in Step 10) to get to the next available modem from the rotary device.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line line-number [ending-line-number]**
4. **no exec**
5. **login authentication listname**
6. **rotary group**
7. **transport input ssh**

8. **exit**
9. **exit**
10. **ssh -l userid:rotary{number} {ip-address}**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>line line-number [ending-line-number]</b>  <b>Example:</b> Router# line 1 200	Identifies a line for configuration and enters line configuration mode.
Step 4	<b>no exec</b>  <b>Example:</b> Router (config-line)# no exec	Disables EXEC processing on a line.
Step 5	<b>login authentication listname</b>  <b>Example:</b> Router (config-line)# login authentication default	Defines a login authentication mechanism for the lines. <p><b>Note</b> The authentication method must use a username and password.</p>
Step 6	<b>rotary group</b>  <b>Example:</b> Router (config-line)# rotary 1	Defines a group of lines consisting of one or more virtual terminal lines or one auxiliary port line.
Step 7	<b>transport input ssh</b>  <b>Example:</b> Router (config-line)# transport input ssh	Defines which protocols to use to connect to a specific line of the router. <ul style="list-style-type: none"> <li>The <b>ssh</b> keyword must be used for the Reverse SSH Enhancements feature.</li> </ul>
Step 8	<b>exit</b>  <b>Example:</b> Router (config-line)# exit	Exits line configuration mode.
Step 9	<b>exit</b>  <b>Example:</b> Router (config)# exit	Exits global configuration mode.

	Command or Action	Purpose
Step 10	<b>ssh -l <i>userid</i>:rotary{<i>number</i>} {<i>ip-address</i>}</b>  <b>Example:</b> Router# ssh -l lab:rotary1 router.example.com	Specifies the user ID to use when logging in on the remote networking device that is running the SSH server. <ul style="list-style-type: none"> <li><i>userid</i>—User ID.</li> <li><b>:</b>—Signifies that a port number and terminal IP address will follow the <i>userid</i> argument.</li> <li><i>number</i>—Terminal or auxiliary line number.</li> <li><i>ip-address</i>—Terminal server IP address.</li> </ul> <b>Note</b> The <i>userid</i> argument and <b>:rotary{<i>number</i>}{<i>ip-address</i>}</b> delimiter and arguments are mandatory when configuring the alternative method of Reverse SSH for modem access.

## Troubleshooting Reverse SSH on the Client

To troubleshoot the reverse SSH configuration on the client (remote device), perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **debug ip ssh client**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>debug ip ssh client</b>  <b>Example:</b> Router# debug ip ssh client	Displays debugging messages for the SSH client.

## Troubleshooting Reverse SSH on the Server

To troubleshoot the reverse SSH configuration on the terminal server, perform the following steps. The steps may be configured in any order or independent of one another.



## SUMMARY STEPS

1. `enable`
2. `debug ip ssh`
3. `show ssh`
4. `show line`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<code>debug ip ssh</code>  <b>Example:</b> Router# <code>debug ip ssh</code>	Displays debugging messages for the SSH server.
Step 3	<code>show ssh</code>  <b>Example:</b> Router# <code>show ssh</code>	Displays the status of the SSH server connections.
Step 4	<code>show line</code>  <b>Example:</b> Router# <code>show line</code>	Displays parameters of a terminal line.

# Configuration Examples for Reverse SSH Enhancements

This section includes the following configuration examples:

- [Reverse SSH Console Access: Example, page 7](#)
- [Reverse SSH Modem Access: Example, page 8](#)

## Reverse SSH Console Access: Example

The following configuration example shows that reverse SSH has been configured for console access for terminal lines 1 through 3:

### Terminal Server Configuration

```
line 1 3
 no exec
 login authentication default
 transport input ssh
```

**Client Configuration**

The following commands configured on the SSH client will form the reverse SSH session with lines 1, 2, and 3, respectively:

```
ssh -l lab:1 router.example.com
ssh -l lab:2 router.example.com
ssh -l lab:3 router.example.com
```

## Reverse SSH Modem Access: Example

The following configuration example shows that dial-out lines 1 through 200 have been grouped under rotary group 1 for modem access:

```
line 1 200
 no exec
 login authentication default
 rotary 1
 transport input ssh
 exit
```

The following command shows that reverse SSH will connect to the first free line in the rotary group:

```
ssh -l lab:rotary1 router.example.com
```

## Additional References

The following sections provide references related to Reverse SSH Enhancements.

### Related Documents

Related Topic	Document Title
Configuring Secure Shell	The following chapters of the Cisco <i>IOS Security Configuration Guide</i> : <ul style="list-style-type: none"> <li>• <a href="#">Configuring Secure Shell</a></li> <li>• <a href="#">Secure Shell Version 2 Support</a></li> <li>• <a href="#">SSH Terminal-Line Access</a></li> </ul>
Security commands	<a href="#">Cisco IOS Security Command Reference</a>

### Standards

Standards	Title
No new or modified standards are supported by this feature.	—

## MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	—

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- `ssh`

---

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



# Secure Copy

---

The Secure Copy (SCP) feature provides a secure and authenticated method for copying router configuration or router image files. SCP relies on Secure Shell (SSH), an application and a protocol that provide a secure replacement for the Berkeley r-tools.

## Feature History for Secure Copy

Release	Modification
12.2(2)T	This feature was introduced.
12.0(21)S	This feature was integrated into Cisco IOS 12.0(21)S.
12.2(25)S	This feature was integrated into Cisco IOS 12.2(25)S.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for Secure Copy, page 2](#)
- [Information About Secure Copy, page 2](#)
- [How to Configure SCP, page 2](#)
- [Configuration Examples for Secure Copy, page 4](#)
- [Additional References, page 5](#)
- [Command Reference, page 6](#)
- [Glossary, page 8](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

## Prerequisites for Secure Copy

- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the router.
- Because SCP relies on SSH for its secure transport, the router must have an Rivest, Shamir, and Adelman (RSA) key pair.

## Information About Secure Copy

To configure Secure Copy feature, you should understand the following concepts.

- [How SCP Works, page 2](#)

## How SCP Works

The behavior of SCP is similar to that of remote copy (r<sub>cp</sub>), which comes from the Berkeley r-tools suite, except that SCP relies on SSH for security. In addition, SCP requires that authentication, authorization, and accounting (AAA) authorization be configured so the router can determine whether the user has the correct privilege level.

SCP allows a user who has appropriate authorization to copy any file that exists in the Cisco IOS File System (IFS) to and from a router by using the **copy** command. An authorized administrator may also perform this action from a workstation.

## How to Configure SCP

This section contains the following procedures:

- [Configuring SCP, page 2](#)
- [Verifying SCP, page 3](#)
- [Troubleshooting SCP, page 4](#)

## Configuring SCP

To enable and configure a Cisco router for SCP server-side functionality, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** {default | list-name} method1 [method2...]
5. **aaa authorization** {network | exec | commands level | reverse-access | configuration} {default | list-name} [method1 [method2...]]
6. **username** name [privilege level] {password encryption-type encrypted-password}

## 7. ip scp server enable

### DETAILED STEPS

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>aaa new-model</b>  <b>Example:</b> Router (config)# aaa new-model	Sets AAA authentication at login.
Step 4	<b>aaa authentication login {default   list-name} method1 [method2...]</b>  <b>Example:</b> Router (config)# aaa authentication login default group tacacs+	Enables the AAA access control system.
Step 5	<b>aaa authorization {network   exec   commands level   reverse-access   configuration} {default   list-name} [method1 [method2...]]</b>  <b>Example:</b> Router (config)# aaa authorization exec default group tacacs+	Sets parameters that restrict user access to a network.  <b>Note</b> The <b>exec</b> keyword runs authorization to determine if the user is allowed to run an EXEC shell; therefore, you must use it when you configure SCP.
Step 6	<b>username name [privilege level] {password encryption-type encrypted-password}</b>  <b>Example:</b> Router (config)# username superuser privilege 2 password 0 superpassword	Establishes a username-based authentication system.  <b>Note</b> You may skip this step if a network-based authentication mechanism—such as TACACS+ or RADIUS—has been configured.
Step 7	<b>ip scp server enable</b>  <b>Example:</b> Router (config)# ip scp server enable	Enables SCP server-side functionality.

## Verifying SCP

To verify SCP server-side functionality, perform the following steps.

**SUMMARY STEPS**

1. `enable`
2. `show running-config`

**DETAILED STEPS**

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>show running-config</b>  <b>Example:</b> Router# show running-config	Verifies the SCP server-side functionality.

**Troubleshooting SCP**

To troubleshoot SCP authentication problems, perform the following steps.

**SUMMARY STEPS**

1. `enable`
2. `debug ip scp`

**DETAILED STEPS**

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>debug ip scp</b>  <b>Example:</b> Router# debug ip scp	Troubleshoots SCP authentication problems.

**Configuration Examples for Secure Copy**

This section provides the following configuration examples:

- [SCP Server-Side Configuration Using Local Authentication: Example, page 5](#)
- [SCP Server-Side Configuration Using Network-Based Authentication: Example, page 5](#)



## SCP Server-Side Configuration Using Local Authentication: Example

The following example shows how to configure the server-side functionality of SCP. This example uses a locally defined username and password.

```
! AAA authentication and authorization must be configured properly for SCP to work.
aaa new-model
aaa authentication login default local
aaa authorization exec default local
username tiger privilege 15 password 0 lab
! SSH must be configured and functioning properly.
ip ssh time-out 120
ip ssh authentication-retries 3
ip scp server enable
```

## SCP Server-Side Configuration Using Network-Based Authentication: Example

The following example shows how to configure the server-side functionality of SCP using a network-based authentication mechanism:

```
! AAA authentication and authorization must be configured properly for SCP to work.
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
! SSH must be configured and functioning properly.
ip ssh time-out 120
ip ssh authentication-retries 3
ip scp server enable
```

## Additional References

The following sections provide references related to Secure Copy.

## Related Documents

Related Topic	Document Title
Secure Shell	<ul style="list-style-type: none"> <li><a href="#">Secure Shell Version 1 Support</a></li> <li><a href="#">Secure Shell Version 2 Support</a></li> </ul>
Authentication and authorization commands	<a href="#">Cisco IOS Security Command Reference</a> , Release 12.3 T
Configuring authentication and authorization	“ <a href="#">Authentication, Authorization, and Accounting (AAA)</a> ” section of <a href="#">Cisco IOS Security Configuration Guide</a> , Release 12.3

## Standards

Standards	Title
No new or modified standards are supported by this feature.	—

## MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	—

## Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug ip scp**
- **ip scp server enable**

# Glossary

**AAA**—authentication, authorization, and accounting. Framework of security services that provide the method for identifying users (authentication), for remote access control (authorization), and for collecting and sending security server information used for billing, auditing, and reporting (accounting).

**rcp**—remote copy. Relying on Remote Shell (Berkeley r-tools suite) for security, rcp copies files, such as router images and startup configurations, to and from routers.

**SCP**—secure copy. Relying on SSH for security, SCP support allows the secure and authenticated copying of anything that exists in the Cisco IOS File Systems. SCP is derived from rcp.

**SSH**—Secure Shell. Application and a protocol that provide a secure replacement for the Berkeley r-tools. The protocol secures the sessions using standard cryptographic mechanisms, and the application can be used similarly to the Berkeley rexec and rsh tools. SSH Version 1 is implemented in the Cisco IOS software.



---

**Note**

Refer to [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

---



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



# Secure Shell Version 2 Support

---

**First Published: November 3, 2003**

**Last Updated: July 11, 2008**

The Secure Shell Version 2 Support feature allows you to configure Secure Shell (SSH) Version 2 (SSH Version 1 support was implemented in an earlier Cisco IOS software release). SSH runs on top of a reliable transport layer and provides strong authentication and encryption capabilities. Currently, the only reliable transport that is defined for SSH is TCP. SSH provides a means to securely access and securely execute commands on another computer over a network. The Secure Copy Protocol (SCP) feature that is provided with SSH also allows for the secure transfer of files.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Secure Shell Version 2 Support” section on page 20](#).

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for Secure Shell Version 2 Support, page 2](#)
- [Restrictions for Secure Shell Version 2 Support, page 2](#)
- [Information About Secure Shell Version 2 Support, page 2](#)
- [How to Configure Secure Shell Version 2 Support, page 4](#)
- [Configuration Examples for Secure Shell Version 2 Support, page 13](#)
- [Where to Go Next, page 17](#)
- [Additional References, page 17](#)
- [Command Reference, page 19](#)
- [Feature Information for Secure Shell Version 2 Support, page 20](#)



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

## Prerequisites for Secure Shell Version 2 Support

Prior to configuring SSH, perform the following task:

- Download the required image on your router. The SSH server requires you to have a k9 (Triple Data Encryption Standard [3DES]) software image from Cisco IOS Release 12.3(4)T, 12.2(25)S, or 12.3(7)JA downloaded on your router.

**Note**

The SSH Version 2 server is supported in Cisco IOS Release 12.3(4)T, 12.3(2)XE, 12.2(25)S, and 12.3(7)JA; the SSH Version 2 client is supported beginning with Cisco IOS Release 12.3(7)T and is supported in Cisco IOS Release 12.3(7)JA. (The SSH client runs both the SSH Version 1 and Version 2 protocol and is supported in both k8 and k9 images in Cisco IOS Release 12.3(4)T.)

For more information on downloading a software image, refer to [Cisco IOS Configuration Fundamentals and Network Management Configuration Guide](#).

## Restrictions for Secure Shell Version 2 Support

- Rivest, Shamir, and Adelman (RSA) user authentication is not supported in the SSH server or SSH client for Cisco IOS software.
- SSH servers and SSH clients are supported in 3DES software images.
- Execution Shell, remote command execution, and Secure Copy Protocol (SCP) are the only applications supported.
- Compression is not supported.
- The RSA key-pair size must be greater than or equal to 768.

## Information About Secure Shell Version 2 Support

To configure SSH Version 2, you should understand the following concept:

- [Secure Shell Version 2, page 2](#)
- [SNMP Trap Generation, page 3](#)
- [SSH Keyboard Interactive Authentication, page 4](#)

## Secure Shell Version 2

The Secure Shell Version 2 Support feature allows you to configure SSH Version 2.

The configuration for the SSH Version 2 server is similar to the configuration for SSH Version 1. The command **ip ssh version** has been introduced so that you may define which version of SSH that you want to configure. If you do not configure this command, SSH by default runs in compatibility mode; that is, both SSH Version 1 and SSH Version 2 connections are honored.

**Note**

SSH Version 1 is a protocol that has never been defined in a standard. If you do not want your router to fall back to the undefined protocol (Version 1), you should use the **ip ssh version** command and specify Version 2.

The **ip ssh rsa keypair-name** command was also introduced in Cisco IOS Release 12.3(4)T so that you can enable a SSH connection using RSA keys that you have configured. Previously, SSH was linked to the first RSA keys that were generated (that is, SSH was enabled when the first RSA key pair was generated). The behavior still exists, but by using the **ip ssh rsa keypair-name** command, you can overcome that behavior. If you configure the **ip ssh rsa keypair-name** command with a key-pair name, SSH is enabled if the key pair exists, or SSH will be enabled if the key pair is generated later. If you use this command to enable SSH, you are not forced to configure a host name and a domain name, which was required in SSH Version 1 of the Cisco IOS software.

**Note**

The login banner is supported in Secure Shell Version 2, but it is not supported in Secure Shell Version 1.

## Secure Shell Version 2 Enhancements

The Secure Shell Version 2 Enhancements include a number of additional capabilities such as supporting VRF aware SSH, SSH debug enhancements, and Diffie-Hellman group exchange support.

The Cisco IOS SSH implementation has traditionally used 768 bit modulus but with an increasing need for higher key sizes to accommodate Diffie-Hellman (DH) Group 14 (2048 bits) and Group 16 (4096 bits) cryptographic applications a message exchange between the client and server to establish the favored DH group becomes necessary. The **ip ssh dh min size** command was introduced in Cisco IOS Release 12.4(20)T so you can configure modulus size on the SSH server. In addition to this the **ssh** command was extended to add VRF awareness to SSH client side functionality through which the VRF instance name in the client is provided with the IP address to look up the correct routing table and establish a connection.

Debugging has been enhanced by modifying SSH debug commands. The **debug ip ssh** command has been extended to allow you to simplify the debugging process. Previously this command printed all debug messages related to SSH regardless of what was specifically required. The behavior still exists, but if you configure the **debug ip ssh** command with a keyword messages are limited to information specified by the keyword.

## SNMP Trap Generation

Effective with Cisco IOS Release 12.4(17), Simple Network Management Protocol (SNMP) traps will be generated automatically when an SSH session terminates if the traps have been enabled and SNMP debugging has been turned on. For information about enabling SNMP traps, see the chapter “[Configuring SNMP Support](#)” in the *Cisco IOS Network Management Configuration Guide*.

**Note**

When configuring the **snmp-server host** command, the IP address must be the address of the PC that has the SSH (telnet) client and that has IP connectivity to the SSH server. For an example of an SNMP trap generation configuration, see the section “[Setting an SNMP Trap: Example](#).”

You must also turn on SNMP debugging using the **debug snmp packet** command to display the traps. The trap information includes information such as the number of bytes sent and the protocol that was used for the SSH session. For an example of SNMP debugging, see the section “[SNMP Debugging: Example](#).”

## SSH Keyboard Interactive Authentication

The SSH Keyboard Interactive Authentication feature, also known as Generic Message Authentication for SSH, is a method that can be used to implement different types of authentication mechanisms. Basically, any currently supported authentication method that requires only user input can be performed with this feature. The feature is automatically deployed.

The following methods are currently supported:

- Password
- SecurID and hardware tokens printing a number or a string in response to a challenge sent by the server
- Pluggable Authentication Module (PAM)
- S/KEY (and other One-Time-Pads)

For examples of various scenarios in which the SSH Keyboard Interactive Authentication feature has been automatically deployed, see the chapter “[SSH Keyboard Interactive Authentication: Examples](#).”

## How to Configure Secure Shell Version 2 Support

This section contains the following procedures:

- [Configuring a Router for SSH Version 2 Using a Host Name and Domain Name, page 4](#) (required)
- [Configuring a Router for SSH Version 2 Using RSA Key Pairs, page 5](#) (optional)
- [Starting an Encrypted Session with a Remote Device, page 7](#) (optional)
- [Verifying the Status of the Secure Shell Connection Using the show ssh Command, page 7](#) (optional)
- [Verifying the Secure Shell Status Using the show ip ssh Command, page 9](#) (optional)
- [Monitoring and Maintaining Secure Shell Version 2, page 10](#) (optional)

## Configuring a Router for SSH Version 2 Using a Host Name and Domain Name

To configure your router for SSH Version 2 using a host name and domain name, perform the following steps. You may also configure SSH Version 2 by using the RSA key pair configuration (See the section “[Configuring a Router for SSH Version 2 Using RSA Key Pairs](#)”).

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **hostname** *hostname*
4. **ip domain-name** *name*



5. **crypto key generate rsa**
6. **ip ssh [timeout *seconds* | authentication-retries *integer*]**
7. **ip ssh version [1 | 2]**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>hostname <i>hostname</i></b>  <b>Example:</b> Router (config)# hostname cisco 7200	Configures a host name for your router.
Step 4	<b>ip domain-name <i>name</i></b>  <b>Example:</b> Router (config)# ip domain-name cisco.com	Configures a domain name for your router.
Step 5	<b>crypto key generate rsa</b>  <b>Example:</b> Router (config)# crypto key generate rsa	Enables the SSH server for local and remote authentication.
Step 6	<b>ip ssh [timeout <i>seconds</i>   authentication-retries <i>integer</i>]</b>  <b>Example:</b> Router (config)# ip ssh timeout 120	(Optional) Configures SSH control variables on your router.
Step 7	<b>ip ssh version [1   2]</b>  <b>Example:</b> Router (config)# ip ssh version 1	(Optional) Specifies the version of SSH to be run on your router.

## Configuring a Router for SSH Version 2 Using RSA Key Pairs

To enable SSH Version 2 without configuring a host name or domain name, perform the following steps. SSH Version 2 will be enabled if the key pair that you configure already exists or if it is generated later. You may also configure SSH Version 2 by using the host name and domain name configuration (See the section “[Configuring a Router for SSH Version 2 Using a Host Name and Domain Name](#)”).

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ssh rsa keypair-name** *keypair-name*
4. **crypto key generate rsa usage-keys label** *key-label* **modulus** *modulus-size*
5. **ip ssh [timeout** *seconds* **| authentication-retries** *integer***]**
6. **ip ssh version 2**

## DETAILED STEPS

Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip ssh rsa keypair-name</b> <i>keypair-name</i>  <b>Example:</b> Router (config)# ip ssh rsa keypair-name sshkeys	Specifies which RSA keypair to use for SSH usage.  <b>Note</b> A Cisco IOS router can have many RSA key pairs.
Step 4	<b>crypto key generate rsa usage-keys label</b> <i>key-label</i> <b>modulus</b> <i>modulus-size</i>  <b>Example:</b> Router (config)# crypto key generate rsa usage-keys label sshkeys modulus 768	Enables the SSH server for local and remote authentication on the router.  For SSH Version 2, the modulus size must be at least 768 bits.  <b>Note</b> To delete the RSA key-pair, use the <b>crypto key zeroize rsa</b> command. After you have deleted the RSA key-pair, you automatically disable the SSH server.
Step 5	<b>ip ssh [timeout</b> <i>seconds</i> <b> </b> <b>authentication-retries</b> <i>integer</i> <b>]</b>  <b>Example:</b> Router (config)# ip ssh timeout 120	Configures SSH control variables on your router.
Step 6	<b>ip ssh version 2</b>  <b>Example:</b> Router (config)# ip ssh version 2	Specifies the version of SSH to be run on a router.

## Starting an Encrypted Session with a Remote Device

To start an encrypted session with a remote networking device, perform the following step. (You do not have to enable your router. SSH can be run in disabled mode.)



### Note

The device you wish to connect with must support a SSH server that has an encryption algorithm that is supported in Cisco IOS software.

### SUMMARY STEPS

1. `ssh [-v {1 | 2}] [-c {3des | aes128-cbc | aes192-cbc | aes256-cbc}] [-m {hmac-md5 | hmac-md5-96 | hmac-sha1 | hmac-sha1-96}] [1 userid] [-o numberofpasswordprompts n] [-p port-num] {ip-addr | hostname} [command]`

### DETAILED STEPS

#### Step 1

```
ssh [-v {1 | 2}] [-c {3des | aes128-cbc |
aes192-cbc | aes256-cbc}] [-m {hmac-md5 |
hmac-md5-96 | hmac-sha1 | hmac-sha1-96}] [1
userid] [-o numberofpasswordprompts n] [-p
port-num] {ip-addr | hostname} [command]
```

#### Example:

```
Router# ssh -v 2 -c aes256-cbc -m hmac-sha1-96
-l user2 10.76.82.24
```

Or

The above example adheres to the SSH Version 2 conventions. A more natural and common way to start a session is by linking the username with the hostname. For example, the following configuration example provides an end result that is identical to that of the above example:

```
Router# ssh -v 2 -c aes256-cbc -m hmac-sha1-96
user2@10.76.82.24
```

Starts an encrypted session with a remote networking device.

### Troubleshooting Tips

The **ip ssh version** command can be used for troubleshooting your SSH configuration. By changing versions, you can determine which SSH version has a problem.

## Verifying the Status of the Secure Shell Connection Using the show ssh Command

To display the status of the SSH connection on your router, use the **show ssh** command.

SUMMARY STEPS

- 1. enable
- 2. show ssh

DETAILED STEPS

Step 1	<div>enable</div> <div>Example: Router&gt; enable</div>	<div>Enables privileged EXEC mode.</div> <div><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul></div>
Step 2	<div>show ssh</div> <div>Example: Router# show ssh</div>	<div>Displays the status of SSH server connections.</div>

Examples

The following output examples from the **show ssh** command display status about various SSH Version 1 and Version 2 connections.

Version 1 and Version 2 Connections

```
Router# show ssh

Connection Version Encryption State Username
0 1.5 3DES Session started lab
Connection Version Mode Encryption Hmac State
Username
1 2.0 IN aes128-cbc hmac-md5 Session started lab
1 2.0 OUT aes128-cbc hmac-md5 Session started lab
```

Version 2 Connection with No Version 1

```
Router# show ssh

Connection Version Mode Encryption Hmac State
Username
1 2.0 IN aes128-cbc hmac-md5 Session started lab
1 2.0 OUT aes128-cbc hmac-md5 Session started lab
%No SSHv1 server connections running.
```

Version 1 Connection with No Version 2

```
Router# show ssh

Connection Version Encryption State Username
0 1.5 3DES Session started lab
%No SSHv2 server connections running.
```

# Verifying the Secure Shell Status Using the show ip ssh Command

To verify your SSH configuration, perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **show ip ssh**

## DETAILED STEPS

Step 1	<b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
	<b>Example:</b> Router> enable	
Step 2	<b>show ip ssh</b>	Displays the version and configuration data for SSH.
	<b>Example:</b> Router# show ip ssh	

## Examples

The following examples from the **show ip ssh** command display the version of SSH that is enabled, the authentication timeout values, and the number of authentication retries.

### Version 1 and Version 2 Connections

```

router# show ip ssh

3d06h: %SYS-5-CONFIG_I: Configured from console by consoleh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3

```

### Version 2 Connection with No Version 1

```

Router# show ip ssh

SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3

```

### Version 1 Connection with No Version 2

```

Router# show ip ssh

3d06h: %SYS-5-CONFIG_I: Configured from console by console
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3

```

## Monitoring and Maintaining Secure Shell Version 2

To display debug messages about the SSH connections, use the **debug ip ssh** command.

### SUMMARY STEPS

1. **enable**
2. **debug ip ssh**
3. **debug snmp packet**

### DETAILED STEPS

Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>debug ip ssh</b>  <b>Example:</b> Router# debug ip ssh	Displays debugging messages for SSH.
Step 3	<b>debug snmp packet</b>  <b>Example:</b> Router# debug snmp packet	Displays information about every SNMP packet sent or received by the router.

### Example

The following output from the **debug ip ssh** command shows that the digit 2 keyword has been assigned, signifying that it is an SSH Version 2 connection.

```
Router# debug ip ssh

00:33:55: SSH1: starting SSH control process
00:33:55: SSH1: sent protocol version id SSH-1.99-Cisco-1.25
00:33:55: SSH1: protocol version id is - SSH-2.0-OpenSSH_2.5.2p2
00:33:55: SSH2 1: send: len 280 (includes padlen 4)
00:33:55: SSH2 1: SSH2_MSG_KEXINIT sent
00:33:55: SSH2 1: ssh_receive: 536 bytes received
00:33:55: SSH2 1: input: packet len 632
00:33:55: SSH2 1: partial packet 8, need 624, maclen 0
00:33:55: SSH2 1: ssh_receive: 96 bytes received
00:33:55: SSH2 1: partial packet 8, need 624, maclen 0
00:33:55: SSH2 1: input: padlen 11
00:33:55: SSH2 1: received packet type 20
00:33:55: SSH2 1: SSH2_MSG_KEXINIT received
00:33:55: SSH2: kex: client->server aes128-cbc hmac-md5 none
00:33:55: SSH2: kex: server->client aes128-cbc hmac-md5 none
00:33:55: SSH2 1: expecting SSH2_MSG_KEXDH_INIT
00:33:55: SSH2 1: ssh_receive: 144 bytes received
00:33:55: SSH2 1: input: packet len 144
00:33:55: SSH2 1: partial packet 8, need 136, maclen 0
00:33:55: SSH2 1: input: padlen 5
00:33:55: SSH2 1: received packet type 30
```

```
00:33:55: SSH2 1: SSH2_MSG_KEXDH_INIT received
00:33:55: SSH2 1: signature length 111
00:33:55: SSH2 1: send: len 384 (includes padlen 7)
00:33:55: SSH2: kex_derive_keys complete
00:33:55: SSH2 1: send: len 16 (includes padlen 10)
00:33:55: SSH2 1: newkeys: mode 1
00:33:55: SSH2 1: SSH2_MSG_NEWKEYS sent
00:33:55: SSH2 1: waiting for SSH2_MSG_NEWKEYS
00:33:55: SSH2 1: ssh_receive: 16 bytes received
00:33:55: SSH2 1: input: packet len 16
00:33:55: SSH2 1: partial packet 8, need 8, maclen 0
00:33:55: SSH2 1: input: padlen 10
00:33:55: SSH2 1: newkeys: mode 0
00:33:55: SSH2 1: received packet type 2100:33:55: SSH2 1: SSH2_MSG_NEWKEYS received
00:33:56: SSH2 1: ssh_receive: 48 bytes received
00:33:56: SSH2 1: input: packet len 32
00:33:56: SSH2 1: partial packet 16, need 16, maclen 16
00:33:56: SSH2 1: MAC #3 ok
00:33:56: SSH2 1: input: padlen 10
00:33:56: SSH2 1: received packet type 5
00:33:56: SSH2 1: send: len 32 (includes padlen 10)
00:33:56: SSH2 1: done calc MAC out #3
00:33:56: SSH2 1: ssh_receive: 64 bytes received
00:33:56: SSH2 1: input: packet len 48
00:33:56: SSH2 1: partial packet 16, need 32, maclen 16
00:33:56: SSH2 1: MAC #4 ok
00:33:56: SSH2 1: input: padlen 9
00:33:56: SSH2 1: received packet type 50
00:33:56: SSH2 1: send: len 32 (includes padlen 13)
00:33:56: SSH2 1: done calc MAC out #4
00:34:04: SSH2 1: ssh_receive: 160 bytes received
00:34:04: SSH2 1: input: packet len 64
00:34:04: SSH2 1: partial packet 16, need 48, maclen 16
00:34:04: SSH2 1: MAC #5 ok
00:34:04: SSH2 1: input: padlen 13
00:34:04: SSH2 1: received packet type 50
00:34:04: SSH2 1: send: len 16 (includes padlen 10)
00:34:04: SSH2 1: done calc MAC out #5
00:34:04: SSH2 1: authentication successful for lab
00:34:04: SSH2 1: input: packet len 64
00:34:04: SSH2 1: partial packet 16, need 48, maclen 16
00:34:04: SSH2 1: MAC #6 ok
00:34:04: SSH2 1: input: padlen 6
00:34:04: SSH2 1: received packet type 2
00:34:04: SSH2 1: ssh_receive: 64 bytes received
00:34:04: SSH2 1: input: packet len 48
00:34:04: SSH2 1: partial packet 16, need 32, maclen 16
00:34:04: SSH2 1: MAC #7 ok
00:34:04: SSH2 1: input: padlen 19
00:34:04: SSH2 1: received packet type 90
00:34:04: SSH2 1: channel open request
00:34:04: SSH2 1: send: len 32 (includes padlen 10)
00:34:04: SSH2 1: done calc MAC out #6
00:34:04: SSH2 1: ssh_receive: 192 bytes received
00:34:04: SSH2 1: input: packet len 64
00:34:04: SSH2 1: partial packet 16, need 48, maclen 16
00:34:04: SSH2 1: MAC #8 ok
00:34:04: SSH2 1: input: padlen 13
00:34:04: SSH2 1: received packet type 98
00:34:04: SSH2 1: pty-req request
00:34:04: SSH2 1: setting TTY - requested: height 24, width 80; set: height 24,
width 80
00:34:04: SSH2 1: input: packet len 96
00:34:04: SSH2 1: partial packet 16, need 80, maclen 16
```

```
00:34:04: SSH2 1: MAC #9 ok
00:34:04: SSH2 1: input: padlen 11
00:34:04: SSH2 1: received packet type 98
00:34:04: SSH2 1: x11-req request
00:34:04: SSH2 1: ssh_receive: 48 bytes received
00:34:04: SSH2 1: input: packet len 32
00:34:04: SSH2 1: partial packet 16, need 16, maclen 16
00:34:04: SSH2 1: MAC #10 ok
00:34:04: SSH2 1: input: padlen 12
00:34:04: SSH2 1: received packet type 98
00:34:04: SSH2 1: shell request
00:34:04: SSH2 1: shell message received
00:34:04: SSH2 1: starting shell for vty
00:34:04: SSH2 1: send: len 48 (includes padlen 18)
00:34:04: SSH2 1: done calc MAC out #7
00:34:07: SSH2 1: ssh_receive: 48 bytes received
00:34:07: SSH2 1: input: packet len 32
00:34:07: SSH2 1: partial packet 16, need 16, maclen 16
00:34:07: SSH2 1: MAC #11 ok
00:34:07: SSH2 1: input: padlen 17
00:34:07: SSH2 1: received packet type 94
00:34:07: SSH2 1: send: len 32 (includes padlen 17)
00:34:07: SSH2 1: done calc MAC out #8
00:34:07: SSH2 1: ssh_receive: 48 bytes received
00:34:07: SSH2 1: input: packet len 32
00:34:07: SSH2 1: partial packet 16, need 16, maclen 16
00:34:07: SSH2 1: MAC #12 ok
00:34:07: SSH2 1: input: padlen 17
00:34:07: SSH2 1: received packet type 94
00:34:07: SSH2 1: send: len 32 (includes padlen 17)
00:34:07: SSH2 1: done calc MAC out #9
00:34:07: SSH2 1: ssh_receive: 48 bytes received
00:34:07: SSH2 1: input: packet len 32
00:34:07: SSH2 1: partial packet 16, need 16, maclen 16
00:34:07: SSH2 1: MAC #13 ok
00:34:07: SSH2 1: input: padlen 17
00:34:07: SSH2 1: received packet type 94
00:34:07: SSH2 1: send: len 32 (includes padlen 17)
00:34:07: SSH2 1: done calc MAC out #10
00:34:08: SSH2 1: ssh_receive: 48 bytes received
00:34:08: SSH2 1: input: packet len 32
00:34:08: SSH2 1: partial packet 16, need 16, maclen 16
00:34:08: SSH2 1: MAC #14 ok
00:34:08: SSH2 1: input: padlen 17
00:34:08: SSH2 1: received packet type 94
00:34:08: SSH2 1: send: len 32 (includes padlen 17)
00:34:08: SSH2 1: done calc MAC out #11
00:34:08: SSH2 1: ssh_receive: 48 bytes received
00:34:08: SSH2 1: input: packet len 32
00:34:08: SSH2 1: partial packet 16, need 16, maclen 16
00:34:08: SSH2 1: MAC #15 ok
00:34:08: SSH2 1: input: padlen 17
00:34:08: SSH2 1: received packet type 94
00:34:08: SSH2 1: send: len 32 (includes padlen 16)
00:34:08: SSH2 1: done calc MAC out #12
00:34:08: SSH2 1: send: len 48 (includes padlen 18)
00:34:08: SSH2 1: done calc MAC out #13
00:34:08: SSH2 1: send: len 16 (includes padlen 6)
00:34:08: SSH2 1: done calc MAC out #14
00:34:08: SSH2 1: send: len 16 (includes padlen 6)
00:34:08: SSH2 1: done calc MAC out #15
00:34:08: SSH1: Session terminated normally
```



# Configuration Examples for Secure Shell Version 2 Support

This section provides the following configuration examples:

- [Configuring Secure Shell Version 1: Example, page 13](#)
- [Configuring Secure Shell Version 2: Example, page 13](#)
- [Configuring Secure Shell Versions 1 and 2: Example, page 13](#)
- [Starting an Encrypted Session with a Remote Device: Example, page 13](#)
- [Setting an SNMP Trap: Example, page 13](#)
- [SSH Keyboard Interactive Authentication: Examples, page 14](#)
- [SNMP Debugging: Example, page 16](#)
- [SSH Debugging Enhancements: Examples, page 16](#)

## Configuring Secure Shell Version 1: Example

```
Router# configure terminal
Router (config)# ip ssh version 1
c7200-25-2013(config)# end
```

## Configuring Secure Shell Version 2: Example

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ssh version 2
Router(config)# end
```

## Configuring Secure Shell Versions 1 and 2: Example

```
Router# configure terminal
Router (config)# no ip ssh version
Router (config)# end
```

## Starting an Encrypted Session with a Remote Device: Example

```
Router# ssh -v 2 -c aes256-cbc -m hmac-sha1-160 -l shaship 10.76.82.24
```

## Setting an SNMP Trap: Example

The following shows that an SNMP trap has been set. The trap notification is generated automatically when the SSH session terminates. For an example of SNMP trap debug output, see the section [“SNMP Debugging: Example.”](#)

```
snmp-server
snmp-server host a.b.c.d public tty
```

Where a.b.c.d is the IP address of the SSH client.

## SSH Keyboard Interactive Authentication: Examples

The following are examples of various scenarios in which the SSH Keyboard Interactive Authentication feature has been automatically deployed:

### Client-Side Debugs

In the following example, client-side debugs are turned on and the maximum number of prompts = six, (three each for the SSH Keyboard Interactive Authentication method and for the password method of authentication).

```
Password:
Password:
Password:
Password:
Password:
Password: cisco123
Last login: Tue Dec 6 13:15:21 2005 from 10.76.248.213
user1@courier:~> exit
logout
[Connection to 10.76.248.200 closed by foreign host]
```

```
Router1# debug ip ssh client
```

```
SSH Client debugging is on
```

```
Router1# ssh -l lab 10.1.1.3
Password:
*Nov 17 12:50:53.199: SSH0: sent protocol version id SSH-1.99-Cisco-1.25
*Nov 17 12:50:53.199: SSH CLIENT0: protocol version id is - SSH-1.99-Cisco-1.25
*Nov 17 12:50:53.199: SSH CLIENT0: sent protocol version id SSH-1.99-Cisco-1.25
*Nov 17 12:50:53.199: SSH CLIENT0: protocol version exchange successful
*Nov 17 12:50:53.203: SSH0: protocol version id is - SSH-1.99-Cisco-1.25
*Nov 17 12:50:53.335: SSH CLIENT0: key exchange successful and encryption on
*Nov 17 12:50:53.335: SSH2 CLIENT 0: using method keyboard-interactive
Password:
Password:
Password:
*Nov 17 12:51:01.887: SSH2 CLIENT 0: using method password authentication
Password:
Password: lab
```

```
Router2>
*Nov 17 12:51:11.407: SSH2 CLIENT 0: SSH2_MSG_USERAUTH_SUCCESS message received
*Nov 17 12:51:11.407: SSH CLIENT0: user authenticated
*Nov 17 12:51:11.407: SSH2 CLIENT 0: pty-req request sent
*Nov 17 12:51:11.411: SSH2 CLIENT 0: shell request sent
*Nov 17 12:51:11.411: SSH CLIENT0: session open
```

### TACACS+ ACS Is the Backend AAA Server, ChPass Is Enabled, and a Blank Password Change Is Made

In the following example, a TACACS+ access control server (ACS) is the backend Accounting, Authentication, and Authorization (AAA) server; the ChPass feature is enabled; and a blank password change is accomplished using the SSH Keyboard Interactive Authentication method:

```
Router1# ssh -l cisco 10.1.1.3
Password:
Old Password: cisco
New Password: cisco123
Re-enter New password: cisco123

Router2> exit
[Connection to 10.1.1.3 closed by foreign host]
```

**TACACS+ ACS Is the Backend AAA Server, ChPass Is Enabled, and the Password Is Changed on First Login**

In the following example, a TACACS+ ACS is the backend server, and the ChPass feature is enabled. The password is changed on the first login using the SSH Keyboard Interactive Authentication method:

```
Router1# ssh -l cisco 10.1.1.3
Password: cisco
Your password has expired.
Enter a new one now.
New Password: cisco123
Re-enter New password: cisco123

Router2> exit
[Connection to 10.1.1.3 closed by foreign host]
```

```
Router1# ssh -l cisco 10.1.1.3
Password:cisco1
Your password has expired.
Enter a new one now.
New Password: cisco
Re-enter New password: cisco12
The New and Re-entered passwords have to be the same.
Try again.
New Password: cisco
Re-enter New password: cisco

Router2>
```

**TACACS+ ACS Is the Backend AAA Server, ChPass Is Enabled, and the Password Expires After Three Logins**

In the following example, a TACACS+ ACS is the backend AAA server, and the ChPass feature is enabled. The password expires after three logins using the SSH Keyboard Interactive Authentication method:

```
Router# ssh -l cisco. 10.1.1.3
Password: cisco

Router2> exit
[Connection to 10.1.1.3 closed by foreign host]

Router1# ssh -l cisco 10.1.1.3
Password: cisco

Router2> exit

Router1# ssh -l cisco 10.1.1.3
Password: cisco

Router2> exit
[Connection to 10.1.1.3 closed by foreign host]

Router1# ssh -l cisco 10.1.1.3
Password: cisco
Your password has expired.
Enter a new one now.
New Password: cisco123
Re-enter New password: cisco123

Router2>
```

## SNMP Debugging: Example

The following is sample output using the **debug snmp packet** command. The output provides SNMP trap information for an SSH session.

```
Router1# debug snmp packet

SNMP packet debugging is on

Router1# ssh -l lab 10.0.0.2

Password:

Router2# exit

[Connection to 10.0.0.2 closed by foreign host]
Router1#
*Jul 18 10:18:42.619: SNMP: Queuing packet to 10.0.0.2
*Jul 18 10:18:42.619: SNMP: V1 Trap, ent cisco, addr 10.0.0.1, gentrap 6, spectrap 1
local.9.3.1.1.2.1 = 6
tcpConnEntry.1.10.0.0.1.22.10.0.0.2.55246 = 4
ltcpConnEntry.5.10.0.0.1.22.10.0.0.2.55246 = 1015
ltcpConnEntry.1.10.0.0.1.22.10.0.0.2.55246 = 1056
ltcpConnEntry.2.10.0.0.1.22.10.0.0.2.55246 = 1392
local.9.2.1.18.2 = lab
*Jul 18 10:18:42.879: SNMP: Packet sent via UDP to 10.0.0.2
Router1#
```

## SSH Debugging Enhancements: Examples

The following is sample output from the **debug ip ssh detail** command. The output provides debugging information regarding the SSH protocol and channel requests.

```
Router# debug ip ssh detail

00:04:22: SSH0: starting SSH control process
00:04:22: SSH0: sent protocol version id SSH-1.99-Cisco-1.25
00:04:22: SSH0: protocol version id is - SSH-1.99-Cisco-1.25
00:04:22: SSH2 0: SSH2_MSG_KEXINIT sent
00:04:22: SSH2 0: SSH2_MSG_KEXINIT received
00:04:22: SSH2:kex: client->server enc:aes128-cbc mac:hmac-sha1
00:04:22: SSH2:kex: server->client enc:aes128-cbc mac:hmac-sha1
00:04:22: SSH2 0: expecting SSH2_MSG_KEXDH_INIT
00:04:22: SSH2 0: SSH2_MSG_KEXDH_INIT received
00:04:22: SSH2: kex_derive_keys complete
00:04:22: SSH2 0: SSH2_MSG_NEWKEYS sent
00:04:22: SSH2 0: waiting for SSH2_MSG_NEWKEYS
00:04:22: SSH2 0: SSH2_MSG_NEWKEYS received
00:04:24: SSH2 0: authentication successful for lab
00:04:24: SSH2 0: channel open request
00:04:24: SSH2 0: pty-req request
00:04:24: SSH2 0: setting TTY - requested: height 24, width 80; set: height 24, width 80
00:04:24: SSH2 0: shell request
00:04:24: SSH2 0: shell message received
00:04:24: SSH2 0: starting shell for vty
00:04:38: SSH0: Session terminated normally
```

The following is sample output from the **debug ip ssh packet** command. The output provides debugging information regarding the ssh packet.

```
Router# debug ip ssh packet
```

```
00:05:43: SSH2 0: send:packet of length 280 (length also includes padlen of 4)
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: input: total packet length of 280 bytes
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 272 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 272 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 272 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 272 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 24 bytes received
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 272 bytes, maclen 0
00:05:43: SSH2 0: input: padlength 4 bytes
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: input: total packet length of 144 bytes
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 136 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 136 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 16 bytes received
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 136 bytes, maclen 0
00:05:43: SSH2 0: input: padlength 6 bytes
00:05:43: SSH2 0: signature length 143
00:05:43: SSH2 0: send:packet of length 448 (length also includes padlen of 7)
00:05:43: SSH2 0: send:packet of length 16 (length also includes padlen of 10)
00:05:43: SSH2 0: newkeys: mode 1
00:05:43: SSH2 0: ssh_receive: 16 bytes received
00:05:43: SSH2 0: input: total packet length of 16 bytes
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 8 bytes, maclen 0
00:05:43: SSH2 0: input: padlength 10 bytes
00:05:43: SSH2 0: newkeys: mode 0
00:05:43: SSH2 0: ssh_receive: 52 bytes received
00:05:43: SSH2 0: input: total packet length of 32 bytes
00:05:43: SSH2 0: partial packet length(block size)16 bytes,needed 16 bytes, maclen 20
00:05:43: SSH2 0: MAC compared for #3 :ok
```

## Where to Go Next

You have to use a SSH remote device that supports SSH Version 2, and you have to connect to a Cisco IOS router.

## Additional References

The following sections provide references related to Secure Shell Version 2.

## Related Documents

Related Topic	Document Title
AAA	“ <a href="#">Authentication, Authorization, and Accounting (AAA)</a> ” section of the <i>Cisco IOS Security Configuration Guide</i>
Configuring a host name and host domain	“ <a href="#">Configuring Secure Shell</a> ” chapter in the <i>Cisco IOS Security Configuration Guide</i>

Related Topic	Document Title
Configuring Secure Shell	<a href="#">“Configuring Secure Shell”</a> chapter of the <i>Cisco IOS Security Configuration Guide</i>
Debugging commands	<i>Cisco IOS Debug Command Reference</i> , Release 12.4T
Downloading a Cisco software image	<i>Cisco IOS Configuration Fundamentals and Network Management Configuration Guide</i>
IOS configuration fundamentals	<i>Cisco IOS Configuration Fundamentals and Network Management Configuration Guide</i> and <i>Cisco IOS Configuration Fundamentals and Network Management Command Reference</i>
IPSec	“IP Security and Encryption” section of the <i>Cisco IOS Security Configuration Guide</i>
Security commands	<i>Cisco IOS Security Command Reference</i> , Release 12.4 T
SNMP, configuring traps	“Configuring SNMP Support” chapter in <i>Cisco IOS Network Management Configuration Guide</i>

## Standards

Standards	Title
Internet Engineering Task Force (IETF) Secure Shell Version 2 Draft Standards	<a href="#">Internet Engineering Task Force website</a>

## MIBs

MIBs	MIBs Link
•	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	—

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

- **debug ip ssh**
- **ip ssh min dh size**
- **ip ssh rsa keypair-name**
- **ip ssh version**
- **ssh**

# Feature Information for Secure Shell Version 2 Support

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for Secure Shell Version 2 Support

Feature Name	Releases	Feature Information
Secure Shell Version 2 Support	12.3(4)T 12.2(25)S	The Secure Shell Version 2 Support feature allows you to configure Secure Shell (SSH) Version 2 (SSH Version 1 support was implemented in an earlier Cisco IOS software release). SSH runs on top of a reliable transport layer and provides strong authentication and encryption capabilities.
Secure Shell Version 2 Client and Server Support	12.3(7)JA 12.0(32)SY	This feature was integrated into Cisco IOS Release 12.3(7)JA.
Secure Shell Version 2 Client and Server Support	12.4(17)	The Cisco IOS image was updated to provide for the automatic generation of SNMP traps when an SSH session terminates.  For information about this feature, see the following section: <ul style="list-style-type: none"> <li>• “SNMP Trap Generation” section on page 3</li> <li>• “SNMP Debugging: Example” section on page 16</li> </ul>
SSH Keyboard Interactive Authentication	12.4(18) 12.2(33)SXH3	This feature, also known as Generic Message Authentication for SSH, is a method that can be used to implement different types of authentication mechanisms. Basically, any currently supported authentication method that requires only user input can be performed with this feature.  For information about this feature see the following sections: <ul style="list-style-type: none"> <li>• “SSH Keyboard Interactive Authentication” section on page 4</li> <li>• “SSH Keyboard Interactive Authentication: Examples” section on page 14</li> </ul>



**Table 1**      **Feature Information for Secure Shell Version 2 Support (continued)**

Feature Name	Releases	Feature Information
Secure Shell SSH Version 2 Client Support	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
Secure Shell Version 2 Enhancements	12.4(20)T	<p>The Secure Shell Version 2 Enhancements include a number of additional capabilities such as support for VRF aware SSH, SSH debug enhancements and Diffie-Hellman group 14 and group 16 exchange support.</p> <p>For information about this feature see the following sections:</p> <ul style="list-style-type: none"> <li>• <a href="#">“Secure Shell Version 2 Enhancements” section on page 3</a></li> </ul>

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2003 – 2008 Cisco Systems, Inc. All rights reserved.





# SSH Terminal-Line Access

---

This feature module describes the SSH Terminal-Line Access feature and includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 2](#)
- [Supported Standards, MIBs, and RFCs, page 4](#)
- [Prerequisites, page 4](#)
- [Configuration Tasks, page 4](#)
- [Configuration Examples, page 5](#)
- [Command Reference, page 7](#)

## Feature Overview

Cisco IOS supports reverse Telnet, which allows users to Telnet through the router—via a certain port range—to connect them to tty (asynchronous) lines. Reverse Telnet has allowed users to connect to the console ports of remote devices that do not natively support Telnet. However, this method has provided very little security because all Telnet traffic goes over the network in the clear. The SSH Terminal-Line Access feature replaces reverse Telnet with secure shell (SSH). This feature may be configured to use encryption to access devices on the tty lines, which provide users with connections that support strong privacy and session integrity.

SSH is an application and a protocol that provide secure replacement for the suite of Berkeley r-tools such as rsh, rlogin and rcp. (Cisco IOS supports rlogin.) The protocol secures the sessions using standard cryptographic mechanisms, and the application can be used similarly to the Berkeley rexec and rsh tools. There are currently two versions of SSH available: SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in the Cisco IOS software.

The SSH Terminal-Line Access feature enables users to configure their router with secure access and perform the following tasks:

- Connect to a router that has multiple terminal lines connected to consoles or serial ports of other routers, switches, or devices.



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

- Simplify connectivity to a router from anywhere by securely connecting to the terminal server on a specific line.
- Allow modems attached to routers to be used for dial-out securely.
- Require authentication to each of the lines through a locally defined username and password, TACACS+, or RADIUS.

## Benefits

The SSH Terminal-Line Access feature provides users secure access to tty lines.

## Restrictions

### Console Server Requirement

To configure secure console server access, you must define each line in its own rotary and configure SSH to use SSH over the network when users wish to access each of those devices.

### Memory and Performance Impact

Replacing reverse Telnet with SSH may reduce the performance of available tty lines due to the addition of encryption and decryption processing above the vty processing. (Any cryptographic mechanism uses more memory than a regular access.)

## Related Documents

The following documents provide information related to the SSH Terminal-Line Access feature:

- Cisco IOS Dial Technologies Configuration Guide, Release 12.2
- *Cisco IOS Dial Technologies Command Reference*, Release 12.2
- *Cisco IOS Security Command Reference*, Release 12.2
- *Cisco IOS Security Configuration Guide*, Release 12.2

For more information on SSH, such as the details of the protocol, go to the SSH website at <http://www.ssh.com/>.

## Supported Platforms

This feature is supported on the following platforms:

- Cisco 1700 Series
- Cisco 2600 Series
- Cisco 3620
- Cisco 3640
- Cisco 3660
- Cisco 4500
- Cisco 12000 Series

This feature is supported on all platforms that support SSH.

# Supported Standards, MIBs, and RFCs

## Standards

No new or modified standards are supported by this feature.

## MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

## RFCs

No new or modified RFCs are supported by this feature.

## Prerequisites

Download the required image on your router. The SSH server requires you to have an IPsec (DES or 3DES) encryption software image from Cisco IOS Release 12.1(1)T downloaded on your router; the SSH client requires you to have an IPsec (DES or 3DES) encryption software image from Cisco IOS Release 12.1(3)T downloaded on your router. For more information on downloading a software image, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2.

The SSH server requires the use of a username and password, which must be defined through the use of a local username and password, TACACS+, or RADIUS.

**Note**

---

The SSH Terminal-Line Access feature is available on any image that contains SSH.

---

## Configuration Tasks

See the following section for configuration tasks for the SSH Terminal-Line Access feature:

- [Configuring SSH Terminal-Line Access](#)

## Configuring SSH Terminal-Line Access

**Note**

---

SSH must already be configured on the router.

---

To configure a Cisco router to support reverse secure Telnet, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>line</b> <i>line-number</i> [ <i>ending-line-number</i> ]	Identifies a line for configuration and enters line configuration mode.  <b>Note</b> For router console configurations, each line must be defined in its own rotary, and SSH must be configured to listen in on each rotary.  <b>Note</b> An authentication method requiring a username and password must be configured for each line. This may be done through the use of a local username and password stored on the router, through the use of TACACS+, or through the use of RADIUS. Neither Line passwords nor the enable password are sufficient to be used with SSH.
Step 2	Router(config-line)# <b>no exec</b>	Disables exec processing on each of the lines.
Step 3	Router(config-line)# <b>login</b> { <b>local</b>   <b>authentication</b> <i>listname</i> }	Defines a login authentication mechanism for the lines.  <b>Note</b> The authentication method must utilize a username and password.
Step 4	Router(config-line)# <b>rotary</b> <i>group</i>	Defines a group of lines consisting of one or more lines.  <b>Note</b> All rotaries used must be defined, and each defined rotary must be used when SSH is enabled.
Step 5	Router(config-line)# <b>transport input</b> { <b>all</b>   <b>ssh</b> }	Defines which protocols to use to connect to a specific line of the router.
Step 6	Router(config-line)# <b>exit</b>	Exits line configuration mode.
Step 7	Router(config)# <b>ip ssh port</b> <i>portnum</i> <b>rotary</b> <i>group</i>	Enables secure network access to the tty lines. Use this command to connect the <i>portnum</i> argument with the <i>rotary group</i> argument, which is associated with a line or group of lines.  <b>Note</b> The <i>group</i> argument must correspond with the <b>rotary group</b> number chosen in Step 4.

## Verifying SSH Terminal-Line Access

To verify that this functionality is working, you can connect to a router using an SSH client.

## Configuration Examples

This section provides the following configuration examples:

- [SSH Terminal-Line Access Configuration Example](#)
- [SSH Terminal-Line Access for a Console \(Serial Line\) Ports Configuration Example](#)

## SSH Terminal-Line Access Configuration Example

The following example shows how to configure the SSH Terminal-Line Access feature on a modem used for dial-out on lines 1 through 200. To get any of the dial-out modems, use any SSH client and start a SSH session to port 2000 of the router to get to the next available modem from the rotary.

```
line 1 200
 no exec
 login authentication default
 rotary 1
 transport input ssh
 exit
ip ssh port 2000 rotary 1
```

## SSH Terminal-Line Access for a Console (Serial Line) Ports Configuration Example

The following example shows how to configure the SSH Terminal-Line Access feature to access the console or serial line interface of various devices. For this type of access, each line is put into its own rotary, and each rotary is used for a single port. In this example, lines 1 through 3 are used; the port (line) mappings of the configuration are shown in [Table 68](#).

**Table 68** Port (line) Configuration Mappings

Line Number	SSH Port Number
1	2001
2	2002
3	2003

```
line 1
 no exec
 login authentication default
 rotary 1
 transport input ssh
line 2
 no exec
 login authentication default
 rotary 2
 transport input ssh
line 3
 no exec
 login authentication default
 rotary 3
 transport input ssh

ip ssh port 2001 rotary 1 3
```



# Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **ip ssh port**

---

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





## **802.1X Authentication Services**





# Configuring IEEE 802.1x Port-Based Authentication

---

**First Published: December 7, 2006**

**Last Updated: January 8, 2007**

This document describes how to configure IEEE 802.1x port-based authentication on Cisco integrated services routers (ISRs). IEEE 802.1x authentication prevents unauthorized devices (supplicants) from gaining access to the network.

Cisco ISRs can combine the functions of a router, a switch, and an access point, depending on the fixed configuration or installed modules. The switch functions are provided by either built in switch ports or a plug-in module with switch ports.



## Note

---

This document describes IEEE 802.1x security features available only on the switch ports in a Cisco ISR.

---

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Configuring IEEE 802.1x Port-Based Authentication](#)” section on [page 24](#).

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for Configuring IEEE 802.1x Port-Based Authentication, page 2](#)
- [Restrictions for Configuring IEEE 802.1x Port-Based Authentication, page 3](#)
- [Information About IEEE 802.1x Port-Based Authentication, page 4](#)
- [How to Use IEEE 802.1x Authentication With Other Features, page 12](#)



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

- [Configuration Examples for IEEE 802.1x Features, page 18](#)
- [Additional References, page 22](#)
- [Command Reference, page 23](#)
- [Feature Information for Configuring IEEE 802.1x Port-Based Authentication, page 24](#)
- [Glossary, page 29](#)

## Prerequisites for Configuring IEEE 802.1x Port-Based Authentication

The features described in this document are available only on switch ports installed in Cisco ISR routers. The IEEE 802.1x port-based authentication features are available in Cisco IOS Release 12.4(11)T on Cisco 800, 870, 1800, 2800, and 3800 series ISRs that support switch ports.

The fixed configuration Cisco 1800 series router platforms and the Cisco 870 series routers have integrated 4-port and 8-port switches.

The following cards or modules support switch ports:

- High-speed WAN interface cards (HWIC)
  - HWIC-4ESW
  - HWICD-9ESW
- EtherSwitch Network Modules
  - NM-16ESW
  - NMD-36ESW

**Note**

Not all Cisco ISR routers support all the components listed. For information about module compatibility with a specific router platform, see [Cisco EtherSwitch Modules Comparison](#).

To determine whether your router has switch ports that can be configured with the IEEE 802.1x port-based authentication feature, use the **show interfaces switchport** command.

To configure IEEE 802.1x port-based authentication, you must enable authentication, authorization, and accounting (AAA) and specify the authentication method list. A method list describes the sequence and authentication method to be queried to authenticate a user.

# Restrictions for Configuring IEEE 802.1x Port-Based Authentication

These sections describe the configuration restrictions for these features:

- [IEEE 802.1x Authentication Configuration, page 3](#)
- [VLAN Assignment Configuration, page 4](#)
- [Guest VLAN Configuration, page 4](#)
- [Upgrading from a Previous Software Release, page 4](#)

## IEEE 802.1x Authentication Configuration

These are the IEEE 802.1x authentication configuration restrictions:

- When IEEE 802.1x authentication is enabled, ports are authenticated before any other Layer 2 or Layer 3 features are enabled.
- If you try to change the mode (for example, from access to trunk) of an IEEE 802.1x-enabled port, an error message appears, and the port mode is not changed.
- If the VLAN to which an IEEE 802.1x-enabled port is assigned changes, this change is transparent and does not affect the switch port. For example, this change occurs if a port is assigned to a RADIUS server-assigned VLAN and is then assigned to a different VLAN after reauthentication.

If the VLAN to which an IEEE 802.1x port is assigned is shut down, disabled, or removed, the port becomes unauthorized. For example, the port is unauthorized after the access VLAN to which a port is assigned shuts down or is removed.

- The IEEE 802.1x protocol is supported on Layer 2 static-access ports, voice VLAN enabled ports, and Layer 3 routed ports, but it is not supported on these port types:
  - Dynamic-access ports—If you try to enable IEEE 802.1x authentication on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and IEEE 802.1x authentication is not enabled. If you try to change an IEEE 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.
  - Dynamic ports—If you try to enable IEEE 802.1x authentication on a dynamic port, an error message appears, and IEEE 802.1x authentication is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to dynamic, an error message appears, and the port mode is not changed.
  - Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) destination ports—You can enable IEEE 802.1x authentication on a port that is a SPAN or RSPAN destination port. However, IEEE 802.1x authentication is disabled until the port is removed as a SPAN or RSPAN destination port. You can enable IEEE 802.1x authentication on a SPAN or RSPAN source port.
  - Trunk port—If you try to enable IEEE 802.1x authentication on a trunk port, an error message appears, and IEEE 802.1x authentication is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to trunk, an error message appears, and the port mode is not changed.



### Note

A port in dynamic mode can negotiate with its neighbor to become a trunk port.

## VLAN Assignment Configuration

This is the restriction for configuring VLAN assignment and the guest VLAN feature on switch ports in an ISR router:

- When IEEE 802.1x authentication is enabled on a port, you cannot configure a port VLAN that is equal to a voice VLAN.

## Guest VLAN Configuration

- You can configure any VLAN except an RSPAN VLAN or a voice VLAN as an IEEE 802.1x guest VLAN. The guest VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.
- After you configure a guest VLAN for an IEEE 802.1x port to which a DHCP client is connected, you might have to get a host IP address from a DHCP server. You can change the settings for restarting the IEEE 802.1x authentication process on the switch before the DHCP process on the client times out and tries to get a host IP address from the DHCP server. Decrease the settings for the IEEE 802.1x authentication process (using the **dot1x max-reauth-req** and **dot1x timeout tx-period** interface configuration commands). The amount of decrease depends on the connected IEEE 802.1x client type.

## Upgrading from a Previous Software Release

In Cisco IOS Release 12.4(11)T, the implementation for IEEE 802.1x authentication changed from the previous releases. When IEEE 802.1x authentication is enabled, information about Port Fast is no longer added to the configuration.



### Note

When you enter any IEEE 802.1x-related commands on a port, this information is automatically added to the running configuration to address any backward compatibility issues:

```
dot1xpae authenticator
```

## Information About IEEE 802.1x Port-Based Authentication



### Note

This section describes IEEE 802.1x security features available only on the switch ports in a Cisco ISR.

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that prevents unauthorized clients from connecting to a LAN through publicly accessible ports unless they are properly authenticated. The authentication server authenticates each client connected to a port before making available any services offered by the device or the network.

Until the client is authenticated, IEEE 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.



These sections describe IEEE 802.1x port-based authentication:

- [IEEE 802.1x Authenticator, page 5](#)
- [IEEE 802.1x with RADIUS Accounting, page 9](#)

## IEEE 802.1x Authenticator

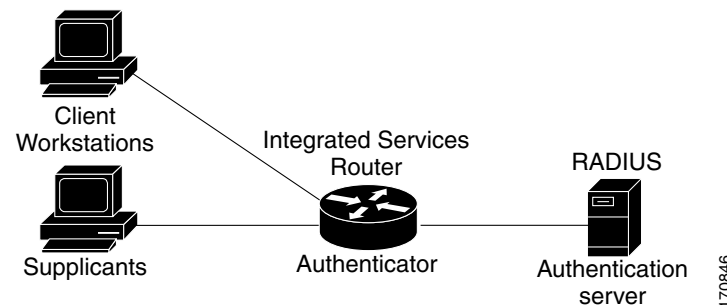
The following sections describe the basic authentication process:

- [Device Roles, page 5](#)
- [Authentication Initiation and Message Exchange, page 6](#)
- [Authentication Process, page 7](#)
- [Ports in Authorized and Unauthorized States, page 8](#)
- [IEEE 802.1x Host Mode, page 9](#)

## Device Roles

With IEEE 802.1x port-based authentication, the devices in the network have specific roles as shown in [Figure 1](#).

**Figure 1** IEEE 802.1x Device Roles



- *Supplicant*—Device (workstation) that requests access to the LAN and switch services and responds to requests from the router. The workstation must be running IEEE 802.1x-compliant client software such as that offered in the Microsoft Windows XP operating system. (The *supplicant* is sometimes called the client.)



### Note

To resolve Windows XP network connectivity and IEEE 802.1x authentication issues, read the Microsoft Knowledge Base article at this URL:

<http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP>

- *Authentication server*—Device that performs the actual authentication of the supplicant. The authentication server validates the identity of the supplicant and notifies the router whether or not the supplicant is authorized to access the LAN and switch services. The Network Access Device (or ISR router in this instance) transparently passes the authentication messages between the supplicant and the authentication server, and the authentication process is carried out between the supplicant and the authentication server. The particular EAP method used will be decided between the supplicant and the authentication server (RADIUS server). The RADIUS security system with EAP

extensions is available in Cisco Secure Access Control Server Version 3.0 or later. RADIUS operates in a client and server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

- *Authenticator (integrated services router (ISR) or wireless access point)*—Router that controls the physical access to the network based on the authentication status of the supplicant. The router acts as an intermediary between the supplicant and the authentication server, requesting identity information from the supplicant, verifying that information with the authentication server, and relaying a response to the supplicant. The router includes the RADIUS client, which is responsible for encapsulating and decapsulating the EAP frames and interacting with the authentication server.

When the authenticator receives EAPOL frames and relays them to the authentication server, the EAPOL is stripped and the remaining EAP frame is reencapsulated in the RADIUS format. The EAP frames are not modified during encapsulation, and the authentication server must support EAP within the native frame format. When the authenticator receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

## Authentication Initiation and Message Exchange

During IEEE 802.1x authentication, the router or the supplicant can initiate authentication. If you enable authentication on a port by using the **dot1x port-control auto** interface configuration command, the router initiates authentication when the link state changes from down to up or periodically if the port remains up and unauthenticated. The router sends an EAP-request/identity frame to the supplicant to request its identity. Upon receipt of the frame, the supplicant responds with an EAP-response/identity frame.

However, if during bootup, the supplicant does not receive an EAP-request/identity frame from the router, the supplicant can initiate authentication by sending an EAPOL-start frame, which prompts the router to request the supplicant's identity.

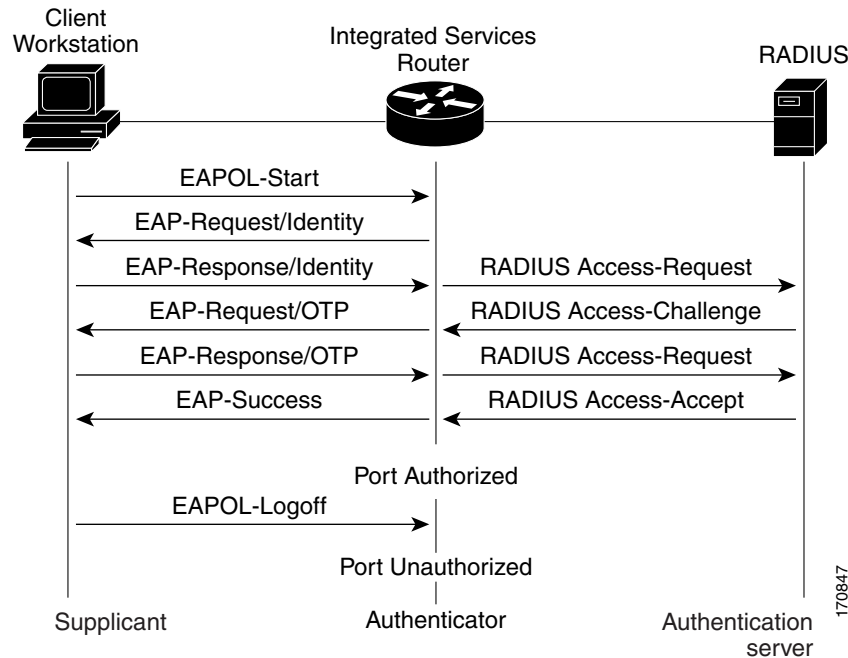


### Note

If IEEE 802.1x authentication is not enabled or supported on the network access device, any EAPOL frames from the supplicant are dropped. If the supplicant does not receive an EAP-request/identity frame after three attempts to start authentication, the supplicant sends frames as if the port is in the authorized state. A port in the authorized state effectively means that the supplicant has been successfully authenticated. For more information, see the [“Ports in Authorized and Unauthorized States” section on page 8](#).

When the supplicant supplies its identity, the router begins its role as the intermediary, passing EAP frames between the supplicant and the authentication server until authentication succeeds or fails. If the authentication succeeds, the router port becomes authorized. If the authentication fails, authentication can be retried, the port might be assigned to a VLAN that provides limited services, or network access is not granted. For more information, see the [“Ports in Authorized and Unauthorized States” section on page 8](#).

The specific exchange of EAP frames depends on the authentication method being used. [Figure 2](#) shows a message exchange initiated by the supplicant using the One-Time-Password (OTP) authentication method with a RADIUS server.

**Figure 2**      **Message Exchange**

## Authentication Process

To configure IEEE 802.1x port-based authentication, you must enable authentication, authorization, and accounting (AAA) and specify the authentication method list. A method list describes the sequence and authentication method to be queried to authenticate a user.

The AAA process begins with authentication. When IEEE 802.1x port-based authentication is enabled and the device attempting to authenticate is IEEE 802.1x-capable (meaning it supports the supplicant functionality) these events occur:

- If the supplicant identity is valid and the IEEE 802.1x authentication succeeds, the router grants the supplicant access to the network.

The router reauthenticates a supplicant when one of these situations occurs:

- Periodic reauthentication is enabled, and the reauthentication timer expires.

You can configure the reauthentication timer to use a router-specific value or to be based on values from the RADIUS server.

After IEEE 802.1x authentication using a RADIUS server is configured, the router uses timers based on the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute [29]).

The Session-Timeout RADIUS attribute (Attribute[27]) specifies the time after which reauthentication occurs.

The Termination-Action RADIUS attribute (Attribute [29]) specifies the action to take during reauthentication. The actions can be *Initialize* or *ReAuthenticate*. When the *Initialize* action is set (the attribute value is *DEFAULT*), the IEEE 802.1x session ends, and connectivity is lost during reauthentication. When the *ReAuthenticate* action is set (the attribute value is *RADIUS-Request*), the session is not affected during reauthentication.

- You manually reauthenticate the supplicant by entering the **dot1x re-authenticate interface interface-id** privileged EXEC command.

## Ports in Authorized and Unauthorized States

During IEEE 802.1x authentication, depending on the port state, the router can grant a supplicant access to the network. The port starts in the *unauthorized* state. While in this state, the port that is not configured as a voice VLAN port disallows all ingress traffic except for IEEE 802.1x authentication, CDP, and STP packets. When a supplicant is successfully authenticated, the port changes to the *authorized* state, allowing all traffic for the supplicant to flow normally. If the port is configured as a voice VLAN port, the port allows VoIP traffic and IEEE 802.1x protocol packets before the supplicant is successfully authenticated.

If a client that does not support IEEE 802.1x authentication connects to an unauthorized IEEE 802.1x port, the router requests the client's identity. In this situation, if the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an IEEE 802.1x-enabled supplicant connects to a port that is not running the IEEE 802.1x standard, the supplicant initiates the authentication process by sending the EAPOL-start frame. When no response is received, the supplicant sends the request for a fixed number of times. Because no response is received, the supplicant begins sending frames as if the port is in the authorized state.

You control the port authorization state by using the **dot1x port-control** interface configuration command and these keywords:

- **force-authorized**—Disables IEEE 802.1x authentication and causes the port to change to the authorized state without any authentication exchange required. The port sends and receives normal traffic without IEEE 802.1x-based authentication of the client. This is the default setting.
- **force-unauthorized**—Causes the port to remain in the unauthorized state, ignoring all attempts by the supplicant to authenticate. The router cannot provide authentication services to the supplicant through the port.
- **auto**—Enables IEEE 802.1x authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes from down to up or when an EAPOL-start frame is received. The router requests the identity of the supplicant and begins relaying authentication messages between the supplicant and the authentication server. Each supplicant attempting to access the network is uniquely identified by the router by using the supplicant MAC address.

If the supplicant is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated supplicant are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the router can resend the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

When a supplicant logs off, it sends an EAPOL-logoff message, causing the router port to change to the unauthorized state.

If the link state of a port changes from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

For information about configuring IEEE 802.1x port-based authentication, see the [“Configuring IEEE 802.1x Authentication”](#) section of the “Configuring IEEE 802.1x Port-Based Authentication” chapter in the *Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE*.

## IEEE 802.1x Host Mode

**Note**

This section describes IEEE 802.1x security features available only on the switch ports in a Cisco ISR.

You can configure an IEEE 802.1x port for single-host or for multi-host mode. In single-host mode (see [Figure 1 on page 5](#)), only one supplicant can be authenticated by the IEEE 802.1x-enabled switch port. The router detects the supplicant by sending an EAPOL frame when the port link state changes to the up state. If a supplicant leaves or is replaced with another supplicant, the router changes the port link state to down, and the port returns to the unauthorized state.

In multi-host mode, you can attach multiple hosts to a single IEEE 802.1x-enabled port. In this mode, only one of the attached supplicants must be authorized for all supplicants to be granted network access. If the port becomes unauthorized (reauthentication fails or an EAPOL-logoff message is received), the router denies network access to all of the attached supplicants.

**Note**

Cisco 870 series platforms do not support single-host mode.

For information about configuring IEEE 802.1x host mode, see the “[Configuring the Host Mode](#)” section of the “Configuring IEEE 802.1x Port-Based Authentication” chapter in the *Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE*.

## IEEE 802.1x with RADIUS Accounting

**Note**

This section describes IEEE 802.1x security features available only on the switch ports in a Cisco ISR.

This section describes IEEE 802.1x RADIUS accounting and includes the following topics:

- [IEEE 802.1x RADIUS Accounting, page 9](#)
- [IEEE 802.1x Accounting Attribute-Value Pairs, page 11](#)

## IEEE 802.1x RADIUS Accounting

**Note**

If you plan to implement system-wide accounting, you should also configure IEEE 802.1x accounting. Moreover, you need to inform the accounting server of the system reload event when the system is reloaded to ensure that the accounting server is aware that all outstanding IEEE 802.1x sessions on this system are closed.

**Note**

To enable IEEE 802.1x accounting, you must first configure IEEE 802.1x authentication and switch-to-RADIUS server communication.

IEEE 802.1x RADIUS accounting relays important events to the RADIUS server (such as the supplicant's connection session). This session is defined as the interval beginning when the supplicant is authorized to use the port and ending when the supplicant stops using the port.

**Note**

You must configure the IEEE 802.1x supplicant to send an EAP-logoff (Stop) message to the switch when the user logs off. If you do not configure the IEEE 802.1x supplicant, an EAP-logoff message is not sent to the switch and the accompanying accounting Stop message is not sent to the authentication server. See the Microsoft Knowledge Base article at the location: <http://support.microsoft.com>. Also see the Microsoft article at this location:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/cableguy/cg0703.asp>,

and set the SupplicantMode registry to 3 and the AuthMode registry to 1.

After the supplicant is authenticated, the switch sends accounting-request packets to the RADIUS server, which responds with accounting-response packets to acknowledge the receipt of the request.

A RADIUS accounting-request packet contains one or more Attribute-Value (AV) pairs to report various events and related information to the RADIUS server. The following events are tracked:

- User successfully authenticates.
- User logs off.
- Link-down occurs on an IEEE 802.1x port.
- Reauthentication succeeds.
- Reauthentication fails.

When the port state transitions between authorized and unauthorized, the RADIUS messages are transmitted to the RADIUS server.

The switch does not log any accounting information. Instead, it sends such information to the RADIUS server, which must be configured to log accounting messages.

This is the IEEE 802.1x RADIUS accounting process

1. A user connects to a port on the router.
2. Authentication is performed.
3. VLAN assignment is enabled, as appropriate, based on the RADIUS server configuration.
4. The router sends a start message to an accounting server.
5. Reauthentication is performed, as necessary.
6. The port sends an interim accounting update to the accounting server that is based on the result of reauthentication.
7. The user disconnects from the port.
8. The router sends a stop message to the accounting server.

The switch port does not log IEEE 802.1x accounting information. Instead, it sends this information to the RADIUS server, which must be configured to log accounting messages.

To configure IEEE 802.1x accounting, you need to do the following tasks:

- Enable accounting in your RADIUS server.
- Enable IEEE 802.1x accounting on your switch.
- Enable AAA accounting by using the **aaa system accounting** command.

Enabling AAA system accounting along with IEEE 802.1x accounting allows system reload events to be sent to the accounting RADIUS server for logging. When the accounting RADIUS server receives notice of a system reload event, the server can infer that all active IEEE 802.1x sessions are appropriately closed.

Because RADIUS uses the unreliable transport protocol User Datagram Protocol (UDP), accounting messages may be lost due to poor network conditions. If the switch does not receive the accounting response message from the RADIUS server after a configurable number of retransmissions of an accounting request, the following system message appears:

```
Accounting message %s for session %s failed to receive Accounting Response.
```

When the stop message is not transmitted successfully, a message like the following appears:

```
00:09:55: %RADIUS-3-NOACCOUNTINGRESPONSE: Accounting message Start for session
172.20.50.145 sam 11/06/03 07:01:16 11000002 failed to receive Accounting Response.
```

Use the **show radius statistics** command to display the number of RADIUS messages that do not receive the accounting response message.

For information about configuring IEEE 802.1x RADIUS accounting, see the [“Enabling 802.1X Accounting”](#) section of the “Configuring 802.1X Port-Based Authentication” chapter in the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(31)SGA*.

## IEEE 802.1x Accounting Attribute-Value Pairs

The information sent to the RADIUS server is represented in the form of AV pairs. These AV pairs provide data for different applications. (For example, a billing application might require information that is in the Acct-Input-Octets or the Acct-Output-Octets attributes of a RADIUS packet.)

AV pairs are automatically sent by a router that is configured for IEEE 802.1x accounting. Three types of RADIUS accounting packets are sent by a router:

- START—sent when a new user session starts
- INTERIM—sent during an existing session for updates
- STOP—sent when a session terminates

[Table 1](#) lists the AV pairs and when they are sent by the router:

**Table 1 Accounting AV Pairs**

Attribute Number	AV Pair Name	START	INTERIM	STOP
Attribute[1]	User-Name	Always	Always	Always
Attribute[4]	NAS-IP-Address	Always	Always	Always
Attribute[5]	NAS-Port	Always	Always	Always
Attribute[6]	Service-Type	Always	Always	Always
Attribute[8]	Framed-IP-Address	Never	Sometimes <sup>1</sup>	Sometimes <sup>1</sup>
Attribute[25]	Class	Always	Always	Always
Attribute[30]	Called-Station-ID	Always	Always	Always
Attribute[31]	Calling-Station-ID	Always	Always	Always
Attribute[40]	Acct-Status-Type	Always	Always	Always
Attribute[41]	Acct-Delay-Time	Always	Always	Always

**Table 1**      *Accounting AV Pairs (continued)*

Attribute Number	AV Pair Name	START	INTERIM	STOP
Attribute[42]	Acct-Input-Octets	Never	Always	Always
Attribute[43]	Acct-Output-Octets	Never	Always	Always
Attribute[44]	Acct-Session-ID	Always	Always	Always
Attribute[45]	Acct-Authentic	Always	Always	Always
Attribute[46]	Acct-Session-Time	Never	Never	Always
Attribute[47]	Acct-Input-Packets	Never	Always	Always
Attribute[48]	Acct-Output-Packets	Never	Always	Always
Attribute[49]	Acct-Terminate-Cause	Never	Never	Always
Attribute[61]	NAS-Port-Type	Always	Always	Always

1. The Framed-IP-Address AV pair is sent only if a valid Dynamic Host Control Protocol (DHCP) binding exists for the host in the DHCP snooping bindings table.

You can configure the ISR to send Cisco vendor-specific attributes (VSAs) to the RADIUS server. [Table 2](#) lists the available Cisco AV pairs.

**Note**

To enable VSAs to be sent in the accounting records you must configure the **radius-server vsa send accounting** command.

**Table 2**      *Cisco Vendor-Specific Attributes*

Attribute Number	AV Pair Name	START	INTERIM	STOP
Attribute[26,9,1]	Cisco-Avpair: connect-progress	Always	Always	Always
Attribute[26,9,2]	cisco-nas-port	Always	Always	Always
Attribute[26,9,1]	Cisco-Avpair: disc-cause	Never	Never	Always

You can view the AV pairs that are being sent by the router by entering the **debug radius accounting** privileged EXEC command. For more information about this command, see the *Cisco IOS Debug Command Reference*, Release 12.4T, at this URL:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcr/tdb\\_r/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcr/tdb_r/index.htm)

For more information about AV pairs, see RFC 3580, *IEEE 802.1x Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*.

## How to Use IEEE 802.1x Authentication With Other Features

The following sections describe how to use IEEE 802.1x Authentication in combination with other features on the switch ports on an ISR router.

- [IEEE 802.1x Authentication with VLAN Assignment, page 13](#)
- [IEEE 802.1x Authentication with Guest VLAN, page 15](#)



- [IEEE 802.1x with RADIUS-Supplied Session Timeout, page 15](#)
- [IEEE 802.1x Authentication with Voice VLAN Ports, page 16](#)
- [Enabling IEEE 802.1x SNMP Notifications, page 17](#)
- [IEEE 802.1x MIB Support, page 17](#)

## IEEE 802.1x Authentication with VLAN Assignment

**Note**

This section describes IEEE 802.1x security features available only on the switch ports in a Cisco ISR.

In Cisco IOS Release 12.4(11)T and later releases, the switch ports support IEEE 802.1x authentication with VLAN assignment. After successful IEEE 802.1x authentication of a port, the RADIUS server sends the VLAN assignment to configure the switch port. You can use the VLAN Assignment feature to limit network access for certain users.

The RADIUS server database maintains the username-to-VLAN mappings, assigning the VLAN based on the username of the supplicant connected to the switch port.

This section contains the following information about IEEE 802.1x VLAN assignment:

- [Prerequisites for IEEE 802.1x VLAN Assignment, page 13](#)
- [Restrictions for IEEE 802.1x VLAN Assignment, page 13](#)
- [Configuring VLAN Assignment, page 14](#)

### Prerequisites for IEEE 802.1x VLAN Assignment

Before the VLAN Assignment feature is implemented, the following conditions must be met:

- IEEE 802.1x must be enabled on the switch port.
- EAP support must be enabled on the RADIUS server.
- AAA authorization must be configured on the port for all network-related service requests.
- The port must be successfully authenticated.

### Restrictions for IEEE 802.1x VLAN Assignment

These are the restrictions that apply to the VLAN Assignment feature:

- The switch port is always assigned to the configured access VLAN when any of the following conditions occurs:
  - No VLAN is supplied by the RADIUS server.
  - The VLAN information from the RADIUS server is not valid.
  - IEEE 802.1x authentication is disabled on the port.
  - The port is in the force authorized, force unauthorized, unauthorized, or shutdown state.

**Note**

An access VLAN is a VLAN assigned to an access port. All packets sent from or received on this port belong to this VLAN.

- Assignment to the configured access VLAN prevents ports from appearing unexpectedly in an inappropriate VLAN because of a configuration error. Examples of configuration errors include the following:
  - A nonexistent or malformed VLAN ID
  - Attempted assignment to a voice VLAN ID
- The IEEE 802.1x authentication with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VLAN Membership Policy Server (VMPS).
- If the multi-host mode is enabled on an IEEE 802.1x port, all hosts are placed in the same VLAN (specified by the RADIUS server) as the first authenticated host.
- If an IEEE 802.1x port is authenticated and put in the RADIUS server-assigned VLAN, any change to the port access VLAN configuration does not take effect.

## Configuring VLAN Assignment



### Note

This section describes IEEE 802.1x security features available only on the switch ports in a Cisco ISR.

To configure VLAN assignment on a switch port, you need to perform these tasks:

- Enable AAA authorization by using the **network** keyword to allow interface configuration from the RADIUS server. For detailed instructions, see the [“Configuring RADIUS Authorization for User Privileged Access and Network Services”](#) section of the “Configuring Switch-Based Authentication” chapter in the *Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE*.
- Enable IEEE 802.1x authentication. For detailed instructions, see the [“Configuring RADIUS Login Authentication”](#) section of the “Configuring Switch-Based Authentication” chapter in the *Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE*.



### Note

The VLAN assignment feature is automatically enabled when you configure IEEE 802.1x authentication on an access port.

- Assign vendor-specific tunnel attributes in the RADIUS server. The RADIUS server must return these attributes to the router:
  - [64] Tunnel-Type = VLAN
  - [65] Tunnel-Medium-Type = 802
  - [81] Tunnel-Private-Group-ID = VLAN name or VLAN ID

Attribute [64] must contain the value “VLAN” (type 13). Attribute [65] must contain the value “802” (type 6). Attribute [81] specifies the VLAN name or VLAN ID assigned to the IEEE 802.1x-authenticated user.

For examples of tunnel attributes, see the [“Configuring the Switch to Use Vendor-Specific RADIUS Attributes”](#) section of the “Configuring Switch-Based Authentication” chapter in the *Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE*.

## IEEE 802.1x Authentication with Guest VLAN

**Note**

This section describes IEEE 802.1x security features available only on the switch ports in a Cisco ISR.

You can configure a guest VLAN for each IEEE 802.1x-capable switch port on the router to provide limited services to clients, such as downloading the IEEE 802.1x client. These clients might be upgrading their system for IEEE 802.1x authentication, and some hosts, such as Windows 98 systems, might not be IEEE 802.1x-capable.

When you enable a guest VLAN on an IEEE 802.1x port, the router assigns clients to a guest VLAN when the router does not receive a response to its EAP request/identity frame or when EAPOL packets are not sent by the client.

The router maintains the EAPOL packet history. If an EAPOL packet is detected on the interface during the lifetime of the link, the router determines that the device connected to that interface is an IEEE 802.1x-capable client, and the interface does not change to the guest VLAN state. EAPOL history is cleared if the interface link status goes down. If no EAPOL packet is detected on the interface, the interface changes to the guest VLAN state.

In Cisco IOS Release 12.4(11)T and later releases, if devices send EAPOL packets to the router during the lifetime of the link, the router does not allow clients that fail authentication access to the guest VLAN.

**Note**

If an EAPOL packet is detected after the interface has changed to the guest VLAN, the interface reverts to an unauthorized state, and IEEE 802.1x authentication restarts.

Any number of IEEE 802.1x-incapable clients are allowed access when the router port is moved to the guest VLAN. If an IEEE 802.1x-capable client joins the same port on which the guest VLAN is configured, the port is put into the unauthorized state in the user-configured access VLAN, and authentication is restarted.

Guest VLANs are supported on IEEE 802.1x ports in single-host or multi-host mode.

You can configure any active VLAN except a remote switch port analyzer (RSPAN) VLAN or a voice VLAN as an IEEE 802.1x guest VLAN. The guest VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.

For information about configuring a guest VLAN, see the [“Configuring a Guest VLAN”](#) section of the “Configuring IEEE 802.1x Port-Based Authentication” chapter in the *Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE*.

## IEEE 802.1x with RADIUS-Supplied Session Timeout

**Note**

This section describes IEEE 802.1x security features available only on the switch ports in a Cisco ISR.

You can specify whether a switch port uses a locally configured or a RADIUS-provided reauthentication timeout. If the switch port is configured to use the local timeout, it reauthenticates the host when the timer expires.

If the switch port is configured to use the RADIUS-provided timeout, it looks in the RADIUS Access-Accept message for the Session-Timeout and optional Termination-Action attributes. The switch port uses the value of the Session-Timeout attribute to determine the duration of the session, and it uses the value of the Termination-Action attribute to determine the switch action when the session's timer expires.

If the Termination-Action attribute is present and its value is RADIUS-Request, the switch port reauthenticates the host. If the Termination-Action attribute is not present, or its value is Default, the switch port terminates the session.

**Note**

The supplicant on the port detects that its session has been terminated and attempts to initiate a new session. Unless the authentication server treats this new session differently, the supplicant may see only a brief interruption in network connectivity as the switch sets up a new session.

If the switch port is configured to use the RADIUS-supplied timeout, but the Access-Accept message does not include a Session-Timeout attribute, the switch port never reauthenticates the supplicant. This behavior is consistent with Cisco's wireless access points.

For details on how to configure RADIUS-provided session timeout, see the [“Configuring RADIUS-Provided Session Timeouts”](#) section in the “Configuring 802.1X Port-Based Authentication” chapter of the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(31)SG*.

## IEEE 802.1x Authentication with Voice VLAN Ports

**Note**

This section describes IEEE 802.1x security features available only on the switch ports in a Cisco ISR.

A voice VLAN port is a special access port associated with two VLAN identifiers:

- Voice VLAN identifier (VVID) to carry voice traffic to and from the IP phone. The VVID is used to configure the IP phone connected to the port.
- Port VLAN identifier (PVID) to carry the data traffic to and from the workstation connected to the router through the IP phone. The PVID is the native VLAN of the port.

The IP phone uses the VVID for its voice traffic, regardless of the authorization state of the port. This allows the phone to work independently of IEEE 802.1x authentication.

In single-host mode, only the IP phone is allowed on the voice VLAN. In multi-host mode, additional supplicants can send traffic on the voice VLAN after a supplicant is authenticated on the PVID. When multi-host mode is enabled, the supplicant authentication affects both the PVID and the VVID.

A voice VLAN port becomes active when there is a link, and the device MAC address appears after the first CDP message from the IP phone. Cisco IP phones do not relay CDP messages from other devices. As a result, if several IP phones are connected in series, the router recognizes only the one directly connected to it. When IEEE 802.1x authentication is enabled on a voice VLAN port, the router drops packets from unrecognized IP phones more than one hop away.

When IEEE 802.1x authentication is enabled on a port, you cannot configure a port VLAN that is equal to a voice VLAN.

**Note**

If you enable IEEE 802.1x authentication on an access port on which a voice VLAN is configured and to which a Cisco IP Phone is connected, the Cisco IP phone loses connectivity to the router for up to 30 seconds.

For information about configuring IEEE 802.1x with voice VLANs, see the [“Configuring IEEE 802.1X with Voice VLAN”](#) section in the [“Configuring 802.1X Port-Based Authentication”](#) chapter of the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(31)SG*.

## Enabling IEEE 802.1x SNMP Notifications

**Note**

This section describes IEEE 802.1x security features available only on the switch ports in a Cisco ISR.

Follow the steps below to enable Simple Network Management Protocol (SNMP) notifications for IEEE 802.1x features on the switch ports.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps dot1x**

### DETAILED STEPS

	Command	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>snmp-server enable traps dot1x notification type</b>  <b>Example:</b> Router (config)# snmp-server enable traps dot1x no-guest-vlan	Enables SNMP logging and reporting when no Guest VLAN is configured or available.

## IEEE 802.1x MIB Support

Cisco IOS Release 12.4(11)T provides support for the following MIBs that provide SNMP access to IEEE 802.1x feature components:

- IEEE8021-PAE-MIB

- Cisco-PAE-MIB

The IEEE8021-PAE-MIB supports reporting of the following information:

- The state of the IEEE 802.1x state machine on a particular port
- Statistics associated with the state of the IEEE 802.1x state machine

The Cisco-PAE-MIB provides SNMP support for the logging and reporting of events, including:

- Port mode
- Guest VLAN number (Details the Guest VLAN number configured on a port.)
- InGuestVLAN (Indicates whether a port is in the Guest VLAN.)

## Configuration Examples for IEEE 802.1x Features

This section provides the following comprehensive configuration examples:

- [Enabling IEEE 802.1x and AAA on a Port: Example, page 18](#)
- [Enabling IEEE 802.1x RADIUS Accounting: Example, page 19](#)
- [Configuring IEEE 802.1x with Guest VLAN: Example, page 19](#)
- [Configuring RADIUS-Provided Session Timeout: Example, page 20](#)
- [Configuring IEEE 802.1x with Voice VLAN: Example, page 20](#)
- [Displaying IEEE 802.1x Statistics and Status: Example, page 20](#)

### Enabling IEEE 802.1x and AAA on a Port: Example

This example shows how to enable IEEE 802.1x and AAA on Fast Ethernet port 2/1, and how to verify the configuration:



#### Note

Whenever you configure any IEEE 802.1x parameter on a port, a dot1x authenticator is automatically created on the port. As a result **dot1x pae authenticator** appears in the configuration to ensure that IEEE 802.1x authentication still works without manual intervention on legacy configurations. The appearance of the IEEE 802.1x information in the configuration is likely to change in future releases.

This example shows how to enable IEEE 802.1x and AAA on Fast Ethernet port 2/1, and how to verify the configuration:

```
Router# configure terminal
Router(config)# dot1x system-auth-control
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# interface fastethernet2/1
Router(config-if)# switchport mode access
Router(config-if)# dot1x pae authenticator
Router(config-if)# dot1x port-control auto
Router(config-if)# end
Router# show dot1x interface fastethernet7/1 details
```

```

Dot1x Info for FastEthernet7/1

PAE = AUTHENTICATOR
PortControl = AUTO
ControlDirection = Both
HostMode = SINGLE_HOST
ReAuthentication = Disabled
QuietPeriod = 60
ServerTimeout = 30
SuppTimeout = 30
ReAuthPeriod = 3600 (Locally configured)
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
RateLimitPeriod = 0

Dot1x Authenticator Client List

Supplicant = 1000.0000.2e00
 Auth SM State = AUTHENTICATED
 Auth BEND SM Stat = IDLE
Port Status = AUTHORIZED

Authentication Method = Dot1x
Authorized By = Authentication Server
Vlan Policy = N/A

```

## Enabling IEEE 802.1x RADIUS Accounting: Example

This example shows how to specify the server with IP address 172.20.39.46 as the RADIUS server. The first command configures the RADIUS server, specifying port 1612 as the authorization port, 1813 as the UDP port for accounting, and rad123 as the encryption key:

```

Router# configure terminal
Router(config)# radius-server host 172.20.39.46 auth-port 1812 acct-port 1813 key rad123
Router(config)# aaa accounting dot1x default start-stop group radius
Router(config)# aaa accounting system default start-stop group radius
Router(config)# end
Router#

```



### Note

You must configure the RADIUS server to perform accounting tasks.

## Configuring IEEE 802.1x with Guest VLAN: Example

This example shows how to enable the guest VLAN feature and to specify VLAN 5 as a guest VLAN:

```

Router# configure terminal
Router(config)# interface gigabitethernet0/1
Router(config-if)# switchport mode access
Router(config-if)# dot1x pae authenticator
Router(config-if)# dot1x guest-vlan 5
Router(config-if)# dot1x port-control auto
Router(config-if)# end
Router#

```

## Configuring RADIUS-Provided Session Timeout: Example

This example assumes you have enabled IEEE 802.1x reauthentication and shows how to configure the switch port to derive the reauthentication period from the server and to verify the configuration:

```
Router# configure terminal
Router(config)# interface fastethernet7/1
Router(config-if)# switchport mode access
Router(config-if)# dot1x pae authenticator
Router(config-if)# dot1x timeout reauth-period server
Router(config-if)# end
Router#
```

## Configuring IEEE 802.1x with Voice VLAN: Example

This example shows how to enable IEEE 802.1x with voice VLAN feature on Fast Ethernet interface 5/9:

```
Router# configure terminal
Router(config)# interface fastethernet5/9
Router(config-if)# switchport access vlan 2
Router(config-if)# switchport mode access
Router(config-if)# switchport voice vlan 10
Router(config-if)# dot1x pae authenticator
Router(config-if)# dot1x port-control auto
Router(config-if)# end
Router(config)# end
Router#
```

## Displaying IEEE 802.1x Statistics and Status: Example

To display IEEE 802.1x statistics for all ports, use the **show dot1x all statistics** privileged EXEC command. To display IEEE 802.1x statistics for a specific port, use the **show dot1x statistics interface interface-id** privileged EXEC command.

To display the IEEE 802.1x administrative and operational status for the switch, use the **show dot1x all [details | statistics | summary]** privileged EXEC command. To display the IEEE 802.1x administrative and operational status for a specific port, use the **show dot1x interface interface-id** privileged EXEC command. For detailed information about the fields in these displays, see the command reference for this release.

This example shows the output of the **show dot1x all** command:

```
Router-871# show dot1x all

Sysauthcontrol Enabled
Dot1x Protocol Version 2

Dot1x Info for FastEthernet1

PAE = AUTHENTICATOR
PortControl = AUTO
ControlDirection = Both
HostMode = MULTI_HOST
ReAuthentication = Disabled
QuietPeriod = 60
ServerTimeout = 30
SuppTimeout = 30
ReAuthPeriod = 3600 (Locally configured)
```



```
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
RateLimitPeriod = 0
Router-871#
```

This example shows the output of the **show dot1x summary** command:

```
Router-871# show dot1x all summary
```

Interface	PAE	Client	Status
Fal	AUTH	000d.bcef.bfdc	AUTHORIZED

# Additional References

The following sections provide references related to the IEEE 802.1x Port-Based Authentication feature.

## Related Documents

Related Topic	Document Title
Configuring IEEE 802.1x Port-Based Authentication	The chapter “ <a href="#">Configuring 802.1X Port-Based Authentication</a> ” in the <i>Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide</i> , 12.2(31)SGA
IEEE 802.1x Commands	<a href="#">Catalyst 4500 Series Switch Cisco IOS Command Reference</a> , Release 12.2(31)SGA
IEEE 802.1x Commands	<a href="#">Catalyst 3750 Switch Command Reference</a> , Cisco IOS Release 12.2(25)SEE
VPN Access Control Using IEEE 802.1x Authentication	The “ <a href="#">VPN Access Control Using 802.1X Authentication</a> ” section in the “Configuring 802.1X Authentication Services” chapter in Part 6: “Other Security Features” of the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4

## Standards

Standard	Title
IEEE 802.1x	<i>Port Based Network Access Control</i>

## MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> <li>• IEEE8021-PAE-MIB</li> <li>• Cisco-PAE-MIB</li> </ul>	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFCs

RFC	Title
RFC 3580	<i>IEEE 802.1x Remote Authentication Dial In User Service (RADIUS) Usage Guidelines</i>

## Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **aaa accounting**
- **dot1x guest-vlan**
- **snmp-server enable traps**

# Feature Information for Configuring IEEE 802.1x Port-Based Authentication

Table 3 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.4(11)T or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 3**      **Feature Information for Configuring IEEE 802.1x Port-Based Authentication**

Feature Name	Releases	Feature Information
IEEE 802.1x Authenticator	12.3(4)T	<p>This feature was introduced to prevent unauthorized devices (supplicants) from gaining access to the network.</p> <p>This feature is available on the following Cisco ISRs equipped with cards or modules that include switch ports:</p> <ul style="list-style-type: none"> <li>• Cisco 800 Series ISR</li> <li>• Cisco 870 Series ISR</li> <li>• Cisco 1800 Series ISR</li> <li>• Cisco 2800 Series ISR</li> <li>• Cisco 3800 Series ISR</li> </ul> <p>In Cisco IOS Release 12.4(11)T, this feature was modified to include the other features listed in <a href="#">Table 3</a>.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">IEEE 802.1x Authenticator, page 5</a></li> <li>• <a href="#">Enabling IEEE 802.1x and AAA on a Port: Example, page 18</a></li> </ul>
IEEE 802.1x RADIUS Accounting	12.4(11)T	<p>This feature relays important events to the RADIUS server (such as the supplicant's connection session). This information is used for security and billing purposes.</p> <p>In Cisco IOS Release 12.4(11)T, this feature was introduced on the following Cisco ISRs equipped with cards or modules that include switch ports:</p> <ul style="list-style-type: none"> <li>• Cisco 800 Series ISR</li> <li>• Cisco 870 Series ISR</li> <li>• Cisco 1800 Series ISR</li> <li>• Cisco 2800 Series ISR</li> <li>• Cisco 3800 Series ISR</li> </ul> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">IEEE 802.1x with RADIUS Accounting, page 9</a></li> <li>• <a href="#">Enabling IEEE 802.1x RADIUS Accounting: Example, page 19</a></li> </ul>

**Table 3**      **Feature Information for Configuring IEEE 802.1x Port-Based Authentication (continued)**

Feature Name	Releases	Feature Information
IEEE 802.1x—VLAN Assignment	12.4(11)T	<p>This feature allows the RADIUS server to send the VLAN assignment to configure the switch port.</p> <p>In Cisco IOS Release 12.4(11)T, this feature was introduced on the following Cisco ISRs equipped with cards or modules that include switch ports:</p> <ul style="list-style-type: none"> <li>• Cisco 800 Series ISR</li> <li>• Cisco 870 Series ISR</li> <li>• Cisco 1800 Series ISR</li> <li>• Cisco 2800 Series ISR</li> <li>• Cisco 3800 Series ISR</li> </ul> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">IEEE 802.1x Authentication with VLAN Assignment, page 13</a></li> <li>• <a href="#">Configuring VLAN Assignment, page 14</a></li> </ul>
IEEE 802.1x Guest VLAN	12.4(11)T	<p>This feature allows you to configure a guest VLAN for each IEEE 802.1x-capable switch port on the router to provide limited services to clients, such as downloading the IEEE 802.1x client.</p> <p>In Cisco IOS Release 12.4(11)T, this feature was introduced on the following Cisco ISRs equipped with cards or modules that include switch ports:</p> <ul style="list-style-type: none"> <li>• Cisco 800 Series ISR</li> <li>• Cisco 870 Series ISR</li> <li>• Cisco 1800 Series ISR</li> <li>• Cisco 2800 Series ISR</li> <li>• Cisco 3800 Series ISR</li> </ul> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">IEEE 802.1x Authentication with Guest VLAN, page 15</a></li> <li>• <a href="#">Configuring IEEE 802.1x with Guest VLAN: Example, page 19</a></li> </ul>

**Table 3**      **Feature Information for Configuring IEEE 802.1x Port-Based Authentication (continued)**

Feature Name	Releases	Feature Information
IEEE 802.1x RADIUS-Supplied Session Timeout	12.4(11)T	<p>This feature allows you to specify whether a switch port uses a locally configured or a RADIUS-provided reauthentication timeout.</p> <p>In Cisco IOS Release 12.4(11)T, this feature was introduced on the following Cisco ISRs equipped with cards or modules that include switch ports:</p> <ul style="list-style-type: none"><li>• Cisco 800 Series ISR</li><li>• Cisco 870 Series ISR</li><li>• Cisco 1800 Series ISR</li><li>• Cisco 2800 Series ISR</li><li>• Cisco 3800 Series ISR</li></ul> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"><li>• <a href="#">IEEE 802.1x with RADIUS-Supplied Session Timeout, page 15</a></li><li>• <a href="#">Configuring RADIUS-Provided Session Timeout: Example, page 20</a></li></ul>

**Table 3**      **Feature Information for Configuring IEEE 802.1x Port-Based Authentication (continued)**

Feature Name	Releases	Feature Information
IEEE 802.1x—Voice VLAN	12.4(11)T	<p>This feature allows you to configure a special access port associated with two VLAN identifiers:</p> <ul style="list-style-type: none"> <li>• Voice VLAN identifier (VVID) to carry voice traffic to and from the IP phone. The VVID is used to configure the IP phone connected to the port.</li> <li>• Port VLAN identifier (PVID) to carry the data traffic to and from the workstation connected to the router through the IP phone. The PVID is the native VLAN of the port.</li> </ul> <p>In Cisco IOS Release 12.4(11)T, this feature was introduced on the following Cisco ISRs equipped with cards or modules that include switch ports:</p> <ul style="list-style-type: none"> <li>• Cisco 800 Series ISR</li> <li>• Cisco 870 Series ISR</li> <li>• Cisco 1800 Series ISR</li> <li>• Cisco 2800 Series ISR</li> <li>• Cisco 3800 Series ISR</li> </ul> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">IEEE 802.1x Authentication with Voice VLAN Ports, page 16</a></li> <li>• <a href="#">Configuring IEEE 802.1x with Voice VLAN: Example, page 20</a></li> </ul>
IEEE 802.1x MIB Support	12.4(11)T	<p>This feature provides support for the following MIBs:</p> <ul style="list-style-type: none"> <li>• IEEE8021-PAE-MIB</li> <li>• Cisco-PAE-MIB</li> </ul> <p>In Cisco IOS Release 12.4(11)T, this feature was introduced on the following Cisco ISRs equipped with cards or modules that include switch ports:</p> <ul style="list-style-type: none"> <li>• Cisco 800 Series ISR</li> <li>• Cisco 870 Series ISR</li> <li>• Cisco 1800 Series ISR</li> <li>• Cisco 2800 Series ISR</li> <li>• Cisco 3800 Series ISR</li> </ul> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">IEEE 802.1x MIB Support, page 17</a></li> <li>• <a href="#">Enabling IEEE 802.1x SNMP Notifications, page 17</a></li> </ul>



# Glossary

**authentication server**—Entity that provides an authentication service to an authenticator. Typically, a RADIUS server operates as an authentication server, with RADIUS acting as a transport for EAP from the authenticator to the authentication server.

**authenticator**—Facilitates the authentication and granting of service to a supplicant. Typically, an authenticator transposes an EAP conversation from supplicant to authentication server. An authenticator is usually an EAP conduit, but is aware of the conversation.

**EAPOL**—Extensible Authentication Protocol over LAN. Primarily, IEEE 802.1x is an encapsulation definition for EAP over IEEE 802 media. The key protocol for the transport of an end-to-end EAP conversation via IEEE 802 media between a supplicant and an authenticator.

**IEEE 802.1x**—Authentication standard for port-based access control over any IEEE 802 or PPP media. Used primarily to identify users before allowing their traffic onto the network. IEEE 802.1x is a framework designed to address and provide port-based access control using authentication.

**supplicant**—Usually a laptop or other device that requires authentication or has to access service from a network point of attachment.

**Note**

See [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





# Remote Site IEEE 802.1X Local Authentication Service

The Remote Site IEEE 802.1X Local Authentication Service feature provides the ability to configure an access point or wireless-aware router to act as a local RADIUS server. Configuring local authentication service provides a backup authentication service in the event of a WAN link or server failure.

## Feature History for the Remote Site IEEE 802.1X Local Authentication Service Feature

Release	Modification
12.2(11)JA	This feature was introduced on the Cisco IOS Release 12.2(11)JA on Cisco Aironet access points.
12.3(11)T	This feature was integrated into the Cisco IOS Release 12.3(11)T on the Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700 series, and Cisco 3800 series routers.

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for Configuring Remote Site IEEE 802.1X Local Authentication Service, page 2](#)
- [Restrictions for Configuring Remote Site IEEE 802.1X Local Authentication Service, page 2](#)
- [Information About Configuring Remote Site IEEE 802.1x Local Authentication Service, page 2](#)
- [How to Configure Remote Site IEEE 802.1X Local Authentication Service, page 3](#)
- [Monitoring and Maintaining 802.1X Local Authentication Service, page 9](#)
- [Configuration Examples for Remote Site IEEE 802.1X Local Authentication Service, page 9](#)
- [Additional References, page 13](#)



**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

- [Command Reference, page 14](#)

## Prerequisites for Configuring Remote Site IEEE 802.1X Local Authentication Service

Follow these guidelines when you configure an access point or wireless-aware router as a local authentication server:

- To prevent performance degradation, configure local authentication service on an access point or a wireless-aware router that does not have a high CPU load.
- Physically secure the access point or router to protect its configuration.

## Restrictions for Configuring Remote Site IEEE 802.1X Local Authentication Service

The following are restrictions of the local authentication service feature:

- The local authentication server does not synchronize its database with the main RADIUS servers. It is necessary to manually configure the local authentication server with client usernames and passwords.
- LEAP is the only supported authentication protocol.
- Although multiple local authentication servers can exist on one network, only one authentication server can be configured on any single device.

## Information About Configuring Remote Site IEEE 802.1x Local Authentication Service

On typical wireless LANs that use 802.1X authentication, access points and wireless-aware routers rely on remote site RADIUS servers to authenticate client devices. This authentication traffic must cross a WAN link. If the WAN link fails, or if the access points and routers cannot reach the RADIUS servers, then the client devices cannot access the wireless network even if their requirements for access are strictly local.

To provide for local authentication service or backup authentication service in the event of a WAN link or server failure, you can configure an access point or wireless-aware router to act as a local RADIUS server. The access point or wireless-aware router can authenticate Light Extensible Authentication Protocol (LEAP)-enabled wireless client devices and allow them to join your network.

Because the local authentication device does not synchronize its database with the main RADIUS servers, you must configure the local authentication server with client usernames and passwords. The local authentication server also permits you to specify a VLAN and a list of service set identifiers (SSIDs) that a client is allowed to use.

[Table 69](#) shows the maximum number of clients that can be configured on a local authentication server.

**Table 69**      *Maximum Number of Clients That Can be Configured on a Local Authentication Server*

Local Authentication Server	Maximum Number of Clients
Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200	50
Cisco 2610XM, Cisco 2611XM routers	50
Cisco 2620XM, Cisco 2621XM routers	50
Cisco 2650XM, Cisco 2651XM routers	50
Cisco 2691 routers	100
Cisco 2811 routers	100
Cisco 2821 routers	100
Cisco 2851 routers	200
Cisco 3725 routers	250
Cisco 3745 routers	500
Cisco 3825 routers	500
Cisco 3845 routers	1000

**Note**

Users that are associated to the local authentication server might notice a drop in performance during authentication of client devices. However, if your wireless LAN contains only one access point, you can configure that device as both the 802.1X authenticator and the local authentication server.

You configure access points and routers to use the local authentication server when they cannot reach the main servers or when a RADIUS server is not available.

The access points and wireless-aware routers stop using the local authentication server automatically when the link to the main servers is restored.

If your local authentication server also serves client devices, you must enter the local authentication server access point or router as a network access server (NAS). When a LEAP client associates to the local authentication server access point, the access point uses itself to authenticate the client.

**Caution**

The access point or wireless-aware router that you use as an authentication server contains detailed authentication information about your wireless LAN, so you should secure it physically to protect its configuration.

## How to Configure Remote Site IEEE 802.1X Local Authentication Service

This section contains the following procedures:

- [Configuring the Local Authentication Server, page 4](#) (required)

- [Configuring User Groups on the Local Authentication Server, page 5](#) (optional)
- [Creating the User List on the Local Authentication Server, page 6](#) (required)
- [Saving the Configuration on the Local Authentication Server, page 6](#) (optional)
- [Configuring Access Points or Routers to Use the Local Authentication Server, page 7](#) (required)

## Configuring the Local Authentication Server

Perform this task to configure the access point as a local authentication server.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server local**
5. **nas ip-address key shared-key**

### DETAILED STEPS

	Command	Purpose
Step 1	Router> <b>enable</b>	Enables privileged EXEC mode.
Step 2	Router# <b>configure terminal</b>	Enters global configuration mode.
Step 3	Router(config)# <b>aaa new-model</b>	Enables AAA.
Step 4	Router(config)# <b>radius-server local</b>	Enables the access point or router as a local authentication server and enters configuration mode for the authentication server.
Step 5	Router(config-radsrv)# <b>nas ip-address key shared-key</b>	<p>Adds an access point or wireless domain services (WDS) device to the list of units that use the local authentication server. Enter the IP address of the access point or WDS device, and the shared key used to authenticate communication between the local authentication server and other access points. You must enter this shared key on the WDS devices that use the local authentication server. Each access point and candidate WDS that uses the local authentication server is a network access server (NAS).</p> <p>If an access point is the local authentication server that also serves client devices, you must enter the local authentication server access point as a NAS.</p> <p><b>Note</b> Leading spaces in the key string are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.</p> <p>Repeat this step to add each access point and candidate WDS device that uses the local authentication server.</p>

## Configuring User Groups on the Local Authentication Server

Perform this optional task (beginning in local RADIUS server configuration mode) to configure user groups on the local authentication server.



### Note

If you do not wish to configure user groups on the local authentication server, skip this task and go to the [“Creating the User List on the Local Authentication Server”](#) section on page 6.

### SUMMARY STEPS

1. **group** *group-name*
2. **vlan** *vlan*
3. **ssid** *ssid*
4. **reauthentication time** *seconds*
5. **block count** *count* **time** {*seconds* | **infinite**}
6. **exit**

### DETAILED STEPS

	Command	Purpose
Step 1	Router(config-radsrv) # <b>group</b> <i>group-name</i>	Enters user group configuration mode and configures a user group to which you can assign shared settings.
Step 2	Router(config-radsrv-group) # <b>vlan</b> <i>vlan</i>	(Optional) Specifies a VLAN to be used by members of the user group. The access point moves group members into that VLAN, overriding other VLAN assignments. You can assign only one VLAN to the group.
Step 3	Router(config-radsrv-group) # <b>ssid</b> <i>ssid</i>	(Optional) Enters up to 20 service set identifiers (SSIDs) to limit members of the user group to those SSIDs. The access point checks whether the client's SSID matches an SSID in the list. If the SSID does not match, the client is disassociated.
Step 4	Router(config-radsrv-group) # <b>reauthentication time</b> <i>seconds</i>	(Optional) Configures the number of seconds after which access points should reauthenticate members of the group. The reauthentication provides users with a new encryption key. The default setting is 0, which means that group members are never required to reauthenticate.
Step 5	Router(config-radsrv-group) # <b>block count</b> <i>count</i> <b>time</b> { <i>seconds</i>   <b>infinite</b> }	(Optional) To help protect against password-guessing attacks, you can lock out group members for a length of time after a set number of incorrect passwords. <ul style="list-style-type: none"> <li>Count—The number of failed passwords that triggers a lockout of the username.</li> <li>Time—The number of seconds that the lockout should last. If you enter <b>infinite</b>, an administrator must manually unblock the locked username. For more information, see the <a href="#">“Unlocking Usernames”</a> section on page 6.</li> </ul>
Step 6	Router(config-radsrv-group) # <b>exit</b>	Returns to authenticator configuration mode.

## Unblocking Usernames

You can unblock usernames before the lockout time expires or when the lockout time is set to infinite. To unblock a locked username, enter the following command in privileged EXEC mode on the local authentication server.

```
Router# clear radius local-server user username
```

## Creating the User List on the Local Authentication Server

Perform the required task described in the following paragraphs to create a user list on the local authentication server and to configure the users that are allowed to authenticate using the local authentication server.



### Note

If you do not wish to configure users on the local authentication server, skip this task and go to the [“Saving the Configuration on the Local Authentication Server” section on page 6](#).

You must enter a username and password for each user. If you know only the NT hash value of the password, which you can often find in the authentication server database, you can enter the NT hash as a string of hexadecimal digits.

To add the user to a user group, enter the group name. If you do not specify a group, the user is not assigned to a specific VLAN and is never forced to reauthenticate.

Beginning in local RADIUS server configuration mode, enter the **user** command for each username:

```
Router(config-radsrv)# user username {password | nthash} password [group group-name]
```

## Saving the Configuration on the Local Authentication Server

Perform this optional task to save the current configuration.

### SUMMARY STEPS

1. **end**
2. **copy running-config startup-config**

### DETAILED STEPS

	Command	Purpose
Step 1	Router(config-radsrv)# <b>end</b>	Returns to privileged EXEC mode.
Step 2	Router# <b>copy running-config startup-config</b>	Saves your entries in the configuration file.



## Configuring Access Points or Routers to Use the Local Authentication Server

Perform this required task to add the local authentication server to the list of servers on the client access point or wireless-aware router.

**Note**

If your local authentication server access point also serves client devices, you must configure the local authentication server to use itself to authenticate client devices.

On the wireless devices that use the local authentication server, use the **radius-server host** command in privileged EXEC mode to enter the local authentication server as a RADIUS server. The order in which the devices attempt to use the servers matches the order in which you enter the servers in the device configuration. If you are configuring the device to use a RADIUS server for the first time, enter the main RADIUS servers first, and enter the local authentication server last.

**Note**

You must enter **1812** as the authentication port and **1813** as the accounting port. The local authentication server listens on User Datagram Protocol (UDP) port 1813 for RADIUS accounting packets. It discards the accounting packets but sends acknowledge packets back to the RADIUS clients to prevent the clients from reacting as though the server is down.

Use the **radius-server deadtime** command in global configuration mode to set an interval during which the access point or router does not attempt to use servers that do not respond, thus avoiding the wait for a request to time out before trying the next configured server. A server marked as dead is skipped by additional requests for the duration of minutes that you specify, up to 1440 (24 hours).

To remove the local authentication server from the access point or router configuration, use the **no radius-server host** command in global configuration mode.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server host** {hostname | ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]
5. **aaa group server** {radius | tacacs+} group-name
6. **server ip-address auth-port 1812 acct-port 1813**
7. **aaa authentication login** named-authentication-list
8. **end**
9. **show running-config**
10. **copy running-config startup-config**

## DETAILED STEPS

	Command	Purpose
Step 1	Router> <b>enable</b>	Enables privileged EXEC mode.
Step 2	Router# <b>configure terminal</b>	Enters global configuration mode.
Step 3	Router(config)# <b>aaa new-model</b>	Enables authentication, authorization, and accounting (AAA). This step must be configured before the rest of the AAA configuration steps.
Step 4	Router(config)# <b>radius-server host</b> {hostname   ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]	<p>Specifies the IP address or hostname of the remote RADIUS server host.</p> <ul style="list-style-type: none"> <li>• (Optional) For <b>auth-port port-number</b>, specify the UDP destination port for authentication requests.</li> <li>• (Optional) For <b>acct-port port-number</b>, specify the UDP destination port for accounting requests.</li> <li>• (Optional) For <b>timeout seconds</b>, specify the time interval that the access point waits for the RADIUS server to reply before retransmitting. The range is 1 to 1000. This setting overrides the setting made using the <b>radius-server timeout</b> command in global configuration mode. If no timeout is set with the <b>radius-server host</b> command, the setting made using the <b>radius-server timeout</b> command is used.</li> <li>• (Optional) For <b>retransmit retries</b>, specify the number of times that a RADIUS request is re-sent to a server if that server is not responding or is responding slowly. The range is 1 to 1000. If no retransmit value is set using the <b>radius-server host</b> command, the setting made using the <b>radius-server retransmit</b> command in global configuration command mode is used.</li> <li>• (Optional) For <b>key string</b>, specify the authentication and encryption key used between the access point and the RADIUS daemon running on the RADIUS server.</li> </ul> <p><b>Note</b> The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the <b>radius-server host</b> command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.</p> <p>To configure the access point to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure to use a different UDP port number for each host. The access point software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.</p>
Step 5	<b>aaa group server</b> {radius   tacacs+} group-name	Defines the AAA server-group with a group name.
Step 6	Router(config-sg-radius)# <b>server ip-address auth-port 1812 acct-port 1813</b>	Defines the AAA server IP address, authentication port, and accounting port.
Step 7	Router(config)# <b>aaa authentication login named-authentication-list</b>	Creates an authentication method list for the server group.

	Command	Purpose
Step 8	Router(config)# <b>end</b>	Returns to privileged EXEC mode.
Step 9	Router# <b>show running-config</b>	Displays the current configuration for your verification.
Step 10	Router# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

## Verifying the Configuration for Local Authentication Service

Use the **show running-config** command in global configuration mode to verify the current configuration for local authentication service.

### SUMMARY STEPS

1. **enable**
2. **show running-config**

### DETAILED STEPS

	Command	Purpose
Step 1	Router> <b>enable</b>	Enables privileged EXEC mode.
Step 2	Router# <b>show running-config</b>	Displays the current access point operating configuration

## Monitoring and Maintaining 802.1X Local Authentication Service

To view statistics collected by the local authentication server, enter the following command in privileged EXEC mode:

```
Router# show radius local-server statistics
```

To reset local authentication server statistics to zero, enter the following command in privileged EXEC mode:

```
Router# clear radius local-server statistics
```

## Configuration Examples for Remote Site IEEE 802.1X Local Authentication Service

This section provides the following configuration examples:

- [Setting Up a Local Authentication Server: Example](#)
- [Setting Up Two Main Servers and a Local Authentication Server: Example](#)
- [Displaying Local Authentication Server Configuration: Example](#)
- [Displaying Local Authentication Server Statistics: Example](#)

## Setting Up a Local Authentication Server: Example

This example shows how to set up a local authentication server used by three access points with three user groups and several users:

```
AP# configure terminal
AP(config)# aaa new-model
AP(config)# aaa group server radius RADIUS_SERVER_GROUP
AP(config-sg-radius)# server 10.0.0.1 auth-port 1812 acct-port 1813
AP(config)# aaa authentication login RADIUS_METHOD_LIST
AP(config)# radius-server host 10.0.0.1 auth-port 1812 acct-port 1813 key 110337
AP(config)# radius-server local
AP(config-radsrv)# nas 10.91.6.159 key 110337
AP(config-radsrv)# nas 10.91.6.162 key 110337
AP(config-radsrv)# nas 10.91.6.181 key 110337
AP(config-radsrv)# group clerks
AP(config-radsrv-group)# vlan 87
AP(config-radsrv-group)# ssid batman
AP(config-radsrv-group)# ssid robin
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# block count 2 time 600
AP(config-radsrv-group)# group cashiers
AP(config-radsrv-group)# vlan 97
AP(config-radsrv-group)# ssid deer
AP(config-radsrv-group)# ssid antelope
AP(config-radsrv-group)# ssid elk
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# block count 2 time 600
AP(config-radsrv-group)# group managers
AP(config-radsrv-group)# vlan 77
AP(config-radsrv-group)# ssid mouse
AP(config-radsrv-group)# ssid chipmunk
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# block count 2 time 600
AP(config-radsrv-group)# exit
AP(config-radsrv)# user jsmith password twain74 group clerks
AP(config-radsrv)# user stpatrick password snake100 group clerks
AP(config-radsrv)# user nick password uptown group clerks
AP(config-radsrv)# user sam password rover32 group cashiers
AP(config-radsrv)# user patsy password crowder group cashiers
AP(config-radsrv)# user carl password 272165 group managers
AP(config-radsrv)# user vic password lid178 group managers
AP(config-radsrv)# end
```

## Setting Up Two Main Servers and a Local Authentication Server: Example

This example shows how to set up two main servers and a local authentication server with a server deadline of 10 minutes:

```
Router(config)# aaa new-model
Router(config)# aaa group server radius RADIUS_SERVER_GROUP
Router(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
Router(config-sg-radius)# server 172.10.0.1 auth-port 1645 acct-port 1646
Router(config-sg-radius)# server 10.91.6.151 auth-port 1812 acct-port 1813
Router(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001 key 77654
Router(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646 key 77654
Router(config)# radius-server host 10.91.6.151 auth-port 1812 acct-port 1813 key 110337
Router(config)# radius-server deadline 10
```

In this example, if the WAN link to the main servers fails, the access point or wireless-aware router completes these steps when a LEAP-enabled client device associates:

1. It tries the first server, times out multiple times, and marks the first server as dead.
2. It tries the second server, times out multiple times, and marks the second server as dead.
3. It tries and succeeds using the local authentication server.

If another client device needs to authenticate during the 10-minute deadtime interval, the access point skips the first two servers and tries the local authentication server first. After the deadtime interval, the access point tries to use the main servers for authentication. When setting a deadtime, you must balance the need to skip dead servers with the need to check the WAN link and begin using the main servers again as soon as possible.

Each time an access point or wireless-aware router tries to use the main servers while they are down, the client device that is trying to authenticate might report an authentication timeout. The client device retries and succeeds when the main servers time out and the access point or wireless-aware router tries the local authentication server. You can extend the timeout value on Cisco client devices to accommodate expected server timeouts.

## Displaying Local Authentication Server Configuration: Example

The following is sample output for configuration of a local authentication server on the Cisco 2621 router.

```
2621-1# show run
Building configuration...

Current configuration : 2954 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 2621-1
!
!
aaa new-model
!
!
aaa group server radius RADIUS_LEAP_GROUP
 server 10.0.0.1 auth-port 1812 acct-port 1813
!
aaa authentication login AUTH_LEAP group RADIUS_LEAP_GROUP
aaa session-id common
ip subnet-zero
!
!
ip dhcp pool 2621-dhcp-pool
 network 10.0.0.0 255.0.0.0
!
!
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
```

```

interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
!
interface FastEthernet1/1
 switchport mode trunk
 no ip address
!
interface FastEthernet1/2
 no ip address
 shutdown
!
interface FastEthernet1/3
 no ip address
 shutdown
!
interface FastEthernet1/4
 no ip address
 shutdown
!
interface FastEthernet1/5
 no ip address
!
!
interface GigabitEthernet1/0
 no ip address
 shutdown
!
interface Vlan1
 ip address 10.0.0.1 255.0.0.0
!
ip classless
!
ip http server
no ip http secure-server
!
!
radius-server local
 nas 10.0.0.1 key 0 cisco
 user ap-1 nthash 7 101B2A415547345A5F25790801706510064152425325720D7D04075D523D4F780A
 user ap-5 nthash 7 144231535C540C7A77096016074B51332753030D0877705A264F450A09720A7307
 user user1 nthash 7 1350344A5B5C227B78057B10107A452232515402097C77002B544B45087D0E7200
!
radius-server host 10.0.0.1 auth-port 1812 acct-port 1813
radius-server key cisco
!
wlccp authentication-server infrastructure AUTH_LEAP
wlccp authentication-server client leap AUTH_LEAP
wlccp wds priority 255 interface Vlan1
!
line con 0
line aux 0
line vty 0 4
!
!
!
end

```

## Displaying Local Authentication Server Statistics: Example

The following is sample output for configuration for the **show radius local-server statistics** command:

```
router-2621-1# show radius local-server statistics
Successes : 11262 Unknown usernames : 0
Client blocks : 0 Invalid passwords : 8
Unknown NAS : 0 Invalid packet from NAS: 0

NAS : 10.0.0.1
Successes : 11262 Unknown usernames : 0
Client blocks : 0 Invalid passwords : 8
Corrupted packet : 0 Unknown RADIUS message : 0
No username attribute : 0 Missing auth attribute : 0
Shared key mismatch : 0 Invalid state attribute: 0
Unknown EAP message : 0 Unknown EAP auth type : 0

Maximum number of configurable users: 50, current user count: 11
Username Successes Failures Blocks
vayu-ap-1 2235 0 0
vayu-ap-2 2235 0 0
vayu-ap-3 2246 0 0
vayu-ap-4 2247 0 0
vayu-ap-5 2247 0 0
vayu-11 3 0 0
vayu-12 5 0 0
vayu-13 5 0 0
vayu-14 30 0 0
vayu-15 3 0 0
scm-test 1 8 0

router-2621-1#
```

The first section shows cumulative statistics from the local authentication server. The second section shows statistics for each access point (NAS) that is authorized to use the local authentication server. The third section shows statistics for individual users. If a user is blocked and the lockout time is set to infinite, *Blocked* appears at the end of the line of statistics for that user. If the lockout time is not set to infinite, *Unblocked in x seconds* appears at the end of the statistics line for that user.

## Additional References

The following sections provide references related to Remote Site IEEE 802.1X Local Authentication Service.

## Related Documents

Related Topic	Document Title
Comprehensive set of software configuration commands	<i>Cisco IOS Software Configuration Guide for Cisco Aironet Access Points</i>
Configuration commands for wireless roaming	<i>Configuring Fast Secure Roaming</i>

## MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

## Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>

## Command Reference

This feature uses no new or modified commands. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.



---

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





# VPN Access Control Using 802.1X Authentication

---

**First Published: August 11, 2003**

**Last Updated: June 2, 2006**

The home access router provides connectivity to the corporate network via a Virtual Private Network (VPN) tunnel through the Internet. In the home LAN, apart from the employee, other members of the household may also be using the same access router. The VPN Access Control Using 802.1X Authentication feature allows enterprise employees to access their enterprise networks from home while allowing other household members to access only the Internet. The feature uses the IEEE 802.1X protocol framework to achieve the VPN access control. The authenticated employee has access to the VPN tunnel and others (unauthenticated users on the same LAN) have access only to the Internet.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all of the features documented in this module.* To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for VPN Access Control Using 802.1X Authentication”](#) section on [page 33](#).

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for VPN Access Control Using 802.1X Authentication, page 2](#)
- [Restrictions for VPN Access Control Using 802.1X Authentication, page 2](#)
- [Information About VPN Access Control Using 802.1X Authentication, page 2](#)
- [How to Configure VPN Access Control Using 802.1X Authentication, page 5](#)
- [Configuration Examples for VPN Access Control Using 802.1X Authentication, page 24](#)
- [Additional References, page 30](#)



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

- [Command Reference, page 32](#)
- [Feature Information for VPN Access Control Using 802.1X Authentication, page 33](#)

## Prerequisites for VPN Access Control Using 802.1X Authentication

- The PCs connecting behind the router should have 802.1X clients running on them.
- You should know how to configure authentication, authorization, and accounting (AAA) and RADIUS.
- You should be familiar with IP Security (IPSec).
- You should be familiar with Dynamic Host Configuration Protocol (DHCP).
- You should know how to configure user lists on a Cisco access control server (ACS).

## Restrictions for VPN Access Control Using 802.1X Authentication

- Easy VPN is not supported.
- VLAN interfaces are currently not supported.
- If there is a switch located between the router and the supplicant (client PC), the Extensible Authentication Protocol over LAN (EAPOL) frames will not reach the router because the switch discards them.

## Information About VPN Access Control Using 802.1X Authentication

To configure the VPN Access Control Using 802.1X Authentication feature, you should understand the following concepts:

- [How VPN Control Using 802.1X Authentication Works, page 2](#)
- [802.1X Supplicant Support, page 4](#)
- [Authentication Using Passwords and MD5, page 5](#)

## How VPN Control Using 802.1X Authentication Works

The home access router provides connectivity to the corporate network via a VPN tunnel through the Internet. In the home LAN, both authenticated (employee) and unauthenticated (other household members) users exist, and both have access to the corporate VPN tunnel. Currently there is no existing mechanism to prevent the unauthenticated user from accessing the VPN tunnel.

To distinguish between the users, the VPN Access Control Using 802.1X Authentication feature uses the IEEE 802.1X protocol that allows end hosts to send user credentials on Layer 2 of the network operating system. Unauthenticated traffic users will be allowed to pass through the Internet but will be blocked from accessing the corporate VPN tunnel. The VPN Access Control Using 802.1X feature expands the scope of the 802.1X standard to authenticate devices rather than ports, meaning that multiple devices can be independently authenticated for any given port. This feature separates traffic from authenticated and unauthenticated users so that separate access policies can be applied.

When an 802.1X-capable host starts up, it will initiate the authentication phase by sending the EAPOL-Start 802.1X protocol data unit (PDU) to the reserved IEEE multicast MAC address (01-80-C2-00-00-03) with the Ethernet type or length set to 0x888E.

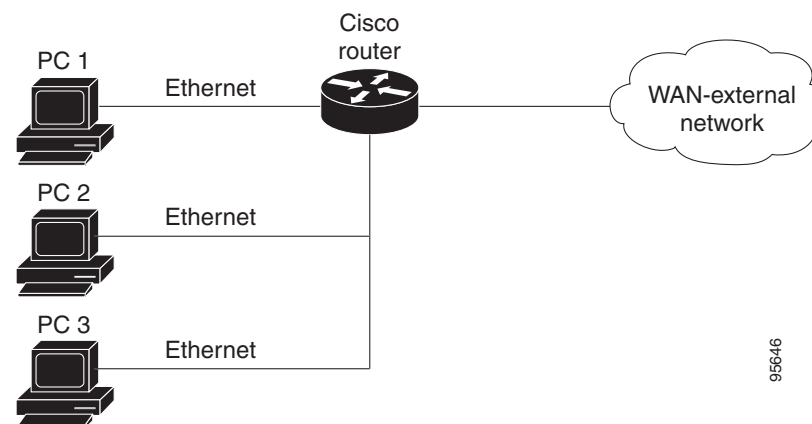
All 802.1X PDUs will be identified as such by the Ethernet driver and will be enqueued to be handled by an 802.1X process. On some platforms, Ethernet drivers have to program the interface address filter so that EAPOL packets can be accepted.

On the router, the receipt of the EAPOL-Start message will result in the source MAC address being “remembered,” and an EAPOL-request or identity PDU being sent to the host. The router will send all host-addressed PDUs to the individual MAC address of the host rather than to the multicast address.

## 802.1X Authentication Sample Topology and Configuration

Figure 1 illustrates a typical scenario in which VPN access control using 802.1X authentication is in place.

**Figure 1** Typical 802.1X Authentication Setup



In Figure 1, all the PCs are 802.1X capable hosts, and the Cisco router is an authenticator. All the PCs are connected to the built-in hub or to an external hub. If a PC does not support 802.1X authentication, MAC-based authentication is supported on the Cisco router.



### Note

- You can have any kind of connectivity or network beyond the Cisco router WAN.
- If there is a switch located between the router and the supplicant (client PC), the EAPOL frames will not reach the router because the switch discards them.
- A supplicant is an entity at one end of a point-to-point LAN segment that is being authenticated by an authenticator that is attached to the other end of that link.

## Converged 802.1X Authenticator Support

The Cisco IOS commands in Cisco IOS Release 12.4(6)T for 802.1X authenticators have been standardized to work the same way on various Cisco IOS platforms.

## 802.1X Supplicant Support

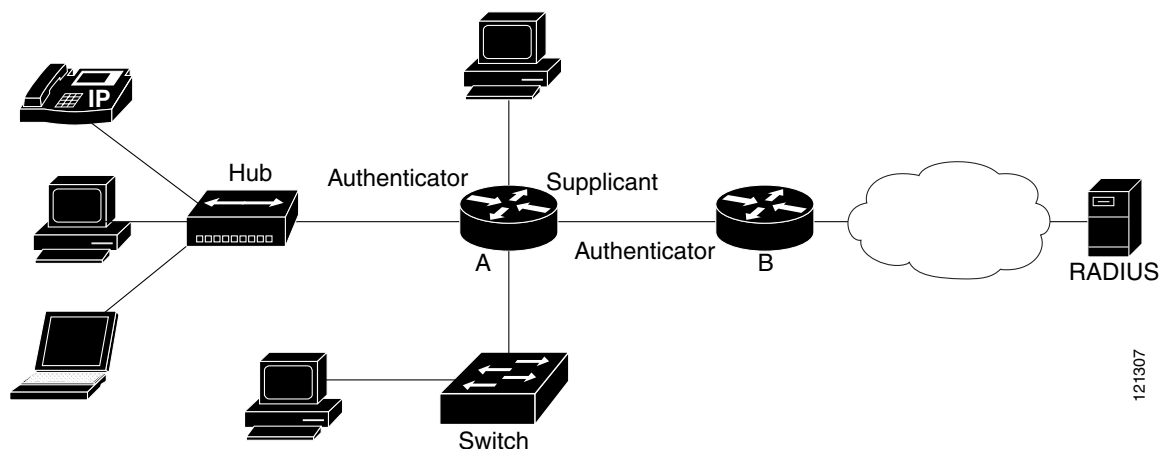
There are deployment scenarios in which a network device (a router acting as an 802.1X authenticator) is placed in an unsecured location and cannot be trusted as an authenticator. This scenario requires that a network device be able to authenticate itself against another network device. The 802.1X supplicant support functionality provides the following solutions for this requirement:

- An Extensible Authentication Protocol (EAP) framework has been included so that the supplicant has the ability to “understand” and “respond” to EAP requests. EAP-Message Digest 5 (EAP-MD5) is currently supported.
- Two network devices that are connected through an Ethernet link can act as a supplicant and as an authenticator simultaneously, thus providing mutual authentication capability.
- A network device that is acting as a supplicant can authenticate itself with more than one authenticator (that is, a single port on a supplicant can be connected to multiple authenticators).

The following illustration is an example of 802.1X supplicant support. The illustration shows that a single supplicant port has been connected to multiple authenticators. Router A is acting as an authenticator to devices that are sitting behind it on the LAN while those devices are acting as supplicants. At the same time, Router B is an authenticator to Router A (which is acting as a supplicant). The RADIUS server is located in the enterprise network.

When Router A tries to authenticate devices on the LAN, it needs to “talk” to the RADIUS server, but before it can allow access to any of the devices that are sitting behind it, it has to prove its identity to Router B. Router B checks the credential of Router A and gives access.

**Figure 2** Multiple Instances of Supplicant Support



121307

## Converged 802.1X Supplicant Support

The Cisco IOS commands in Cisco IOS Release 12.4(6)T for 802.1X supplicants have been standardized to work the same way on various Cisco IOS platforms.

## Authentication Using Passwords and MD5

For information about using passwords and Message Digest 5 (MD5), see the following document on Cisco.com:

- [Improving Security on Cisco Routers](#)

## How to Configure VPN Access Control Using 802.1X Authentication

This section includes the following procedures:

- [Configuring an AAA RADIUS Server, page 5](#)
- [Configuring a Router, page 5](#)
- [Configuring a PC, page 19](#)
- [Monitoring VPN Access Control Using 802.1X Authentication, page 21](#)
- [Verifying VPN Access Control Using 802.1X Authentication, page 23](#)

### Configuring an AAA RADIUS Server

To configure an AAA RADIUS server, perform the following steps.

- 
- |               |                                                                                                                    |
|---------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>Configure entries for the network access server and associated shared secrets.</b>                              |
|               | <b>Note</b> The AAA server can be FreeRADIUS or Cisco Secure ACS or any other similar product with 802.1X support. |
| <b>Step 2</b> | <b>Add the username and configure the password of the user.</b>                                                    |
| <b>Step 3</b> | <b>Configure a global or per-user authentication scheme.</b>                                                       |
- 

### Configuring a Router

This section contains the following procedures:

- [Enabling 802.1X Authentication, page 6](#) (required)
- [Configuring Router and RADIUS Communication, page 7](#) (required)
- [Configuring 802.1X Parameters \(Retransmissions and Timeouts\), page 8](#) (optional)
- [Configuring the Identity Profile, page 11](#) (required)
- [Configuring the Virtual Template and DHCP, page 12](#) (required)
- [Configuring the Necessary Access Control Policies, page 17](#) (optional)
- [Configuring a Router As a Supplicant, page 17](#) (optional)

## Enabling 802.1X Authentication

To enable 802.1X port-based authentication, you should configure the router so that it can communicate with the AAA server, enable 802.1X globally, and enable 802.1X on the interface. To enable 802.1X port-based authentication, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication dot1x default group radius**
5. **dot1x system-auth-control**
6. **identity profile default**
7. **interface type slot/port**
8. **dot1x port-control auto**

### DETAILED STEPS

	Command	Description
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>aaa new-model</b>  <b>Example:</b> Router (config)# aaa new-model	Enables AAA.
Step 4	<b>aaa authentication dot1x default group radius</b>  <b>Example:</b> Router (config)# aaa authentication dot1x default group radius	Creates an 802.1X port-based authentication method list.
Step 5	<b>dot1x system-auth-control</b>  <b>Example:</b> Router (config)# dot1x system-auth-control	Globally enables 802.1X port-based authentication.
Step 6	<b>identity profile default</b>  <b>Example:</b> Router (config)# identity profile default	Creates an identity profile and enters dot1x profile configuration mode.



	Command	Description
Step 7	<b>interface</b> <i>type slot/port</i>  <b>Example:</b> Router (config)# interface fastethernet 5/1	Enters interface configuration mode and specifies the interface to be enabled for 802.1X port-based authentication.
Step 8	<b>dot1x port-control auto</b>  <b>Example:</b> Router (config-if)# dot1x port-control auto	Enables 802.1X port-based authentication on the interface.

## Example

This section provides the following examples:

- [802.1X Configuration](#)
- [Verifying 802.1X Authentication](#)

### 802.1X Configuration

The following example shows that 802.1X authentication has been configured on a router:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# dot1x system-auth-control
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x port-control auto
```

### Verifying 802.1X Authentication

The following **show dot1x** command sample output shows that 802.1X authentication has been configured on a router:

```
Router# show dot1x all

PortControl = AUTO
ReAuthentication = Disabled
ReAuthPeriod = 3600 Seconds
ServerTimeout = 30 Seconds
SuppTimeout = 30 Seconds
QuietWhile = 120 Seconds
MaxReq = 2
```

## Configuring Router and RADIUS Communication

To configure RADIUS server parameters, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip radius source-interface** *interface-name*
4. **radius-server host** {*hostname* | *ip-address*}
5. **radius-server key** *string*

## DETAILED STEPS

	Command	Description
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip radius source-interface</b> <i>interface-name</i>  <b>Example:</b> Router (config)# ip radius source-interface ethernet1	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.
Step 4	<b>radius-server host</b> ( <i>hostname</i>   <i>ip-address</i> )  <b>Example:</b> Router (config)# radius-server host 172.16.39.46	Configures the RADIUS server host name or IP address of the router. <ul style="list-style-type: none"><li>To use multiple RADIUS servers, reenter this command for each server.</li></ul>
Step 5	<b>radius-server key</b> <i>string</i>  <b>Example:</b> Router (config)# radius-server key radiuskey	Configures the authorization and encryption key used between the router and the RADIUS daemon running on the RADIUS server. <ul style="list-style-type: none"><li>The key is a text string that must match the encryption key used on the RADIUS server.</li></ul>

## Example

The following example shows that RADIUS server parameters have been configured on the router:

```
Router# configure terminal
Router(config)# ip radius source-interface ethernet1
Router(config)# radius-server host 172.16.39.46
Router(config)# radius-server key radiuskey
```

## Configuring 802.1X Parameters (Retransmissions and Timeouts)

Various 802.1X retransmission and timeout parameters can be configured. Because all of these parameters have default values, configuring them is optional. To configuring the retransmission and timeout parameters, perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **dot1x max-req** *number-of-retries*

5. **dot1x port-control** [auto | force-authorized | force-unauthorized]
6. **dot1x control-direction** {both | in}
7. **dot1x reauthentication**
8. **dot1x timeout tx-period** *seconds*
9. **dot1x timeout server-timeout** *seconds*
10. **dot1x timeout reauth-period** *seconds*
11. **dot1x timeout quiet-period** *seconds*
12. **dot1x timeout ratelimit-period** *seconds*

## DETAILED STEPS

	Command	Description
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface</b> <i>type slot/port</i>  <b>Example:</b> Router (config)# interface ethernet 0/1	Enters interface configuration mode and specifies the interface to be enabled for 802.1X port-based authentication.
Step 4	<b>dot1x max-req</b> <i>number-of-retries</i>  <b>Example:</b> Router (config-if)# dot1x max-req 3	Sets the maximum number of times that the router sends an EAP request/identity frame (assuming that no response is received) to the supplicant before concluding that the supplicant does not support 802.1X.
Step 5	<b>dot1x port-control</b> [auto   force-authorized   force-unauthorized]  <b>Example:</b> Router (config-if)# dot1x port-control auto	Sets the port control value. <ul style="list-style-type: none"> <li><b>auto (optional)</b>—Authentication status of the supplicant will be determined by the authentication process.</li> <li><b>force-authorized (optional)</b>—All the supplicants on the interface will be authorized. The <b>force-authorized</b> keyword is the default.</li> <li><b>force-unauthorized (optional)</b>—All the supplicants on the interface will be unauthorized.</li> </ul>
Step 6	<b>dot1x control-direction</b> {both   in}  <b>Example:</b> Router (config-if)# dot1x control-direction both	Changes the port control to unidirectional or bidirectional.

	Command	Description
Step 7	<b>dot1x reauthentication</b>  <b>Example:</b> Router (config-if)# dot1x reauthentication	Enables periodic reauthentication of the supplicants on the interface.  <ul style="list-style-type: none"> <li>The reauthentication period can be set using the <b>dot1x timeout</b> command.</li> </ul>
Step 8	<b>dot1x timeout tx-period</b> <i>seconds</i>  <b>Example:</b> Router (config-if)# dot1x timeout tx-period 60	Sets the timeout for supplicant retries.  <ul style="list-style-type: none"> <li>If an 802.1X packet is sent to the supplicant and the supplicant does not send a response, the packet will be sent again after the time that was set using the <i>seconds</i> argument.</li> <li>The value is 1 through 65535 seconds. The default is 30 seconds.</li> </ul>
Step 9	<b>dot1x timeout server-timeout</b> <i>seconds</i>  <b>Example:</b> Router (config-if)# dot1x timeout server-timeout 60	Sets the timeout for RADIUS retries.  <ul style="list-style-type: none"> <li>If an 802.1X packet is sent to the server, and the server does not send a response, the packet will be sent again after the time that was set using the <i>seconds</i> argument.</li> <li>The value is from 1 to 65535 seconds. The default is 30 seconds.</li> </ul>
Step 10	<b>dot1x timeout reauth-period</b> <i>seconds</i>  <b>Example:</b> Router (config-if)# dot1x timeout reauth-period 1800	Sets the time after which an automatic reauthentication should be initiated.  <ul style="list-style-type: none"> <li>The value is from 1 to 65535 seconds. The default is 3600 seconds.</li> </ul>
Step 11	<b>dot1x timeout quiet-period</b> <i>seconds</i>  <b>Example:</b> Router (config-if)# dot1x timeout quiet-period 600	The time after which authentication is restarted after the authentication has failed.  <ul style="list-style-type: none"> <li>The value is from 1 to 65535 seconds. The default is 120 seconds.</li> </ul>
Step 12	<b>dot1x timeout ratelimit-period</b> <i>seconds</i>  <b>Example:</b> Router (config-if)# dot1x timeout ratelimit-period 60	The rate limit period throttles the EAP-START packets from misbehaving supplicants.  <ul style="list-style-type: none"> <li>The value is from 1 to 65535 seconds.</li> </ul>

## Example

The following configuration example shows that various retransmission and timeout parameters have been configured:

```
Router# configure terminal
Router(config)# interface ethernet 0
Router(config-if)# dot1x port-control auto
Router(config-if)# dot1x reauthentication
Router(config-if)# dot1x timeout reauth-period 1800
Router(config-if)# dot1x timeout quiet-period 600
Router(config-if)# dot1x timeout supp-timeout 60
Router(config-if)# dot1x timeout server-timeout 60
```

## Configuring the Identity Profile

The **identity profile default** command allows you to configure the static MAC addresses of the client that do not support 802.1X and to authorize or unauthorize them statically. The VPN Access Control Using 802.1X Authentication feature allows authenticated and unauthenticated users to be mapped to different interfaces. Under the **dot1x profile** configuration mode, you can specify the virtual template interface that should be used to create the virtual-access interface to which unauthenticated supplicants will be mapped. To specify which virtual template interface should be used to create the virtual access interface, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **identity profile default**
4. **description** text *line-of-description*
5. **template** *virtual-template*
6. **device** [authorize | not-authorize] mac-address *mac-address*
7. **device authorize** type *device-type*

### DETAILED STEPS

	Command	Description
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>identity profile default</b>  <b>Example:</b> Router (config)# identity profile default	Creates an identity profile and enters identity profile configuration mode.
Step 4	<b>description</b> <i>line-of-description</i>  <b>Example:</b> Router (config-identity-prof)# description description 1	Associates descriptive text with the profile.
Step 5	<b>template</b> <i>virtual-template</i>  <b>Example:</b> Router (config-identity-prof)# template virtual-template 1	Specifies the virtual template interface that will serve as the configuration clone source for the virtual interface that is dynamically created for authenticated users.

	Command	Description
Step 6	<b>device</b> [ <b>authorize</b>   <b>not-authorize</b> ] <b>mac-address</b> <i>mac-address</i>  <b>Example:</b> Router (config-identity-prof)# <b>device authorize</b> <b>mac-address</b> <i>mac-address</i> H.H.H	Statically authorizes or unauthorizes a supplicant (by giving its MAC address) if the supplicant does not “understand” 802.1X.
Step 7	<b>device authorize type</b> <i>device-type</i>  <b>Example:</b> Router (config-identity-prof)# <b>device authorize type</b> <b>cisco ip phone</b>	Statically authorizes or unauthorizes a device type.

### Example

The following example shows that Cisco IP phones and a specific MAC address have been statically authorized:

```
Router# configure terminal
Router (config)# identity profile default
Router(config-lx-prof)# description put the description here
Router(config-lx-prof)# template virtual-template1
Router(config-lx-prof)# device authorize type cisco ip phone
Router(config-lx-prof)# device authorize mac-address 0001.024B.B4E7
```

## Configuring the Virtual Template and DHCP

The VPN Access Control Using 802.1X Authentication feature can be configured with one DHCP pool or two. If there are two pools, the unauthenticated and authenticated devices will get their addresses from separate DHCP pools. For example, the public pool can have an address block that has only local significance, and the private pool can have an address that is routable over the VPN tunnel. To configure your router for a private pool and for a public pool, perform the following steps.

### SUMMARY STEPS

#### Configuring the Identity Profile

1. **enable**
2. **configure terminal**
3. **identity profile default**
4. **description** *description-string*
5. **template** *virtual-template*
6. **exit**

#### Configuring the DHCP Private Pool

1. **ip dhcp pool** *name*
2. **network** *network-number* [*mask*]
3. **default-router** *address*

**Configuring the DHCP Public Pool**

1. **ip dhcp pool** *name*
2. **network** *network-number* [*mask*]
3. **default-router** *address*
4. **exit**

**Configuring the Interface**

1. **configure terminal**
2. **interface** *type slot/port*
3. **ip address** *ip-address mask* [*secondary*]
4. **interface virtual-template** *number*
5. **ip address** *ip-address mask* [*secondary*]
6. **exit**

**Configuring an Interface Without Assigning an Explicit IP Address to the Interface**

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **ip unnumbered** *type number*

**DETAILED STEPS****Configuring the Identity Profile**

	Command	Description
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>identity profile default</b>  <b>Example:</b> Router (config)# identity profile default	Creates an identity profile and enters identity profile configuration mode.
Step 4	<b>description</b> <i>description-string</i>  <b>Example:</b> Router (config-identity-prof)# description description_string_goes_here	Associates descriptive text with the identity profile.

	Command	Description
Step 5	<b>template</b> <i>virtual-template</i>  <b>Example:</b> Router (config-identity-prof)# template virtualtemplate1	Specifies the virtual template interface that will serve as the configuration clone source for the virtual interface that is dynamically created for authenticated users.
Step 6	<b>exit</b>  <b>Example:</b> Router (config-identity-prof)# exit	Exits identity profile configuration mode.

### Configuring the DHCP Private Pool

	Command	Description
Step 1	<b>ip dhcp pool</b> <i>name</i>  <b>Example:</b> Router (config)# ip dhcp pool private	Configures a DHCP private address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
Step 2	<b>network</b> <i>network-number [mask]</i>  <b>Example:</b> Router (config-dhcp)# network 10.0.0.1 255.0.0.0	Configures the subnet number and mask for a DHCP private address pool on a Cisco IOS DHCP server.
Step 3	<b>default-router</b> <i>address</i>  <b>Example:</b> Router (config-dhcp)# default-router 10.2.2.2	Specifies the default router list for a DHCP client.

### Configuring the DHCP Public Pool

	Command	Description
Step 1	<b>ip dhcp pool</b> <i>name</i>  <b>Example:</b> Router (config-dhcp)# ip dhcp pool public	Configures the DHCP public address pool on a Cisco IOS DHCP server.
Step 2	<b>network</b> <i>network-number [mask]</i>  <b>Example:</b> Router (config-dhcp)# network 10.4.4.255.0.0.0	Configures the subnet number and mask for a DHCP public address pool on a Cisco IOS DHCP server.



	Command	Description
Step 3	<b>default-router</b> <i>address</i>  <b>Example:</b> Router (config-dhcp)# default-router 10.12.12.12	Specifies the default router list for a DHCP client.
Step 4	<b>exit</b>  <b>Example:</b> Router (config-dhcp)# exit	Exits DHCP pool configuration mode.

### Configuring the Interface

	Command	Description
Step 1	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 2	<b>interface</b> <i>type slot/port</i>  <b>Example:</b> Router (config)# interface loopback 0/1	Enters interface configuration mode and specifies the interface to be enabled.
Step 3	<b>ip address</b> <i>ip-address mask</i> [ <b>secondary</b> ]  <b>Example:</b> Router (config-if)# ip address 10.5.5.5 255.255.255.0	Sets the private IP address for the interface.
Step 4	<b>interface virtual-template</b> <i>number</i> Router (config-if)# interface virtual-template 1	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
Step 5	<b>ip address</b> <i>ip-address mask</i> [ <b>secondary</b> ]  <b>Example:</b> Router (config-if)# ip address 10.6.6.6 255.255.255.0	Sets the public IP address for the interface.
Step 6	<b>exit</b>  <b>Example:</b> Router (config-if)# exit	Exits interface configuration mode.

## Configuring an Interface Without Assigning an Explicit IP Address to the Interface

	Command	Description
Step 1	<b>enable</b>  <b>Example:</b> Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface type slot/port</b>  <b>Example:</b> Router (config)# interface virtual-template 1/2	Enters interface configuration mode and specifies the interface to be enabled.
Step 4	<b>ip unnumbered type number</b>  <b>Example:</b> Router (config-if)# ip unnumbered loopback 0	Enables IP processing on an interface without assigning an explicit IP address to the interface.

## Example

The following example shows that the identity profile associates virtual-template1 with unauthenticated supplicants. Virtual-template1 gets its IP address from interface loopback 0, and unauthenticated supplicants are associated with a public pool. Authenticated users are associated with a private pool.

```
Router(config)# identity profile default
Router(config-lx-prof)# description put the description here
Router(config-lx-prof)# template virtual-template1
Router(config-lx-prof)# exit
```

```
Router(config)# ip dhcp pool private
Router(config-dhcp)# network 10.0.0.1 255.0.0.0
Router(config-dhcp)# default-router 10.2.2.2
Router(config-dhcp)# exit
```

```
Router(config)#ip dhcp pool public
Router(config-dhcp)# network 10.4.4.4 255.0.0.0
Router(config-dhcp)# default-router 10.12.12.12
Router(config-dhcp)# exit
```

```
Router(config)# interface loopback0
Router(config-if)# ip address 10.5.5.5 255.255.255.0
Router(config-if)# interface ethernet0
Router(config-if)# ip address 10.6.6.6 255.255.255.0
Router(config-if)# exit
```

```
Router(config)# interface virtual-template1
Router(config-if)# ip unnumbered loopback 0
```

## Configuring the Necessary Access Control Policies

802.1X authentication separates traffic from authenticated and unauthenticated devices. Traffic from authenticated devices transit via the physical interface, and unauthenticated traffic transits via the Virtual-Template1. Therefore, different policies can be applied on each interface. The configuration will also depend on whether two DHCP pools or a single DHCP pool is being used. If a single DHCP pool is being used, access control can be configured on Virtual-Template1, which will block any traffic from going to the networks to which unauthenticated devices should not have access. These networks (to which unauthenticated devices should not have access) could be the corporate subnetworks protected by the VPN or encapsulated by generic routing encapsulation (GRE). There can also be access control that restricts the access between authenticated and unauthenticated devices.

If two pools are configured, the traffic from a non-trusted pool is routed to the Internet using Network Address Translation (NAT), whereas trusted pool traffic is forwarded via a VPN tunnel. The routing can be achieved by configuring ACLs used by NAT and VPN accordingly.

For an example of an access control policy configuration, see the “[Access Control Policies: Example](#)” section.

## Configuring a Router As a Supplicant

To configure a router to act as a supplicant, you have to first configure the identity profile that the supplicant will use to obtain its EAP credentials. Then you have to configure the interface as a supplicant Port Access Entity (PAE) type. To configure a router as a supplicant, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot1x credentials** *name*
4. **username** *name*
5. **password** [**0** | **7**] *password*
6. **description** *text*
7. **exit**
8. **interface** *type number*
9. **dot1x pae supplicant**
10. **exit**
11. **exit**

## DETAILED STEPS

	Command	Description
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>dot1x credentials name</b>  <b>Example:</b> Router (config)# dot1x credentials basic-user	Specifies which 802.1X credential profile to use when configuring a supplicant and enters dot1x credentials configuration mode.
Step 4	<b>username name</b>  <b>Example:</b> Router (config-dot1x-creden)# username router1	Specifies the username for an 802.1X credentials profile.
Step 5	<b>password [0   7] password</b>  <b>Example:</b> Router (config-dot1x-creden)# password secret	Specifies the password for an 802.1X credentials profile.
Step 6	<b>description text</b>  <b>Example:</b> Router (config-dot1x-creden)# description This credentials profile should be used for most configured ports	Specifies a description for an 802.1X profile.
Step 7	<b>exit</b>  <b>Example:</b> Router (config-dot1x-creden)# exit	Exits dot1x credentials configuration mode.
Step 8	<b>interface type number</b>  <b>Example:</b> Router# interface Ethernet1	Configures an interface type and enters interface configuration mode.
Step 9	<b>dot1x pae supplicant</b>  <b>Example:</b> Router (config-if)# dot1x pae supplicant	Sets the PAE type. <ul style="list-style-type: none"><li>The <b>supplicant</b> keyword specifies that the interface will be acting only as a supplicant and will not respond to messages that are meant for an authenticator.</li></ul>

	Command	Description
Step 10	<b>exit</b>  <b>Example:</b> Router (config-if)# exit	Exits interface configuration mode.
Step 11	<b>exit</b>  <b>Example:</b> Router (config-dot1x-creden)# exit	Exits global configuration mode.

## Configuring a PC

This section includes the following procedures.

- [Configuring a PC for VPN Access Control Using 802.1X Authentication, page 19](#)
- [Enabling 802.1X Authentication on a Windows 2000/XP PC, page 19](#)
- [Enabling 802.1X Authentication on a Windows 2000 PC, page 19](#)
- [Enabling 802.1X Authentication on a Windows XP PC, page 20](#)
- [Enabling 802.1X Authentication on Windows 2000 and Windows XP PCs, page 20](#)

## Configuring a PC for VPN Access Control Using 802.1X Authentication

To configure your PC for VPN Access Control Using 802.1X Authentication, perform the following steps.

- 
- |               |                        |
|---------------|------------------------|
| <b>Step 1</b> | Enable 802.1X for MD5. |
| <b>Step 2</b> | Enable DHCP.           |
- 

## Enabling 802.1X Authentication on a Windows 2000/XP PC

802.1X implementation on a Windows 2000/XP PC is unstable. A more stable 802.1X client, AEGIS (beta) for Microsoft Windows, is available at the Meetinghouse Data Communications website at [www.mtghouse.com](http://www.mtghouse.com).

## Enabling 802.1X Authentication on a Windows 2000 PC

To enable 802.1X authentication on your Windows 2000 PC, perform the following steps.

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <p><b>Make sure that the PC has at least Service Pack 3.</b></p> <p>Go to the page “Microsoft 802.1x Authentication Client” on the Microsoft Windows 2000 website at the following URL:</p> <p><a href="http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/8021xclient.asp">http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/8021xclient.asp</a>.</p> <p>At the above site, download and install 802.1X client for Windows 2000.</p> |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

If the above site is unavailable, search for the “Q313664: Recommended Update” page on the Microsoft Windows 2000 website at the following URL:  
<http://www.microsoft.com/windows2000/downloads/recommended/q313664/default.asp>

- Step 2** Reboot your PC after installing the client.
- Step 3** Go to the Microsoft Windows registry and add or install the following entry:  
“HKLM\Software\Microsoft\EAPOL\Parameters\General\Global\SupplicantMode REG\_DWORD 3”  
 (“SupplicantMode” key entry is not there by default under Global option in the registry. So add a new entry named “SupplicantMode” as REG\_DWORD and then set its value to 3.)
- Step 4** Reboot your PC.
- 

## Enabling 802.1X Authentication on a Windows XP PC

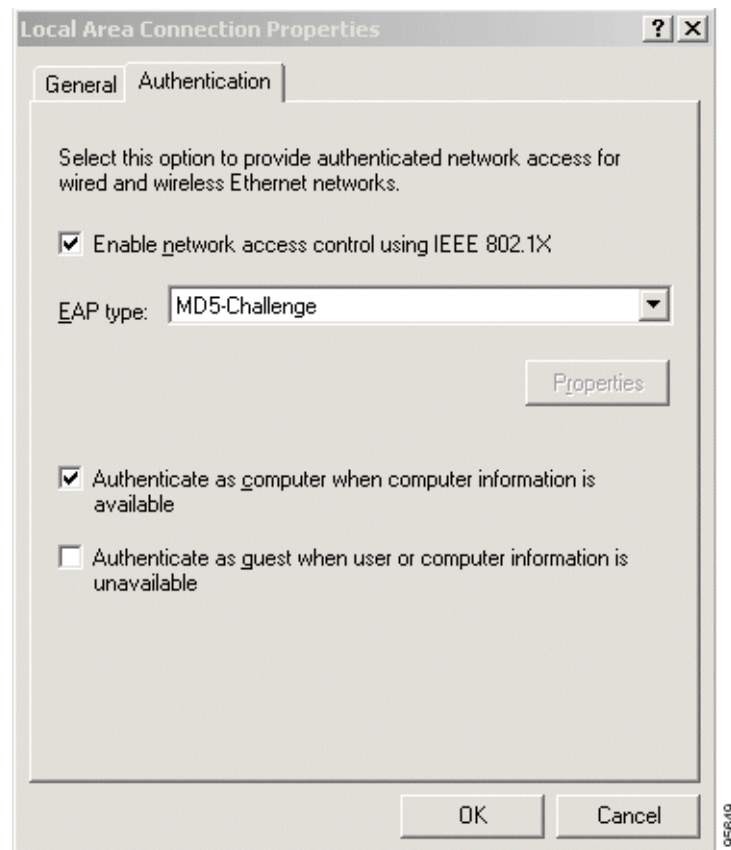
To enable 802.1X authentication on a Windows XP PC, perform the following steps.

- Step 1** Go to the Microsoft Windows registry and install the following entry there:  
“HKLM\Software\Microsoft\EAPOL\Parameters\General\Global\SupplicantMode REG\_DWORD 3”
- Step 2** Reboot your PC.
- 

## Enabling 802.1X Authentication on Windows 2000 and Windows XP PCs

To enable 802.1X authentication on Windows 2000 and Windows XP PCs, that is, if you are operating both at the same time, perform the following steps.

- Step 1** Open the Network and Dial-up Connections window on your computer.
- Step 2** Right-click the Ethernet interface (Local Area Connection) to open the properties window. It should have a tab called “Authentication.”
- Click the Authentication tab. Select the check box titled “Enable network access control using IEEE 802.1X.”
- In a short period of time you should see a dialog box (for Windows 2000) or a floating window asking you to select it. Select it, and when the next window appears, enter the username and password in this dialog box. See [Figure 3](#).
-

**Figure 3** *Local Area Connection Properties Window*


## Monitoring VPN Access Control Using 802.1X Authentication

To monitor VPN Access Control Using 802.1X Authentication, perform the following steps. The commands shown in the steps may be used one at a time and in no particular order.

### SUMMARY STEPS

1. **enable**
2. **clear dot1x**
3. **clear eap** [sessions [credentials *credentials-name* | interface *interface-name* | method *method-name* | transport *transport-name*]]
4. **debug dot1x** [aaa | all | process | rxdata | state-machine | txdata | vlan]
5. **debug eap** [all | method] [authenticator | peer] {all | errors | events | packets | sm}
6. **dot1x initialize** [interface *interface-name*]
7. **dot1x re-authenticate** *interface-type interface-number*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	clear dot1x  <b>Example:</b> Router# clear dot1x	Clears 802.1X interface information.
Step 3	<b>clear eap</b> [ <b>sessions</b> [ <b>credentials</b> <i>credentials-name</i>   <b>interface</b> <i>interface-name</i>   <b>method</b> <i>method-name</i>   <b>transport</b> <i>transport-name</i> ]]  <b>Example:</b> Router# clear eap sessions credentials type1	Clears EAP information on a switch or for a specified port.
Step 4	<b>debug dot1x</b> [ <b>aaa</b>   <b>all</b>   <b>process</b>   <b>rxdata</b>   <b>state-machine</b>   <b>txdata</b>   <b>vlan</b> ]  <b>Example:</b> Router# debug dot1x all	Displays 802.1X debugging information. <ul style="list-style-type: none"> <li><b>aaa</b>—Information is provided for AAA communications.</li> <li><b>all</b>—All 802.1X debugging messages are turned on.</li> <li><b>process</b>—Information is provided regarding the 802.1X process.</li> <li><b>rxdata</b>—Information is provided for packets that have been received from clients.</li> <li><b>state-machine</b>—Information is provided regarding the 802.1X state-machine.</li> <li><b>txdata</b>—Information is provided regarding packets that have been transmitted to clients.</li> <li><b>vlan</b>—Information is provided regarding the MAC address-based VLAN operation.</li> </ul> <div>  <b>Note</b> VLAN interfaces are currently not supported. </div>
Step 5	<b>debug eap</b> [ <b>all</b>   <i>method</i> ] [ <b>authenticator</b>   <b>peer</b> ] { <b>all</b>   <b>errors</b>   <b>events</b>   <b>packets</b>   <b>sm</b> }  <b>Example:</b> Router# debug eap all	Displays information about EAP.



	Command or Action	Purpose
Step 6	dot1x initialize [interface <i>interface-name</i> ] Router# dot1x initialize interface ethernet 0	Initializes an interface.
Step 7	dot1x re-authenticate <i>interface-type</i> <i>interface-number</i>  <b>Example:</b> Router# dot1x re-authenticate ethernet 0	Reauthenticates all the authenticated devices that are attached to the specified interface.

## Verifying VPN Access Control Using 802.1X Authentication

To verify VPN Access Control Using 802.1X Authentication, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **show dot1x** [interface *interface-name* [details]]
3. **show eap registrations** [method | transport]
4. **show eap sessions** [credentials *credentials-name* | interface *interface-name* | method *method-name* | transport *transport-name*]

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>show dot1x</b> [interface <i>interface-name</i> [details]]  <b>Example:</b> Router# show dot1x interface ethernet details	Shows details for an identity profile.
Step 3	<b>show eap registrations</b> [method   transport]  <b>Example:</b> Router# show eap registrations method	Displays EAP registration information.
Step 4	<b>show eap sessions</b> [credentials <i>credentials-name</i>   interface <i>interface-name</i>   method <i>method-name</i>   transport <i>transport-name</i> ]  <b>Example:</b> Router# show eap sessions interface gigabitethernet1/0/1	Displays active EAP session information.

# Configuration Examples for VPN Access Control Using 802.1X Authentication

This section includes the following example:

- [Typical VPN Access Control Using 802.1X Configuration: Example, page 24](#)
- [Access Control Policies: Example, page 28](#)
- [Router Acting As a Supplicant: Example, page 29](#)

## Typical VPN Access Control Using 802.1X Configuration: Example

The following sample output shows that VPN access control using 802.1X authentication has been configured. Output is shown for the router and for the gateway.

### Router

```
Router# show running-config

Building configuration...

Current configuration: 2100 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname c87x-tb
!
memory-size iomem 15
!
aaa new-model
!
!
aaa authentication dot1x default group radius
aaa session-id common
ip subnet-zero
!
ip dhcp pool private
 network 10.0.0.0 255.255.255.0
 default-router 10.0.0.1
 lease 0 0 2
!
ip dhcp pool public
 network 10.3.0.0 255.255.255.0
 default-router 10.3.0.1
!
!
ip audit notify log
ip audit po max-events 100
no ftp-server write-enable
!
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key 0 test address 150.0.0.2
!
```

```
!
crypto ipsec transform-set t1 ah-md5-hmac esp-des
crypto mib ipsec flowmib history tunnel size 2
crypto mib ipsec flowmib history failure size 2
!
crypto map test 1 ipsec-isakmp
 set peer 150.0.0.2
 set transform-set t1
 match address 101
!
dot1x system-auth-control
identity profile default
 template Virtual-Template1
!
!
interface Loopback0
 ip address 10.3.0.1 255.255.255.0
!
interface Ethernet0
 ip address 10.0.0.1 255.255.255.0
 dot1x port-control auto
 dot1x reauthentication
 dot1x timeout reauth-period 36000
!
interface Ethernet1
 no ip address
 duplex auto
 pppoe enable
 pppoe-client dial-pool-number 1
!
interface Virtual-Template1
 ip unnumbered Loopback0
 ip access-group 102 in
 ip access-group 102 out
!
interface Dialer0
 ip address 172.0.0.1 255.255.255.0
 ip mtu 1492
 encapsulation ppp
 dialer pool 1
 crypto map test
!
interface Dialer1
 no ip address
!
router rip
 network 10.0.0.0
 network 10.3.0.0
 network 172.0.0.0
!
ip classless
ip http server
no ip http secure-server
!
!
ip access-list extended list1
access-list 101 permit ip 10.0.0.0 0.0.0.255 10.5.0.0 0.0.0.255
access-list 102 deny ip 10.3.0.0 0.0.0.255 10.5.0.0 0.0.0.255
access-list 102 deny ip 10.2.0.0 0.0.0.255 10.5.0.0 0.0.0.255
access-list 102 permit ip any any
radius-server host 192.168.140.50 auth-port 1812 acct-port 1646 key radiuskey
!
line con 0
 exec-timeout 0 0
```

```

no modem enable
line aux 0
line vty 0 4
!
scheduler max-task-time 5000
!
end

```

### Peer Router As Gateway

Router# **show running-config**

```

Building configuration...
Current configuration: 1828 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname c3725
!
!
no aaa new-model
ip subnet-zero
!
vpdn enable
!
vpdn-group 1
 accept-dialin
 protocol pppoe
 virtual-template 1
!
mpls ldp logging neighbor-changes
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key 0 test address 172.0.0.1
!
!
crypto ipsec transform-set t1 ah-md5-hmac esp-des
crypto mib ipsec flowmib history tunnel size 2
crypto mib ipsec flowmib history failure size 2
!
crypto map test 1 ipsec-isakmp
 set peer 172.0.0.1
 set transform-set t1
 match address 101
!
no voice hpi capture buffer
no voice hpi capture destination
!
interface Loopback0
 description corporate
 ip address 10.5.5.5 255.255.255.0
!
interface Loopback1
 description internet
 ip address 10.6.6.6 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.140.100 255.255.255.0
 duplex auto

```

```
speed auto
!
interface FastEthernet0/1
no ip address
speed auto
half-duplex
pppoe enable
!
interface ATM1/0
ip address 10.0.0.10 255.255.255.0
no atm ilmi-keepalive
pvc 1/43
protocol ip 10.75.0.4 broadcast
encapsulation aal5snap
!
!
interface FastEthernet2/0
no ip address
speed auto
full-duplex
!
interface FastEthernet2/1
no ip address
shutdown
duplex auto
speed auto
!
interface Virtual-Template1
ip address 10.150.0.2 255.255.255.0
ip mtu 1492
crypto map test
!
!
router rip
network 10.5.0.0
network 10.6.0.0
network 10.75.0.0
network 172.0.0.0
network 192.168.140.0
!
ip http server
no ip http secure-server
ip classless
!
access-list 101 permit ip 10.5.0.0 0.0.0.255 10.0.0.1 0.0.0.255
no cdp log mismatch duplex
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
login
!
!
end
```

## Access Control Policies: Example

The following output example shows that access control policies have been configured.

### Single DHCP pool

```
ip dhcp pool private
 network 10.0.0.0 255.255.255.0
 default-router 20.0.0.1
 exit
crypto isakmp policy 1
 authentication pre-share
!
crypto isakmp key test address address
 crypto ipsec transform-set t1 esp-3des esp-sha-hmac
 mode tunnel
crypto map test 1 ipsec-isakmp
 set peer address
 set transform-set t1
 match address 101
access-list 101 permit ip 10.0.0.0 0.0.0.255 50.0.0.0 0.0.0.255
access-list 102 deny ip 10.0.0.0 0.0.0.255 50.0.0.0 0.0.0.255
access-list 102 permit ip any any
!
interface Ethernet0
! inside interface
! dot1x configs
!
interface Virtual-Template1
! Deny traffic from going to VPN
 ip access-group 102 in
!
Interface Ethernet1
! outside interface
 crypto map test
```

### Two DHCP Pools

```
ip dhcp pool private
 network 10.0.0.0 255.255.255.0
 default-router 20.0.0.1
 exit
!
ip dhcp pool public
 network 10.0.0.1 255.255.255.0
 default-router 10.0.0.2
 exit
!
crypto isakmp policy 1
 authentication pre-share
!
crypto isakmp key test address address
 crypto ipsec transform-set t1 esp-3des esp-sha-hmac
 mode tunnel
crypto map test 1 ipsec-isakmp
 set peer address
 set transform-set t1
 match address 101
access-list 101 permit ip 10.0.0.0 0.0.0.255 10.10.0.0 0.0.0.255
access-list 102 permit ip 10.0.0.1 0.0.0.255 any
!
interface Ethernet0
!inside interface
```

```

! dot1x configs
!
interface Loopback0
 ip address 10.0.0.3 255.255.255.0
!
interface Virtual-Template1
 ip unnumbered Loopback0
 ip nat inside
!
Interface Ethernet1
! outside interface
 crypto map test
 ip nat outside
!
ip nat inside source list 102 interface Ethernet1 overload

```

## Router Acting As a Supplicant: Example

The following example shows that dot1x module debugging has been turned on. The **show debugging** command output shows that 802.1X interface information has been cleared for all interfaces.

**Router# debug dot1x supplicant**

dot1x supplicant module debugging is on

**Router# show debugging**

dot1x:

dot1x supplicant module debugging is on

```

3w6d: supp_pae_state_transition: Supplicant State Transition: DISCONNECTED -> CONNECTING
3w6d: supp_pae_txStart: << txStart >>: EAPOL-Start to Authenticator
3w6d: dot1x_pakio_send_pak: Zero destination address, sending to multicast
3w6d: dot1x_pakio_send_pak: Sending packet to group PAE address 0180.c200.0003
3w6d: dot1x_pakio_send_pak: Sending packet to address 0180.c200.0003
3w6d: dot1x_start_supp_timer: Started the Timer for client 0000.0000.0000, 30 seconds
3w6d: dot1x_reset_client: sm->state == CONNECTING
3w6d: clear_dot1x_client_supp_table: Clearing all dot1x supplicant instances
3w6d: supp_pae_state_transition: Supplicant State Transition: AUTHENTICATED -> LOGOFF
3w6d: supp_pae_txLogoff: << Router#txLogoff >>: EAPOL-Logoff to Authenticator
3w6d: dot1x_pakio_send_pak: Sending packet to address 000f.23c4.a401
3w6d: dot1x_client_logoff: sm->state == LOGOFF
3w6d: clear_dot1x_client_supp_bucket: Logoff Sent !!
3w6d: dot1x_reset_client: Stopping timers before re-initialization
3w6d: dot1x_reset_client: Re-initializing the default supplicant
3w6d: supp_pae_state_transition: Supplicant State Transition: CONNECTING -> DISCONNECTED
3w6d: supp_pae_state_transition: Supplicant State Transition: DISCONNECTED -> CONNECTING
3w6d: supp_pae_txStart: << txStart >>: EAPOL-Start to Authenticator
3w6d: dot1x_pakio_send_pak: Zero destination address, sending to multicast
3w6d: dot1x_pakio_send_pak: Sending packet to group PAE address 0180.c200.0003
3w6d: dot1x_pakio_send_pak: Sending packet to address 0180.c200.0003
3w6d: dot1x_start_supp_timer: Started the Timer for client 0000.0000.0000, 30 seconds
3w6d: dot1x_reset_client: sm->state == CONNECTING
3w6d: dot1x_get_def_client_supp_entry: Using the default supplicant instance
3w6d: dot1x_input: Stopping timers on the default supp instance
3w6d: dot1x_stop_supp_timer: Stopped the Timer for client 0000.0000.0000
3w6d: dot1x_get_client_supp_entry: Supplicant 000f.23c4.a401 not found in the supplicant
list
3w6d: dot1x_input: Creating a new supplicant entry
3w6d: dot1x_get_supp_config: Using the default EAP method
3w6d: dot1x_pakio_uplink_addr_set: Uplink address set to 00:0F:23:C4:A4:01

```

```

3w6d: dot1x_pakio_init_ios: Initialising common IOS structures for dot1x
3w6d: dot1x_pakio_init_ios: Done.
3w6d: dot1x_eap_init: Initialising EAP method 4
3w6d: dot1x_eap_init: Username:user, password:cisco
3w6d: dot1x_eap_init: sm->state == DISCONNECTED
3w6d: supp_pae_state_transition: Supplicant State Transition: INVALID -> DISCONNECTED
3w6d: supp_pae_state_transition: Supplicant State Transition: DISCONNECTED -> CONNECTING
3w6d: supp_pae_txStart: << txStart >>: EAPOL-Start to Authenticator
3w6d: dot1x_pakio_send_pak: Sending packet to address 000f.23c4.a401
3w6d: dot1x_start_supp_timer: Started the Timer for client 000f.23c4.a401, 30 seconds
3w6d: dot1x_eap_init: sm->state == CONNECTING
3w6d: add_dot1x_client_supp_to_table:
3w6d: dot1x_get_def_client_supp_entry: Using the default supplicant instance000f.23c4.a401
is added to the supplicant list
3w6d: dot1x_input: QUEUE_EVENT (active pkt count tx 0, rx 1, total tx 3, total rx 10)
3w6d: dot1x_input: Stopping timers on the default supp instance
3w6d: dot1x_get_client_supp_entry: Supplicant instance found
3w6d: dot1x_input: Found an existing supplicant entry
3w6d: supp_pae_event_handler: Received packet:
3w6d: supp_pae_state_transition: Supplicant State Transition: CONNECTING -> AQUIRED
3w6d: dot1x_stop_supp_timer: Stopped the Timer for client 000f.23c4.a401
3w6d: supp_pae_txRspId: << txRspId >>: EAPOL-EAP-Response-Id to Authenticator
3w6d: supp_pae_txRspId: ReceivedId is 0x1 and currentId is 0x100
3w6d: dot1x_pakio_send_pak: Sending packet to address 000f.23c4.a401
3w6d: dot1x_start_supp_timer: Started the Timer for client 000f.23c4.a401, 30 seconds
3w6d: dot1x_input: QUEUE_EVENT (active pkt count tx 0, rx 1, total tx 2, total rx 2)
3w6d: supp_pae_event_handler: Received packet:
3w6d: supp_pae_state_transition: Supplicant State Transition: AQUIRED -> AQUIRED
3w6d: dot1x_stop_supp_timer: Stopped the Timer for client 000f.23c4.a401
3w6d: supp_pae_txRspId: << txRspId >>: EAPOL-EAP-Response-Id to Authenticator
3w6d: supp_pae_txRspId: ReceivedId is 0x1 and currentId is 0x1
3w6d: dot1x_pakio_send_pak: Sending packet to address 000f.23c4.a401
3w6d: dot1x_start_supp_timer: Started the Timer for client 000f.23c4.a401, 30 seconds
3w6d: dot1x_input: QUEUE_EVENT (active pkt count tx 0, rx 0, total tx 3, total rx 2)
3w6d: dot1x_get_def_client_supp_entry: Using the default supplicant instance
3w6d: dot1x_input: Stopping timers on the default supp instance
3w6d: dot1x_get_client_supp_entry: Supplicant instance found
3w6d: dot1x_input: Found an existing supplicant entry
3w6d: supp_pae_event_handler: Received packet:
3w6d: supp_pae_state_transition: Supplicant State Transition: AQUIRED -> AUTHENTICATING
3w6d: dot1x_stop_supp_timer: Stopped the Timer for client 000f.23c4.a401
3w6d: supp_pae_txRspAuth: << txRspAuth >>: EAPOL-EAP-Response to Authenticator
3w6d: dot1x_pakio_send_pak: Sending packet to address 000f.23c4.a401
3w6d: dot1x_start_supp_timer: Started the Timer for client 000f.23c4.a401, 30 seconds
3w6d: dot1x_input: QUEUE_EVENT (active pkt count tx 0, rx 0, total tx 4, total rx 3)
3w6d: dot1x_get_def_client_supp_entry: Using the default supplicant instance
3w6d: dot1x_input: Stopping timers on the default supp instance
3w6d: dot1x_get_client_supp_entry: Supplicant instance found
3w6d: dot1x_input: Found an existing supplicant entry
3w6d: supp_pae_event_handler: Received packet:
3w6d: supp_pae_state_transition: Supplicant State Transition: AUTHENTICATING ->
AUTHENTICATED
3w6d: supp_pae_state_transition: Changing IP addr in AUTHENTICATED state
3w6d: supp_pae_state_transition: Stopped client timers
3w6d: dot1x_stop_supp_timer: Stopped the Timer for client 000f.23c4.a401
3w6d: dot1x_input: QUEUE_EVENT (active pkt count tx 0, rx 0, total tx 4, total rx 4)

```

## Additional References

The following sections provide references related to VPN Access Control Using 802.1X Authentication.



## Related Documents

Related Topic	Document Title
Configuring 802.1X port-based authentication	<a href="#">“Configuring IEEE 802.1x Port-Based Authentication”</a> chapter of the <i>Catalyst 3750 Switch Software Configuration Guide</i> , Release 12.2(25)SEC
DHCP	<a href="#">DHCP</a> chapters in the <i>Cisco IOS IP Addressing Services Configuration Guide</i>
IPSec	<a href="#">“Configuring Security for VPNs with IPSec”</a> chapter of the <i>Cisco IOS Security Configuration Guide</i>
RADIUS	<a href="#">“Configuring RADIUS”</a> chapter of the <i>Cisco IOS Security Configuration Guide</i>
Security commands	<a href="#">Cisco IOS Security Command Reference</a>
User lists on a Cisco ACS	<a href="#">User Guide for Cisco Secure ACS for Windows Server Version 3.2.</a>

## Standards

Standards	Title
IEEE 802.1X protocol	—

## MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
RFC-2284	<a href="#">“RFC 2284 (PPP Extensible Authentication Protocol [EAP])”</a> document from <i>The Internet Requests for Comments (RFC) document series</i>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or a Cisco IOS master commands list.

- **aaa authentication dot1x**
- **clear dot1x**
- **clear eap**
- **debug dot1x**
- **debug eap**
- **description (dot1x credentials)**
- **description (identity profile)**
- **device (identity profile)**
- **dot1x control-direction**
- **dot1x credentials**
- **dot1x default**
- **dot1x guest-vlan**
- **dot1x host-mode**
- **dot1x initialize**
- **dot1x max-reauth-req**
- **dot1x max-req**
- **dot1x max-start**
- **dot1x multiple-hosts**
- **dot1x pae**

- **dot1x port-control**
- **dot1x re-authenticate (privileged EXEC)**
- **dot1x reauthentication**
- **dot1x system-auth-control**
- **dot1x timeout**
- **eap**
- **identity profile**
- **macro global**
- **macro name**
- **password (dot1x credentials)**
- **show dot1x**
- **show eap registrations**
- **show eap sessions**
- **show ip igmp snooping**
- **template (identity profile)**
- **username (dot1x credentials)**

## Feature Information for VPN Access Control Using 802.1X Authentication

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



### Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for VPN Access Control Using 802.1X Authentication

Feature Name	Releases	Feature Information
VPN Access Control Using 802.1X Authentication	12.3(2)XA	The VPN Access Control Using 802.1X Authentication feature was introduced. This feature allows enterprise employees to access their enterprise networks from home while allowing other household members to access only the Internet.

**Table 1** Feature Information for VPN Access Control Using 802.1X Authentication (continued)

Feature Name	Releases	Feature Information
VPN Access Control Using 802.1X Authentication	12.3(4)T	This feature was integrated into Cisco IOS Release 12.3(4)T, and the following platform support was added: Cisco 1751, Cisco 2610XM – Cisco 2611XM, Cisco 2620XM – Cisco 2621XM, Cisco 2650XM – Cisco 2651XM, Cisco 2691, Cisco 3640, Cisco 3640A, and Cisco 3660.
802.1X Supplicant Support	12.3(11)T	802.1X supplicant support was added.
Converged 802.1X Authenticator and Converged 802.1X Supplicant Support	12.4(6)T	Converged 802.1X authenticator and converged 802.1X supplicant support was added. (This update is a standardization of Cisco IOS 802.1X commands for various Cisco IOS platforms. This is no change in 802.1X features.)  Affected commands include the following: <b>clear eap</b> , <b>debug dot1x</b> , <b>debug eap</b> , <b>description (dot1x credentials)</b> , <b>dot1x control-direction</b> , <b>dot1x credentials</b> , <b>dot1x default</b> , <b>dot1x host-mode</b> , <b>dot1x max-reauth-req</b> , <b>dot1x max-start</b> , <b>dot1x multiple-hosts</b> , <b>dot1x timeout</b> , <b>eap</b> , <b>identity profile</b> , <b>password (dot1x credentials)</b> , <b>show eap registrations</b> , <b>show eap sessions</b> , and <b>username</b>
VPN Access Control Using 802.1X Authentication	12.4(4)XC	Various 802.1X commands were integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.  Affected commands include the following: <b>dot1x control-direction</b> , <b>dot1x default</b> , <b>dot1x guest-vlan</b> , <b>dot1x host-mode</b> , <b>dot1x max-reauth-req</b> , <b>dot1x max-req</b> , <b>dot1x max-start</b> , <b>dot1x pae</b> , <b>dot1x port-control</b> , <b>dot1x re-authenticate (privileged EXEC)</b> , <b>dot1x reauthentication</b> , <b>dot1x system-auth-control</b> , <b>dot1x timeout</b> , <b>macro global</b> , <b>macro name</b> , and <b>show ip igmp snooping</b>

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007-2008 Cisco Systems, Inc. All rights reserved.



## **SSL VPN**





# SSL VPN

---

**First Published: February 27, 2006**

**Last Updated: July 11, 2008**

The SSL VPN feature (also known as WebVPN) provides support, in Cisco IOS software, for remote user access to enterprise networks from anywhere on the Internet. Remote access is provided through a Secure Socket Layer- (SSL-) enabled SSL VPN gateway. The SSL VPN gateway allows remote users to establish a secure Virtual Private Network (VPN) tunnel using a web browser. This feature provides a comprehensive solution that allows easy access to a broad range of web resources and web-enabled applications using native HTTP over SSL (HTTPS) browser support. SSL VPN delivers three modes of SSL VPN access: clientless, thin-client, and full-tunnel client support.

This document is primarily for system administrators. If you are a remote user, see the document *SSL VPN Remote User Guide*.



## Note

The Cisco AnyConnect VPN Client is introduced in Cisco IOS Release 12.4(15)T. This feature is the next-generation SSL VPN Client. If you are using Cisco software before Cisco IOS Release 12.4(15)T, you should be using SSL VPN Client and see GUI for the SSL VPN Client when you are web browsing. However, if you are using Cisco software Release 12.4(15)T or later, you should be using Cisco AnyConnect VPN Client and see GUI for Cisco AnyConnect VPN Client when you are web browsing.

For “What’s New” information about SSL VPN features by release, see the section “[Finding Feature Information in This Module](#),” which follows.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for SSL VPN](#)” section on page 104.

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007–2008 Cisco Systems, Inc. All rights reserved.

# Contents

- [Prerequisites for SSL VPN, page 2](#)
- [Restrictions for SSL VPN, page 3](#)
- [Information About SSL VPN, page 4](#)
- [How to Configure SSL VPN Services on a Router, page 26](#)
- [Configuration Examples for SSL VPN, page 84](#)
- [Additional References, page 100](#)
- [Command Reference, page 101](#)
- [Feature Information for SSL VPN, page 104](#)
- [Notices, page 110](#)

## Prerequisites for SSL VPN

- To securely access resources on a private network behind an SSL VPN gateway, the remote user of an SSL VPN service must have the following:
  - An account (login name and password)
  - An SSL-enabled browser (for example, Internet Explorer, Netscape, Mozilla, or FireFox)
  - Operating system support




---

**Note** Later versions of the following software are also supported.

---

- Microsoft Windows 2000, Windows XP, or Windows Vista
- Macintosh OS X 10.4.6
- Linux (Redhat RHEL 3.0 +, FEDORA 5, or FEDORA 6)
- SSL VPN-supported browser—The following browsers have been verified for SSL VPN. Other browsers might not fully support SSL VPN features.




---

**Note** Later versions of the following software are also supported.

---

- Internet Explorer 6.0 or 7.0
- Firefox 2.0 (Windows and Linux)
- Safari 2.0.3
- “Thin Client” support used for TCP port-forwarding applications requires administrative privileges on the computer of the remote user.
- “Tunnel mode” for Cisco SSL VPN requires administrative privileges for initial installation of the full tunnel client.
- The remote user must have local administrative privileges to use thin client or full tunnel client features.



- The SSL VPN gateway and context configuration must be completed before a remote user can access resources on a private network behind an SSL VPN. This configuration is shown in the section “[How to Configure SSL VPN Services on a Router](#).”

**ACL Support**

- Before configuring this feature, the time range should have already been configured.

**Single SignOn (SSO) Netegrity Cookie Support**

- A Cisco plug-in must be installed on a Netegrity SiteMinder server.

## Restrictions for SSL VPN

- URLs referred by the Macromedia Flash player cannot be modified for secure retrieval by the SSL VPN gateway.

**Cisco AnyConnect VPN Client**

CiscoAnyConnect VPN Client does not support the following:

- Datagram Transport Layer Security (DTLS) with SSL connections
- Standalone Mode (Cisco IOS Release 12.4(20)T and later versions)
- IPsec
- IPv6 VPN access
- Compression support
- Language translation (localization)
- Client-side authentication
- Adaptive Security Appliance (ASA) and Adaptive Security Device Manager (ASDM) and any command-line interface (CLI) associated with them
- Adjusting Maximum Transmission Unit (MTU) size
- Sequencing

**Thin Client Control List Support**

- Although there is no limitation on the maximum number of filtering rules that can be applied for each access control list (ACL) entry, keeping the number below 50 should have no impact on router performance.

**HTTP Proxy**

- This feature works only with Microsoft Internet Explorer.
- This feature will not work if the browser proxy setup cannot be modified because of any security policies that have been placed on the client workstation.

# Information About SSL VPN

To configure SSL VPN, you should understand the following concepts:

- [SSL VPN Overview, page 4](#)
- [Modes of Remote Access, page 5](#)
- [SSL VPN Features, page 10](#)
- [Other SSL VPN Features, page 23](#)
- [Platform Support, page 26](#)

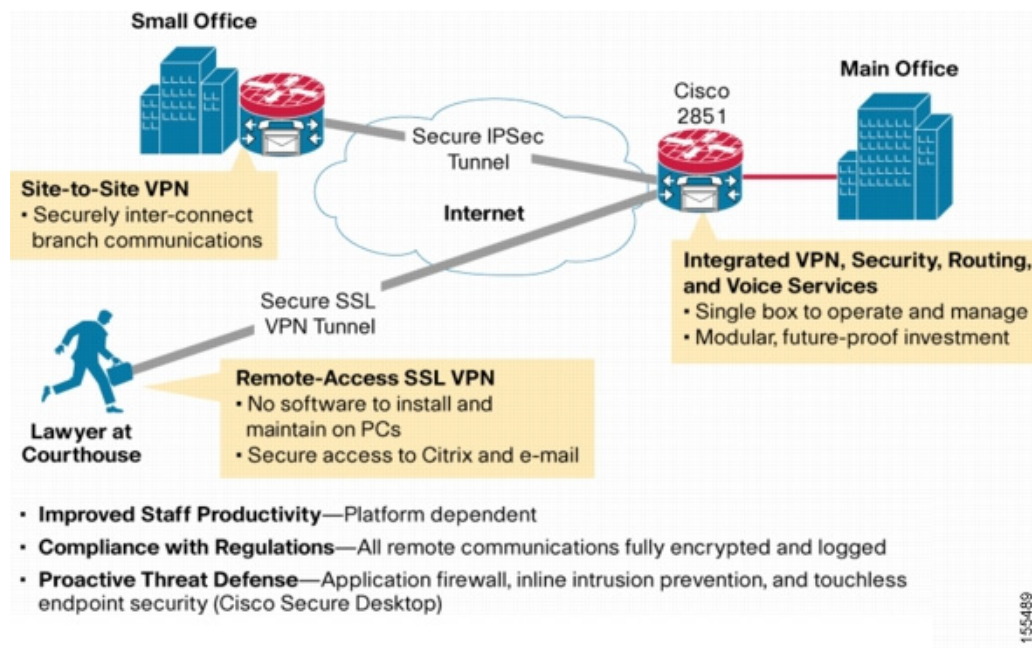
## SSL VPN Overview

Cisco IOS SSL VPN provides SSL VPN remote-access connectivity from almost any Internet-enabled location using only a web browser that natively supports SSL encryption. This feature allows your company to extend access to its secure enterprise network to any authorized user by providing remote-access connectivity to corporate resources from any Internet-enabled location.

Cisco IOS SSL VPN can also support access from noncorporate-owned machines, including home computers, Internet kiosks, and wireless hot spots. These locations are difficult places to deploy and manage VPN client software and remote configuration required to support IPsec VPN connections.

[Figure 1](#) shows how a mobile worker (the lawyer at the courthouse) can access protected resources from the main office and branch offices. Site-to-site IPsec connectivity between the main and remote sites is unaltered. The mobile worker needs only Internet access and supported software (web browser and operating system) to securely access the corporate network.

**Figure 1** *Secure SSL VPN Access Model*



SSL VPN delivers the following three modes of SSL VPN access:

- *Clientless*—Clientless mode provides secure access to private web resources and will provide access to web content. This mode is useful for accessing most content that you would expect to access in a web browser, such as Internet access, databases, and online tools that employ a web interface.
- *Thin Client* (port-forwarding Java applet)—Thin client mode extends the capability of the cryptographic functions of the web browser to enable remote access to TCP-based applications such as Post Office Protocol version 3 (POP3), Simple Mail Transfer Protocol (SMTP), Internet Message Access protocol (IMAP), Telnet, and Secure Shell (SSH).
- *Tunnel Mode*—Full tunnel client mode offers extensive application support through its dynamically downloaded Cisco AnyConnect VPN Client (next-generation SSL VPN Client) for SSL VPN. Full tunnel client mode delivers a lightweight, centrally configured and easy-to-support SSL VPN tunneling client that provides network layer access to virtually any application.

SSL VPN application accessibility is somewhat constrained relative to IPsec VPNs; however, SSL-based VPNs provide access to a growing set of common software applications, including web page access, web-enabled services such as file access, e-mail, and TCP-based applications (by way of a downloadable thin-client applet). SSL-based VPN requires slight changes to user workflow because some applications are presented through a web browser interface, not through their native GUI. The advantage for SSL VPN comes from accessibility from almost any Internet-connected system without needing to install additional desktop software.

## Modes of Remote Access

This section includes the following:

- [Remote Access Overview, page 5](#)
- [Clientless Mode, page 6](#)
- [Thin-Client Mode, page 7](#)
- [Tunnel Mode, page 9](#)

## Remote Access Overview

End-user login and authentication is performed by the web browser to the secure gateway using an HTTP request. This process creates a session that is referenced by a cookie. After authentication, the remote user is shown a portal page that allows access to the SSL VPN networks. All requests sent by the browser include the authentication cookie. The portal page provides all the resources available on the internal networks. For example, the portal page could provide a link to allow the remote user to download and install a thin-client Java applet (for TCP port forwarding) or a tunneling client.

[Figure 2](#) shows an overview of the remote access modes.

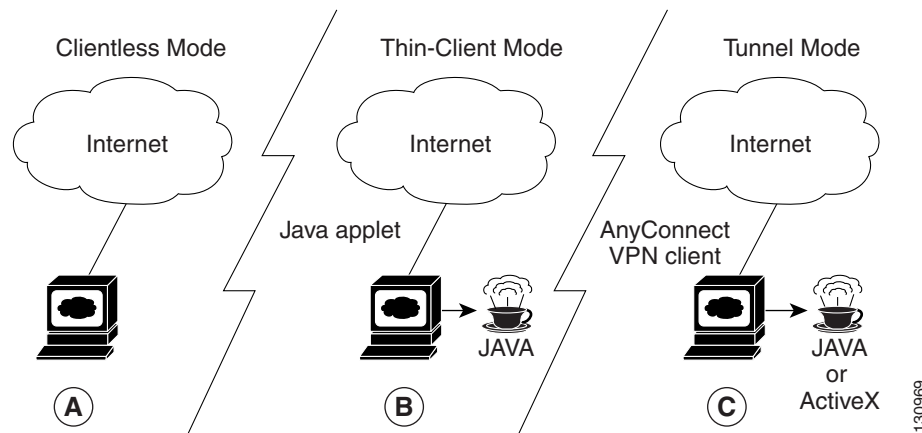
**Figure 2** *Modes of Remote Access Overview*

Table 1 summarizes the level of SSL VPN support that is provided by each access mode.

**Table 1** *Access Mode Summary*

A Clientless Mode	B Thin-Client Mode	C Tunnel Mode
<ul style="list-style-type: none"> <li>• Browser-based (clientless)</li> <li>• Microsoft Windows or Linux</li> <li>• Web-enabled applications, file sharing, Outlook Web Access</li> <li>• Gateway performs address or protocol conversion and content parsing and rewriting</li> </ul>	<ul style="list-style-type: none"> <li>• TCP port forwarding</li> <li>• Uses Java Applet</li> <li>• Extends application support</li> <li>• Telnet, e-mail, SSH, Meeting Maker, Sametime Connect</li> <li>• Static port-based applications</li> </ul>	<ul style="list-style-type: none"> <li>• Works like “clientless” IPsec VPN</li> <li>• Tunnel client loaded through Java or ActiveX (approximately 500 kB)</li> <li>• Application agnostic—supports all IP-based applications</li> <li>• Scalable</li> <li>• Local administrative permissions required for installation</li> </ul>

## Clientless Mode

In clientless mode, the remote user accesses the internal or corporate network using the web browser on the client machine. The PC of the remote user must run the Windows 2000, Windows XP, or Linux operating systems.

The following applications are supported in clientless mode:

- Web browsing (using HTTP and secure HTTP [HTTPS])—provides a URL box and a list of web server links in the portal page that allows the remote user to browse the web.
- File sharing (using common Internet file system [CIFS])—provides a list of file server links in the portal page that allows the remote user to do the following operations:
  - Browse a network (listing of domains)
  - Browse a domain (listing of servers)
  - Browse a server (listing of shares)
  - List the files in a share
  - Create a new file

- Create a directory
- Rename a directory
- Update a file
- Download a file
- Remove a file
- Rename a file

**Note**

Linux requires that the Samba application is installed before CIFS file shares can be remotely accessed.

- Web-based e-mail, such as Microsoft Outlook Web Access (OWA) 2003 (using HTTP and HTTPS) with Web Distributed Authoring and Versioning (WebDAV) extensions—provides a link that allows the remote user to connect to the exchange server and read web-based e-mail.

## Thin-Client Mode

Thin-client mode, also called TCP port forwarding, assumes that the client application uses TCP to connect to a well-known server and port. In thin-client mode, the remote user downloads a Java applet by clicking the link provided on the portal page, or the Java applet is downloaded automatically (see [“Options for Configuring HTTP Proxy and the Portal Page”](#) and [“Options for Configuring HTTP Proxy and the Portal Page”](#)). The Java applet acts as a TCP proxy on the client machine for the services that you configure on the gateway.

The applications that are supported in thin-client mode are mainly e-mail-based (SMTP, POP3, and Internet Map Access Protocol version 4 [IMAP4] applications).

**Note**

The TCP port-forwarding proxy works only with the Sun Microsystems Java Runtime Environment (JRE) version 1.4 or later versions. A Java applet is loaded through the browser that verifies the JRE version. The Java applet will refuse to run if a compatible JRE version is not detected.

The Java applet initiates an HTTP request from the remote user client to the SSL VPN gateway. The name and port number of the internal e-mail server is included in the HTTP request (POST or CONNECT). The SSL VPN gateway creates a TCP connection to that internal e-mail server and port.

The Java applet starts a new SSL connection for every client connection.

You should observe the following restrictions when using thin-client mode:

- The remote user must allow the Java applet to download and install.
- You cannot use thin-client mode for applications such as FTP, where the ports are negotiated dynamically. You can use TCP port forwarding only with static ports.

**Note**

There is a known compatibility issue with the encryption type and Java. If the Java port-forwarding applet does not download properly and the configuration line **ssl encryption 3des-sha1 aes-sha1** is present, you should remove the line from the webvpn gateway subconfiguration.

## Options for Configuring HTTP Proxy and the Portal Page

Effective with Cisco IOS Release 12.4(11)T, administrators have more options for configuring the HTTP proxy and the portal page. If HTTP proxy is enabled, the Java applet acts as the proxy for the browser of the user, thereby connecting the client workstation with the gateway. The home page of the user (as defined by the user group) is opened automatically or, if configured by the administrator, the user is directed to a new website.

HTTP proxy supports both HTTP and HTTPS.

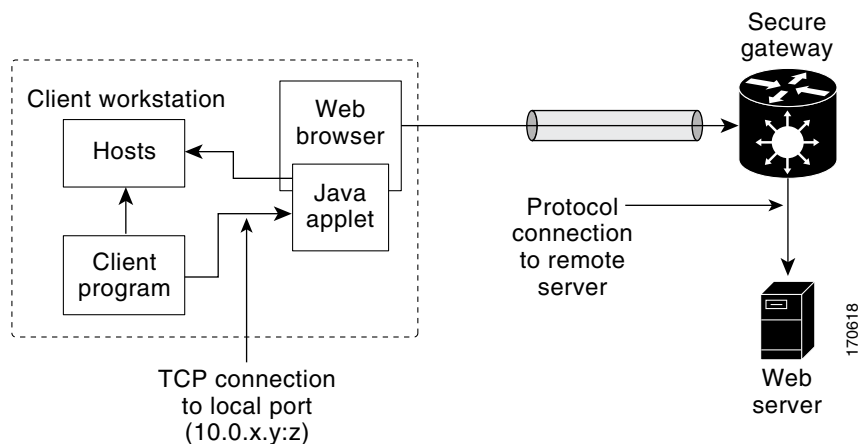
### Benefits of Configuring HTTP Proxy

HTTP supports all client-side web technologies (including HTML, Cascading Style Sheets [CSS], JavaScript, VBScript, ActiveX, Java, and flash), HTTP Digest authentication, and client certificate authentication. Remote users can use their own bookmarks, and there is no limit on cookies. Because there is no mangling involved and the client can cache the objects, performance is much improved over previous options for configuring the HTTP proxy and portal page.

### Illustrations of Port Forwarding with and Without an HTTP Proxy Configuration

Figure 3 illustrates TCP port forwarding without HTTP proxy configured.

**Figure 3** TCP Port Forwarding Without HTTP Proxy Configured



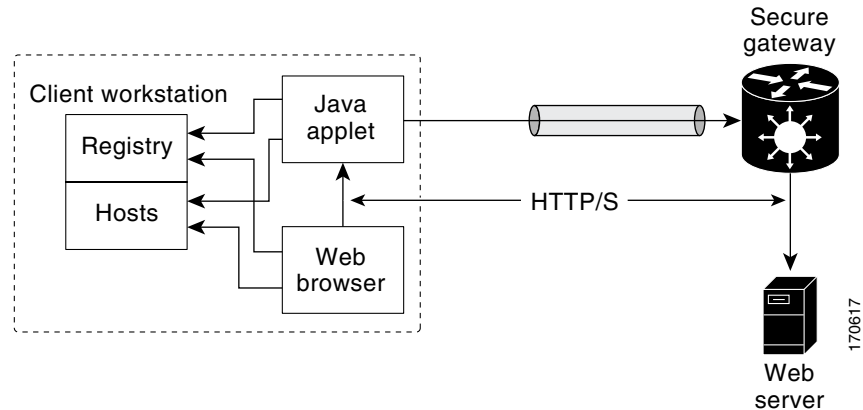
In Figure 3, the following steps must occur:

1. User downloads the proxy applet.
2. Applet updates the registry to add HTTP as a Remote Procedure Call (RPC) transport.
3. Applet examines the registry to determine the exchange (and local catalog) server and create server entries that refer to those servers.
4. Applet opens local port 80 and listens for connections.
5. User starts Outlook, and Outlook connects to 10.0.0.254:80.
6. Applet opens a connection to the secure gateway and delivers the requests from Outlook.
7. Secure gateway examines the requests to determine the end-point exchange server.
8. Data flows from Outlook, through the applet and the secure gateway, to the exchange server.
9. User terminates Outlook.

10. User closes the applet. Before closing, the applet undoes configuration Steps 3 and 4.

Figure 4 illustrates TCP port forwarding when HTTP proxy is configured.

**Figure 4** HTTP Proxy



In Figure 4, the following steps occur:

1. Proxy applet is downloaded automatically.
2. Applet saves the original proxy configuration of the browser.
3. Applet updates the proxy configuration of the browser to be the local loopback address with an available local port (by default, port 8080).
4. Applet opens the available local port and listens for connections.
5. Applet, if so configured, opens the home page of the user, or the user browses to a new website.
6. Applet accepts and looks at the HTTP or HTTPS request to determine the destination web server.
7. Applet opens a connection to the secure gateway and delivers the requests from the browser.
8. Secure gateway examines the requests to determine the end-point web server.
9. Data flows from the browser, through the applet and the secure gateway, to the web server.
10. User closes applet. Before closing, the applet undoes configuration Steps 2 and 3.



**Note**

HTTP proxy can also be enabled on a AAA server. See the section “[SSL VPN RADIUS Attribute-Value Pairs](#)” (port-forward-http-proxy and port-forward-http-proxy-url attributes).

## Tunnel Mode

In a typical clientless remote access scenario, remote users establish an SSL tunnel to move data to and from the internal networks at the application layer (for example, web and e-mail). In tunnel mode, remote users use an SSL tunnel to move data at the network (IP) layer. Therefore, tunnel mode supports most IP-based applications. Tunnel mode supports many popular corporate applications (for example, Microsoft Outlook, Microsoft Exchange, Lotus Notes E-mail, and Telnet).

The tunnel connection is determined by the group policy configuration. The Cisco AnyConnect VPN Client is downloaded and installed on the remote user PC, and the tunnel connection is established when the remote user logs into the SSL VPN gateway.

By default, the Cisco AnyConnect VPN Client is removed from the client PC after the connection is closed. However, you have the option to keep the Cisco AnyConnect VPN Client installed on the client PC.

## SSL VPN Features

SSL VPN includes the following features:

- [Access Control Enhancements, page 10](#)
- [AnyConnect Client Support, page 10](#)
- [Application ACL Support, page 11](#)
- [Automatic Applet Download, page 11](#)
- [Backend HTTP Proxy, page 11](#)
- [Front-Door VRF Support, page 11](#)
- [Full-Tunnel CEF Support, page 12](#)
- [GUI Enhancements, page 12](#)
- [Netegrity Cookie-Based Single SignOn Support, page 18](#)
- [NTLM Authentication, page 18](#)
- [RADIUS Accounting, page 18](#)
- [Stateless High Availability with Hot Standby Router Protocol, page 19](#)
- [TCP Port Forwarding and Thin Client, page 20](#)
- [URL Obfuscation, page 22](#)
- [URL Rewrite Splitter, page 22](#)
- [User-Level Bookmarking, page 22](#)

### Access Control Enhancements

Effective with Cisco IOS Release 12.4(20)T, administrators can configure automatic authentication and authorization for users. Users provide their usernames and passwords via the gateway page URL and do not have to reenter their usernames and passwords from the login page. Authorization is enhanced to support more generic authorization, including local authorization. In previous releases, only RADIUS authorization was supported.

For information about configuring this feature, see the section “[Configuring Automatic Authentication and Authorization](#).”

### AnyConnect Client Support

Effective with Cisco IOS Release 12.4(20)T, AnyConnect Client support has been added for several client-side platforms, such as Microsoft Windows, Apple-Mac, and Linux. The ability to install AnyConnect in a standalone mode is also added. In addition, the Release 12.4(20)T allows you to install multiple AnyConnect VPN client packages to a gateway. For information on configuring multiple packages, see the section “[Configuring the SSL VPN Gateway to Distribute CSD and Cisco AnyConnect VPN Client Package Files](#).”



## Application ACL Support

Effective with Cisco IOS Release 12.4(11)T, this feature provides administrators with the flexibility to fine-tune access control on the application layer level, for example, on the basis of a URL.

For information about configuring this feature, see the sections “[Configuring ACL Rules](#)” and “[Associating an ACL Attribute with a Policy Group](#).”

## Automatic Applet Download

Effective with Cisco IOS Release 12.4(9)T, administrators have the option of automatically downloading the port-forwarding Java applet. This feature must be configured on a group policy basis.

**Note**

Users still have to allow the Java applet to be downloaded. The dialog box pops up, asking for permission.

To configure the automatic download, see the section “[Configuring an SSL VPN Policy Group](#).”

## Backend HTTP Proxy

This feature, added in Cisco IOS Release 12.4(20)T, allows administrators to route user requests through a backend HTTP proxy, providing more flexibility and controllability than routing requests through internal web servers. This feature adds the following new authentication, authorization, and accounting (AAA) attributes:

```
http-proxy-server
http-proxy-server-port
```

For information about configuring this feature, see the section “[Configuring a Backend HTTP Proxy](#).”

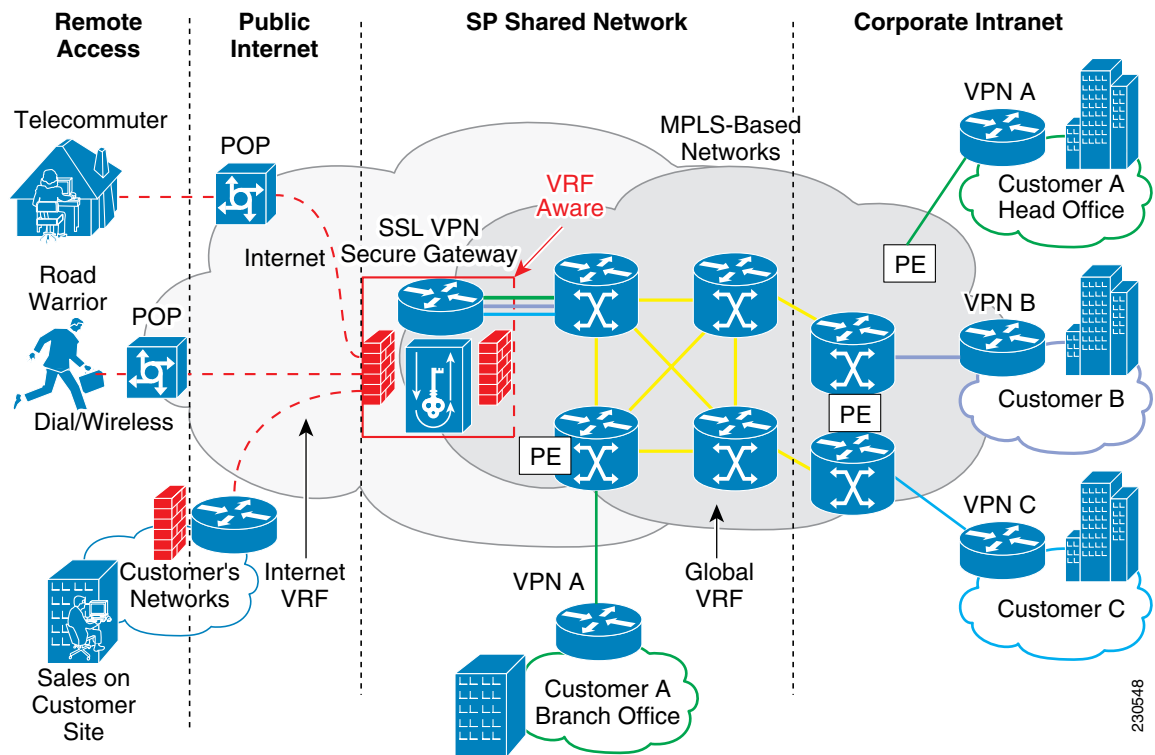
## Front-Door VRF Support

Effective with Cisco IOS Release 12.4(15)T, front-door virtual routing and forwarding (FVRF) support, coupled with the already supported internal virtual routing and forwarding (IVRF), provides for increased security. The feature allows the SSL VPN gateway to be fully integrated into a Multiprotocol Label Switching (MPLS) or non-MPLS network (wherever the VRFs are deployed). The virtual gateway can be placed into a VRF that is separate from the Internet to avoid internal MPLS and IP network exposure. This placement reduces the vulnerability of the router by separating the Internet routes or the global routing table. Clients can now reach the gateway by way of the FVRF, which can be separate from the global VRF. The backend, or IVRF, functionality remains the same.

This FVRF feature provides for overlapping IP addresses.

[Figure 5](#) is a scenario in which FVRF has been applied.

**Figure 5** Scenario in Which FVRF Has Been Applied



To configure FVRF, see [“Configuring FVRF” section on page 75](#).

## Full-Tunnel CEF Support

Effective with Cisco IOS Release 12.4(20)T, Full-Tunnel Cisco Express Forwarding (CEF) support has been added for better throughput performance than in earlier releases. This feature is enabled by default. To turn off full-tunnel CEF support, use the **no webvpn cef** command.



### Note

To take full advantage of CEF support, the hardware crypto engine is required.

For an example of output showing CEF-processed packets, see the section [“CEF-Processed Packets: Example, page 90.”](#)

## GUI Enhancements

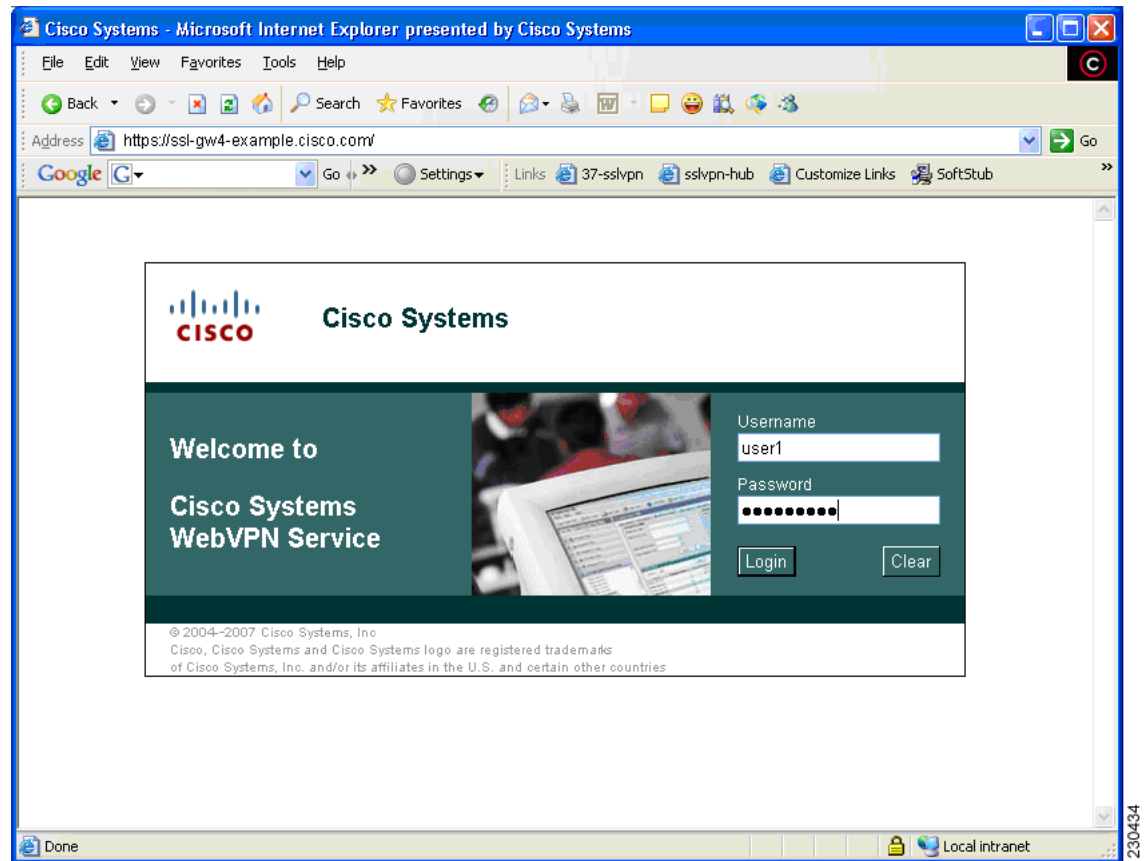
In Cisco IOS Release 12.4(15)T, ergonomic improvements were made to the GUI user interface of the Cisco IOS SSL VPN gateway. The improved customization of the user interface provides for greater flexibility and the ability to tailor portal pages for individualized looks. Enhancements were made to the following web screens:

- Login screen
- Portal page

## Login Screen

Figure 6 is an example of a typical login screen.

**Figure 6** Typical Login Screen



## Banner

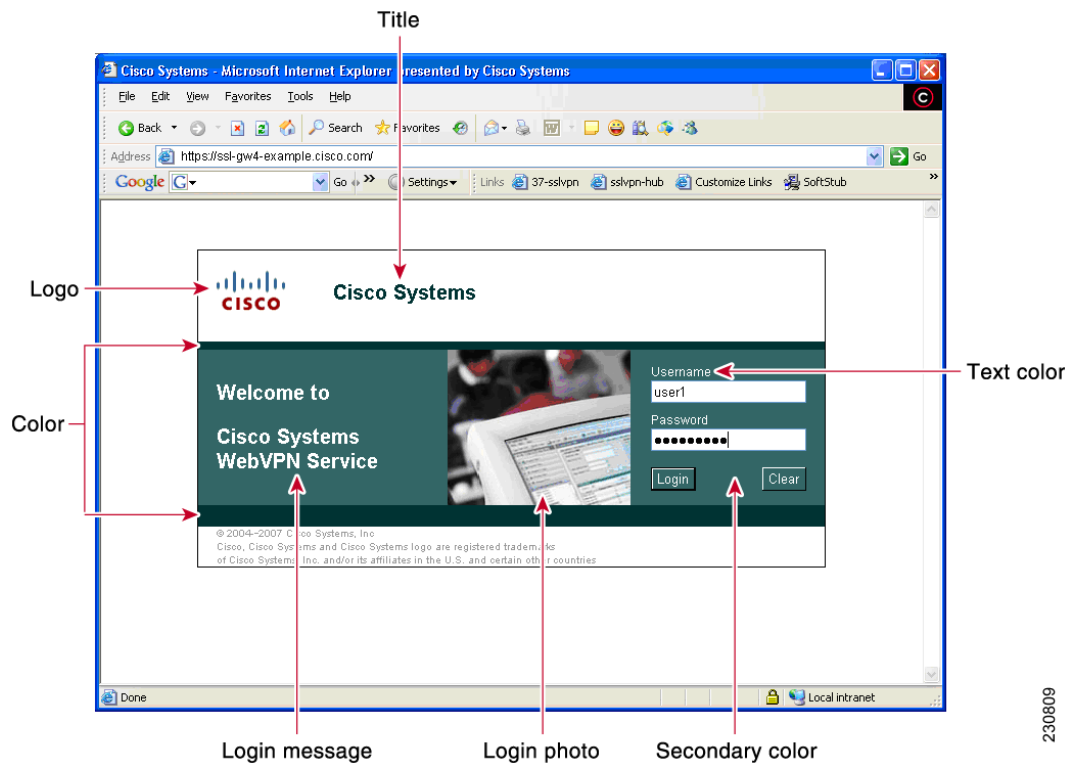
The banner is a small pop-up box (see Figure 7) that appears after the user is logged in and before the portal page appears.

The message in the pop-up box is configured using the **banner** command.

**Figure 7**      **Banner**

## Customizing a Login Page

Login screens can be customized by an administrator. [Figure 8](#) shows the fields that can be customized. For information about setting various elements of the login page, see the document [Cisco IOS Security Command Reference](#), Release 12.4T, for the `logo`, `title`, `title-color`, `login-message`, `text-color`, `secondary-color`, `login-photo`, and `color` commands.

**Figure 8**      **Login Page with Callouts of the Fields That Can Be Customized**

230809

## Portal Page

The portal page ([Figure 9](#)) is the main page for the SSL VPN functionality. You can customize this page to contain the following:

- Custom logo (the default is the Cisco bridge logo)
- Custom title (the default is “WebVPN Services”)
- Custom banner (the default is an empty string)
- Custom colors (the default is a combination of white and greens)
- List of web server links (can be customized)



---

**Note** The Bookmark links are listed under the Personal folder, and the server links are listed under Network File in [Figure 9](#).

---

- URL entry box (may be present or can be hidden using the **hide-url-bar** command)
- Thin Client link (may or may not be present)



---

**Note** The Application Access box allows you to download and install the Tunnel Connection and Thin Client Application.

---

- Links for Help, Home (that is, the portal page), and Logout

Items that you have not configured are not displayed on the portal page.



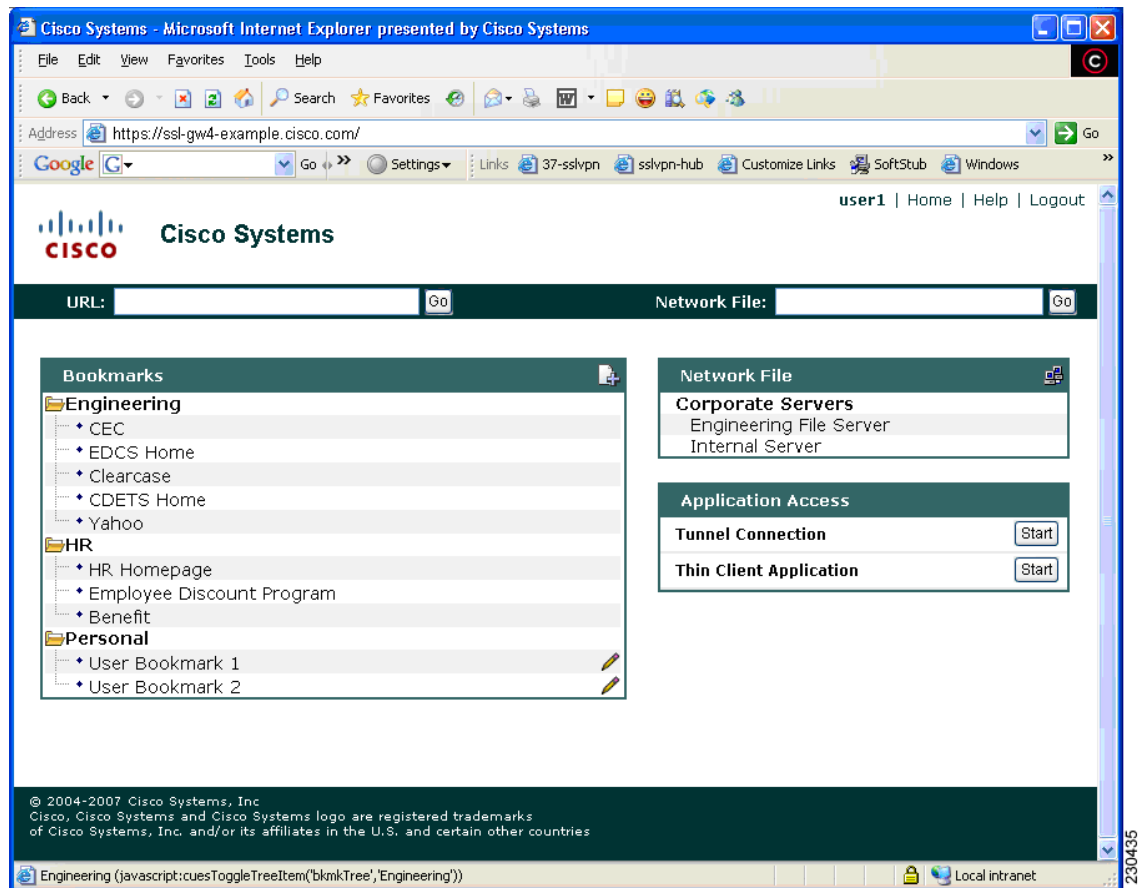
---

**Note** E-mail access is supported by thin-client mode, which is downloaded using the Thin Client link.

---

[Figure 9](#) is an example of a typical portal page.

**Figure 9** Typical Portal Page



### Customizing a Portal Page

Portal pages can be customized by an administrator. Figure 10 shows various fields, including the fields that can be customized by an administrator. The fields that can be customized by an administrator are as follows:

- Title
- Logo
- Secondary color
- Administrator-defined bookmarks
- Color

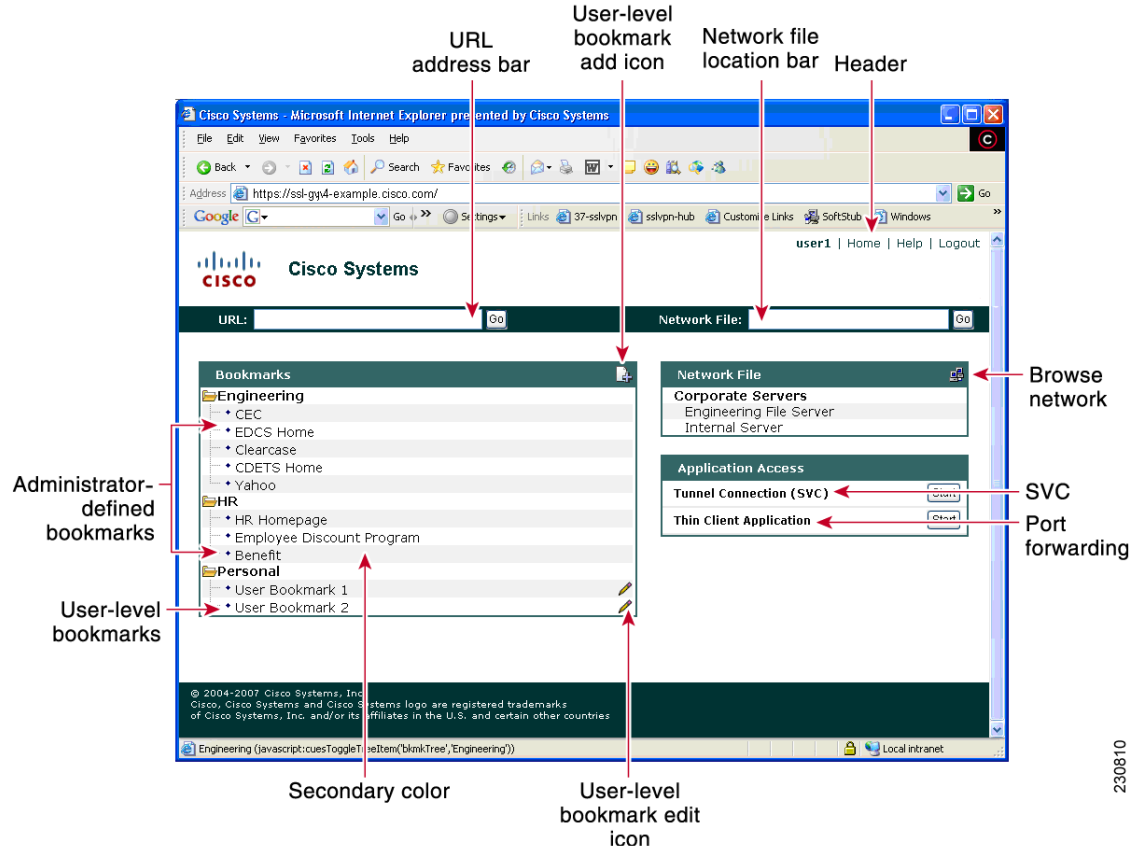

**Figure 10** Portal Page with Callouts of Various Fields, Including Those That Can Be Customized

Table 2 provides information about various fields on the portal page. For information about setting elements such as color or titles, see command information in the [Cisco IOS Security Command Reference](#), Release 12.4T, for the **logo**, **title**, **title-color**, **functions**, **port-forward**, **color**, **secondary-text-color**, **url-list**, **secondary-color**, and **hide-url-bar** commands.

**Table 2** Information About Fields on the Portal Page

Field	Description
User-level bookmark add icon	If a user clicks it, a dialog box is added so that a new bookmark can be added to the Personal folder.
Network File location bar	A user can enter the file server here. Both of the <b>functions file-access</b> and <b>functions file-entry</b> commands must be configured for the input box to appear.
Header	Shares the same color value as the title.
Last login	Timestamp of the last login.
Browse network	Allows a user to browse the file network. Both commands <b>functions file-access</b> and <b>functions file-browse</b> must be configured for the icon to appear.
Tunnel Connection	A user can choose when to start the tunnel connection by configuring the <b>functions svc-enabled</b> command.

**Table 2**      **Information About Fields on the Portal Page (continued)**

Field	Description
Port forwarding	Downloads the applet and starts port forwarding.
User-level bookmark edit icon	Allows a user to edit or delete an existing bookmark.
User-level bookmarks	<p>A user can add a bookmark by using the plus icon (see below)</p>  <p>on the bookmark panel or toolbar. See the document <i>SSL VPN Remote User Guide</i> for information about the toolbar. A new window is opened when the link is clicked.</p>
Administrator-defined bookmarks	Administrator-defined URL lists cannot be edited by the user.
URL address bar	A new window is opened when a user clicks Go.

## Netegrity Cookie-Based Single SignOn Support

The Netegrity SiteMinder product provides a Single SignOn (SSO) feature that allows a user to log on a single time for various web applications. The benefit of this feature is that users are prompted to log on only once. This feature is accomplished by setting a cookie in the browser of a user when the user initially logs on.

Effective with Cisco IOS Release 12.4(11)T, Netegrity cookie-based SSO is integrated with SSL VPN. It allows administrators to configure an SSO server that sets a SiteMinder cookie in the browser of a user when the user initially logs on. This cookie is validated by a SiteMinder agent on subsequent user requests to resources that are protected by a SiteMinder realm. The agent decrypts the cookie and verifies whether the user has already been authenticated.

For information about configuring SSO Netegrity Cookie Support and associating it with a policy group using the CLI, see the sections “[Configuring SSO Netegrity Cookie Support for a Virtual Context](#)” and “[Associating an SSO Server with a Policy Group](#),” respectively.

An SSO server can also be associated with a policy group using RADIUS attributes, as in the following example:

```
webvpn:sso-server-name=server1
```

For a list of RADIUS attribute-value (AV) pairs that support SSL VPN, see the section “[Configuring RADIUS Attribute Support for SSL VPN](#).”

## NTLM Authentication

NT LAN Manager (NTLM) is supported for SSL VPN effective with Cisco IOS Release 12.4(9)T. The feature is configured by default.

## RADIUS Accounting

Effective with Cisco IOS Release 12.4(9)T, this feature provides for RADIUS accounting of SSL VPN user sessions.



For information about configuring SSL VPN RADIUS accounting for SSL VPN user sessions, see the section “[Configuring RADIUS Accounting for SSL VPN User Sessions](#).”

For more information about configuring RADIUS accounting, see the “Configuring RADIUS” chapter in the *Cisco IOS Security Configuration Guide*, Release 12.4 at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsec\\_c/part10/ch05/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsec_c/part10/ch05/index.htm)

For a list of RADIUS AV pairs that support SSL VPN, see the section “[Configuring RADIUS Attribute Support for SSL VPN](#).”

## Stateless High Availability with Hot Standby Router Protocol

Hot Standby Router Protocol (HSRP) provides high network availability by routing IP traffic from hosts on ethernet networks without having to rely on the availability of any single router. HSRP is particularly useful for hosts that do not support a router discovery protocol, such as ICMP Router Discovery Protocol (IRDP), and that do not have the functionality to switch to a new router when their selected router reloads or loses power. Without this functionality, a router that loses its default gateway because of a router failure is unable to communicate with the network.

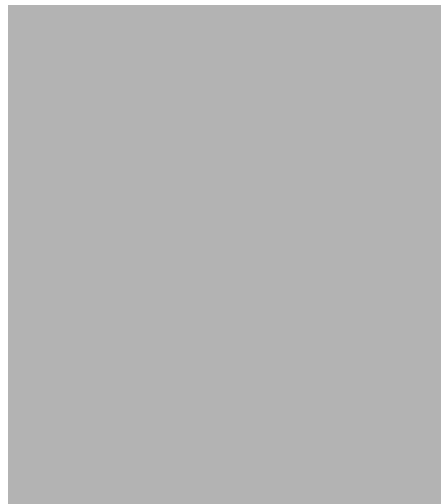
HSRP is configurable on LAN interfaces using standby command-line interface (CLI). It is now possible to use the standby IP address from an interface as the local IPsec identity, or local tunnel endpoint.

By using the standby IP address as the SSL VPN gateway address, failover can be applied to VPN routers by using HSRP. Remote SSLVPN users connect to the local VPN gateway using the standby address that belongs to the active device in the HSRP group. In the event of failover, the standby device takes over ownership of the standby IP address and begins to service remote VPN users.

Using the Stateless High Availability with Hot Standby Router Protocol feature, the remote user has to be aware of only the HSRP standby address instead of a list of gateway addresses.

[Figure 11](#) shows the enhanced HSRP functionality topology. Traffic is serviced by the active Router P, the active device in the standby group. In the event of failover, traffic is diverted to Router S, the original standby device. Router S assumes the role of the new active router and takes ownership of the standby IP address.

**Figure 11**      **Stateless High Availability with HSRP for SSL VPN**



For information about configuring Stateless High Availability with HSRP, see [“Configuring Stateless High Availability with HSRP for SSL VPN” section on page 80.](#)

**Note**

In case of a failover, HSRP does not facilitate SSL VPN state information transference between VPN gateways. Without this state transference, existing SSL VPN sessions with the remote users will be deleted, requiring users to reauthenticate and establish SSL VPN sessions with the new active gateway.

## TCP Port Forwarding and Thin Client

**Note**

This feature requires the JRE version 1.4 or later releases to properly support SSL connections.

**Note**

Because this feature requires installing JRE and configuring the local clients, and because doing so requires administrator permissions on the local system, it is unlikely that remote users will be able to use applications when they connect from public remote systems.

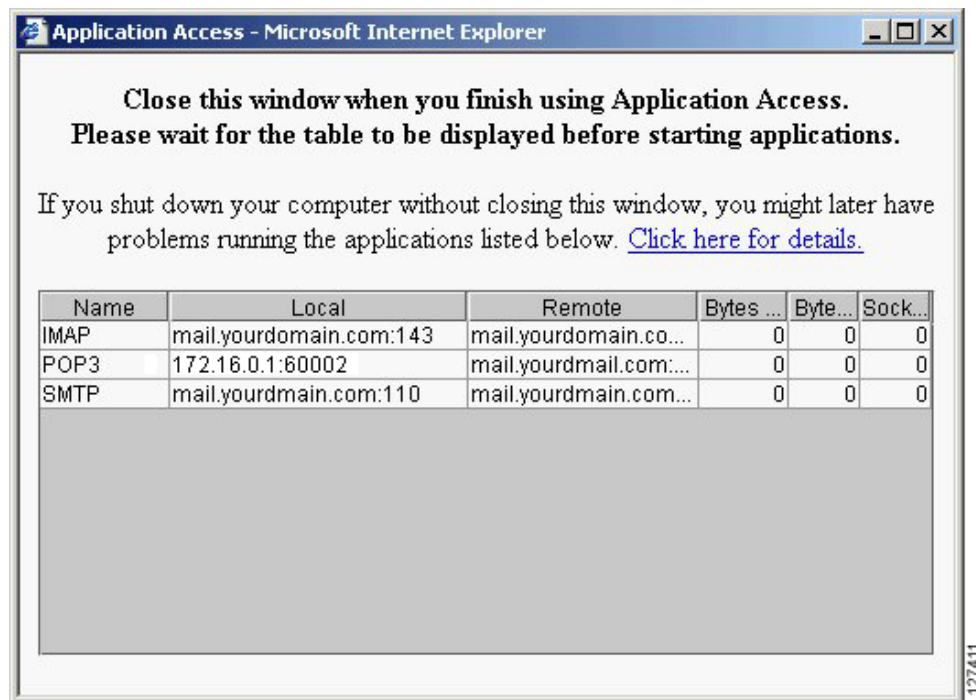
When the remote user clicks the Start button of the Thin Client Application (under “Application Access”), a new window is displayed. This window initiates the downloading of a port-forwarding applet. Another window is then displayed. This window asks the remote user to verify the certificate with which this applet is signed. When the remote user accepts the certificate, the applet starts running, and port-forwarding entries are displayed (see [Figure 12](#)). The number of active connections and bytes that are sent and received is also listed on this window.

**Note**

When remote users launch Thin Client, their system may display a dialog box regarding digital certificates, and this dialog box may appear behind other browser windows. If the remote user connection hangs, tell the remote user to minimize the browser windows to check for this dialog box.

You should have configured IP addresses, Domain Name System (DNS) names, and port numbers for the e-mail servers. The remote user can then launch the e-mail client, which is configured to contact the above e-mail servers and send and receive e-mails. POP3, IMAP, and SMTP protocols are supported.

The window attempts to close automatically if the remote user is logged out using JavaScript. If the session terminated and a new port forwarding connection is established, the applet displays an error message.

**Figure 12** TCP Port Forwarding Page**Caution**

Users should always close the Thin Client window when finished using applications by clicking the close icon. Failure to quit the window properly can cause Thin Client or the applications to be disabled. See the section “Application Access—Recovering from Hosts File Errors” in the document SSL VPN Remote User Guide.

[Table 3](#) lists remote system requirements for Thin Client.

**Table 3** SSL VPN Remote System Thin Client Requirements

Remote User System Requirements	Specifications or Use Suggestions
Client applications installed.	—
Cookies enabled on browser.	—
Administrator privileges.	You must be the local administrator on your PC.
Sun Microsystems JRE version 1.4 or later installed.	SSL VPN automatically checks for JRE whenever the remote user starts Thin Client. If it is necessary to install JRE, a pop-up window displays directing remote users to a site where it is available.

**Table 3**      **SSL VPN Remote System Thin Client Requirements (continued)**

Remote User System Requirements	Specifications or Use Suggestions
<p>Client applications configured, if necessary.</p> <p><b>Note</b>    The Microsoft Outlook client does not require this configuration step.</p>	<p>To configure the client application, use the locally mapped IP address and port number of the server. To find this information, do the following:</p> <ul style="list-style-type: none"> <li>• Start SSL VPN on the remote system and click the Thin Client link on the SSL VPN home page. The Thin Client window is displayed.</li> <li>• In the Name column, find the name of the server that you want to use, and then identify its corresponding client IP address and port number (in the Local column).</li> <li>• Use this IP address and port number to configure the client application. The configuration steps vary for each client application.</li> </ul>
Windows XP SP2 patch.	<p>If you are running Windows XP SP2, you must install a patch from Microsoft that is available at the following address:</p> <p><a href="http://support.microsoft.com/?kbid=884020">http://support.microsoft.com/?kbid=884020</a></p> <p>This problem is a known Microsoft issue.</p>

## URL Obfuscation

The URL Obfuscation feature provides administrators with the ability to obfuscate, or mask, sensitive portions of an enterprise URL, such as IP addresses, hostnames, or part numbers. For example, if URL masking is configured for a user, the URL in the address bar could have the port and hostname portion garbled, as in this example:

`https://slvpn-gateway.examplecompany.com/http/cF9HxnBjRmSFzBWpDtfXfigzL559MQo51Qj/cgi-bin/submit.p`

For information about configuring this feature, see the section “[Associating an SSO Server with a Policy Group](#).”

## URL Rewrite Splitter

Effective with Cisco IOS Release 12.4(20)T, the URL Rewrite Splitter feature allows administrators to mangle selective URLs. Mangling is a CPU-intensive and time-consuming process, so mangling only selective URLs can result in a savings of memory and time.

For information about configuring this feature, see the section “[Configuring a URL Rewrite Splitter](#).”

## User-Level Bookmarking

Effective with Cisco IOS Release 12.4(15)T, users can bookmark URLs while connected through an SSL VPN tunnel. Users can access the bookmarked URLs by clicking the URLs.

User-level bookmarking is turned by default. There is no way to turn it off. To set the storage location, administrators can use the **user-profile location** command. If the **user-profile location** command is not configured, the location `flash:/webvpn/{context name}/` is used.

## Other SSL VPN Features

Table 4 lists the requirements for various SSL VPN features.



**Table 4** *SSL VPN Remote User System Requirements*

Task	Remote User System Requirements	Additional Information
Web Browsing	Username and passwords for protected websites	Users should log out on SSL VPN sessions when they are finished.
		<p>The look and feel of web browsing with SSL VPN might be different from what users are accustomed to. For example, when they are using SSL VPN, the following should be noted:</p> <ul style="list-style-type: none"> <li>• The SSL VPN title bar appears above each web page.</li> <li>• Websites can be accessed as follows: <ul style="list-style-type: none"> <li>– Entering the URL in the Enter Web Address field on the SSL VPN home page</li> <li>– Clicking a preconfigured website link on the SSL VPN home page</li> <li>– Clicking a link on a webpage accessed by one of the previous two methods</li> </ul> </li> </ul> <p>Also, depending on how a particular account was configured, the following might have occurred:</p> <ul style="list-style-type: none"> <li>• Some websites are blocked.</li> <li>• Only the websites that appear as links on the SSL VPN home page are available.</li> </ul>
Network Browsing and File Management	File permissions configured for shared remote access	Only shared folders and files are accessible through SSL VPN.
	Server name and passwords are necessary for protected file servers	
	Domain, workgroup, and server names where folders and files reside	A user might not be familiar with how to locate his or her files through the network of an organization.
	<p><b>Note</b> The user should not interrupt the Copy File to Server operation or navigate to a different window while the copying is in progress. Interrupting this operation can cause an incomplete file to be saved on the server.</p>	

**Table 4**      **SSL VPN Remote User System Requirements (continued)**

Task	Remote User System Requirements	Additional Information
Using e-mail: Thin Client	Same requirements as for Thin Client (see the <a href="#">“TCP Port Forwarding and Thin Client”</a> section on page 20)	To use e-mail, users must start Thin Client from the SSL VPN home page. The e-mail client is then available for use.
	<b>Note</b> If a user is using an IMAP client and loses the e-mail server connection or is unable to make a new connection, the user should close the IMAP application and restart SSL VPN.	
	Other Mail Clients	Microsoft Outlook Express versions 5.5 and 6.0 have been tested.  SSL VPN should support other SMTPS, POP3S, or IMAP4S e-mail programs, such as Netscape Mail, Lotus Notes, and Eudora, but they have not been verified.

**Table 4** *SSL VPN Remote User System Requirements (continued)*

Task	Remote User System Requirements	Additional Information
Using e-mail: Web Access	Web-based e-mail product installed	<p>Supported products are as follows:</p> <ul style="list-style-type: none"> <li>OWA 5.5, 2000, and 2003</li> </ul> <p>Netscape, Mozilla, and Internet Explorer are supported with OWA 5.5 and 2000.</p> <p>Internet Explorer 6.0 or later version is required with OWA 2003. Netscape and Mozilla are supported with OWA 2003.</p> <ul style="list-style-type: none"> <li>Lotus Notes</li> </ul> <p>Operating system support:</p> <p> <b>Note</b> Later versions of the following browsers are also supported.</p> <ul style="list-style-type: none"> <li>Microsoft Windows 2000, Windows XP, or Windows Vista</li> <li>Macintosh OS X 10.4.6</li> <li>Linux (Redhat RHEL 3.0 +, FEDORA 5, or FEDORA 6)</li> </ul> <p>SSL VPN-supported browser:</p> <p>The following browsers have been verified for SSL VPN. Other browsers might not fully support SSL VPN features.</p> <p> <b>Note</b> Later versions of the following software are also supported.</p> <ul style="list-style-type: none"> <li>Internet Explorer 6.0 or 7.0</li> <li>Firefox 2.0 (Windows and Linux)</li> <li>Safari 2.0.3</li> </ul> <p>Other web-based e-mail products should also work, but they have not been verified.</p>
Using the Cisco Tunnel Connection		To retrieve Tunnel Connection log messages using the Windows Event Viewer, go to Program Files > Administrative Tools > Event Viewer in Windows.
Using Secure Desktop Manager	A Secure Desktop Manager-supported browser	<p>On Microsoft Windows:</p> <ul style="list-style-type: none"> <li>Internet Explorer version 6.0 or 7.0</li> <li>Netscape version 7.2</li> </ul> <p>On Linux:</p> <ul style="list-style-type: none"> <li>Netscape version 7.2</li> </ul>

**Table 4** *SSL VPN Remote User System Requirements (continued)*

Task	Remote User System Requirements	Additional Information
Using Cache Cleaner or Secure Desktop	A Cisco Secure Desktop-supported browser	Any browser supported for Secure Desktop Manager.

## Platform Support

For information about platform support for the SSL VPN feature, see the data sheet [Cisco IOS SSL VPN](#) (“Feature Availability” section).

## Licensing

Cisco IOS SSL VPN is a licensed feature available on Cisco routers running the Cisco IOS Advanced Security feature set. Each security bundle entitles you to a certain number of free users. Beyond that, you need to purchase additional feature licenses. For more information about licensing, see the bulletin [Cisco IOS SSL VPN Licensing Information](#).

# How to Configure SSL VPN Services on a Router

This section contains the following tasks and shows whether they are required or optional:

### Configuring and Enabling SSL VPN Services

- [Configuring an SSL VPN Gateway, page 27](#) (required)
- [Configuring a Generic SSL VPN Gateway, page 29](#) (optional)
- [Configuring an SSL VPN Context, page 30](#) (required)
- [Configuring an SSL VPN Policy Group, page 34](#) (required)

### Configuring AAA-Related Features for SSL VPN

- [Configuring Local AAA Authentication for SSL VPN User Sessions, page 37](#) (optional)
- [Configuring AAA for SSL VPN Users Using a Secure Access Control Server, page 38](#) (optional)
- [Configuring RADIUS Accounting for SSL VPN User Sessions, page 40](#) (optional)
- [Monitoring and Maintaining RADIUS Accounting for an SSL VPN Session, page 41](#) (optional)
- [Configuring RADIUS Attribute Support for SSL VPN, page 41](#) (optional)

### Customizing and Enabling SSL VPN Features

- [Configuring a URL List for Clientless Remote Access, page 44](#) (optional)
- [Configuring Microsoft File Shares for Clientless Remote Access, page 46](#) (optional)
- [Configuring Citrix Application Support for Clientless Remote Access, page 49](#) (optional)
- [Configuring Application Port Forwarding, page 50](#) (optional)
- [Configuring the SSL VPN Gateway to Distribute CSD and Cisco AnyConnect VPN Client Package Files, page 53](#) (optional)
- [Configuring Cisco Secure Desktop Support, page 55](#) (optional)



- [Configuring Cisco AnyConnect VPN Client Full Tunnel Support, page 56](#) (optional)
- [Configuring Advanced SSL VPN Tunnel Features, page 61](#) (optional)
- [Configuring VRF Virtualization, page 64](#) (optional)
- [Configuring ACL Rules, page 65](#) (optional)
- [Associating an ACL Attribute with a Policy Group, page 68](#) (optional)
- [Configuring SSO Netegrity Cookie Support for a Virtual Context, page 69](#) (optional)
- [Associating an SSO Server with a Policy Group, page 71](#) (optional)
- [Configuring URL Obfuscation \(Masking\), page 71](#) (optional)
- [Adding a CIFS Server URL List to an SSL VPN Context and Attaching It to a Policy Group, page 72](#) (optional)
- [Configuring User-Level Bookmarks, page 74](#) (optional)
- [Configuring FVRF, page 75](#) (optional)
- [Disabling Full-Tunnel CEF, page 76](#) (optional)
- [Configuring Automatic Authentication and Authorization, page 77](#) (optional)
- [Configuring a URL Rewrite Splitter, page 78](#) (optional)
- [Configuring a Backend HTTP Proxy, page 79](#) (optional)
- [Configuring Stateless High Availability with HSRP for SSL VPN, page 80](#) (optional)

#### Monitoring and Maintaining SSL VPN Features

- [Using SSL VPN Clear Commands, page 81](#) (optional)
- [Verifying SSL VPN Configurations, page 82](#) (optional)
- [Using SSL VPN Debug Commands, page 84](#) (optional)

## Configuring an SSL VPN Gateway

The SSL VPN gateway acts as a proxy for connections to protected resources. Protected resources are accessed through an SSL-encrypted connection between the gateway and a web-enabled browser on a remote device, such as a personal computer. Entering the **webvpn gateway** command places the router in SSL VPN gateway configuration mode. The following are accomplished in this task:

- The gateway is configured with an IP address.
- A port number is configured to carry HTTPS traffic (443 is default).
- A hostname is configured for the gateway.
- Crypto encryption and trust points are configured.
- The gateway is configured to redirect HTTP traffic (port 80) over HTTPS.
- The gateway is enabled.

## SSL VPN Encryption

The SSL VPN provides remote-access connectivity from almost any Internet-enabled location using only a web browser and its native SSL encryption. The **ssl encryption** command is configured to restrict the encryption algorithms that SSL uses in Cisco IOS software.

**Note**

There is a known compatibility issue with the encryption type and Java. If the Java port-forwarding applet does not download properly and the configuration line **ssl encryption 3des-sha1 aes-sha1** is present, you should remove the line from the webvpn gateway subconfiguration.

## SSL VPN Trustpoints

The configuration of the **ssl trustpoint** command is required only if you need to configure a specific CA certificate. A self-signed certificate is automatically generated when an SSL VPN gateway is put in service.

### SUMMARY STEPS

#### Required Steps

1. **enable**
2. **configure terminal**
3. **webvpn gateway** *name*

#### Optional Steps

4. **hostname** *name*
5. **ip address** *number* [*port number*] [*standby name*]
6. **http-redirect** [*port number*]
7. **ssl encryption** [*3des-sha1*] [*aes-sha1*] [*rc4-md5*]
8. **ssl trustpoint** *name*
9. **inservice**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>webvpn gateway</b> <i>name</i>  <b>Example:</b> Router(config)# webvpn gateway GW_1	Enters webvpn gateway configuration mode to configure an SSL VPN gateway. <ul style="list-style-type: none"><li>• Only one gateway is configured in an SSL VPN-enabled network.</li></ul>
Step 4	<b>hostname</b> <i>name</i>  <b>Example:</b> Router(config-webvpn-gateway)# hostname VPN_1	Configures the hostname for an SSL VPN gateway.

	Command or Action	Purpose
Step 5	<b>ip address</b> <i>number</i> [ <b>port</b> <i>number</i> ] [ <b>standby</b> <i>name</i> ]  <b>Example:</b> Router(config-webvpn-gateway)# ip address 10.1.1.1	Configures a proxy IP address on an SSL VPN gateway. <ul style="list-style-type: none"> <li><b>port</b>—Specifies the port number for proxy traffic. A number from 1 to 65535 can be entered for this argument.</li> <li><b>standby</b>—Indicates that the gateway is standby. A redundancy group name must be entered for the <i>name</i> argument.</li> </ul>
Step 6	<b>http-redirect</b> [ <b>port</b> <i>number</i> ]  <b>Example:</b> Router(config-webvpn-gateway)# http-redirect	Configures HTTP traffic to be carried over HTTPS. <ul style="list-style-type: none"> <li>When this command is enabled, the SSL VPN gateway listens on port 80 and redirects HTTP traffic over port 443 or the port number specified with the <b>port</b> keyword.</li> </ul>
Step 7	<b>ssl encryption</b> [ <b>3des-sha1</b> ] [ <b>aes-sha1</b> ] [ <b>rc4-md5</b> ]  <b>Example:</b> Router(config-webvpn-gateway)# ssl encryption rc4-md5	Specifies the encryption algorithm that the SSL protocol uses for SSL VPN connections. <ul style="list-style-type: none"> <li>The ordering of the algorithms specifies the preference.</li> </ul>
Step 8	<b>ssl trustpoint</b> <i>name</i>  <b>Example:</b> Router(config-webvpn-gateway)# ssl trustpoint CA_CERT	(Optional if a self-signed certificate is to be used.) Configures the certificate trust point on an SSL VPN gateway.  <b>Tip</b> Entering the <b>no</b> form of this command configures the SSL VPN gateway to revert to using an autogenerated self-signed certificate.
Step 9	<b>inservice</b>  <b>Example:</b> Router(config-webvpn-gateway)# inservice	Enables an SSL VPN gateway.  A gateway cannot be enabled or put “in service” until a proxy IP address has been configured.

## What to Do Next

SSL VPN context and policy group configurations must be configured before an SSL VPN gateway can be operationally deployed. Proceed to the section “[Configuring an SSL VPN Context](#)” to see information on SSL VPN context configuration.

## Configuring a Generic SSL VPN Gateway

To configure a generic SSL VPN gateway, perform the following steps in privileged EXEC mode.



### Note

The advantage of this configuration over the one in the configuration task “[Configuring an SSL VPN Gateway](#)” is that basic commands and context can be configured quickly using just the **webvpn enable** command.

## SUMMARY STEPS

1. **enable**
2. **webvpn enable** *gateway\_IP-address*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>webvpn enable name</b> <i>gateway_IP-address</i>  <b>Example:</b> Router# configure terminal	Enables an SSL VPN gateway.

## Configuring an SSL VPN Context

The SSL VPN context defines the virtual configuration of the SSL VPN. Entering the **webvpn context** command places the router in SSL VPN configuration mode. The following are accomplished in this task:

- A gateway and domain is associated.
- The AAA authentication method is specified.
- A group policy is associated.
- The remote user portal (web page) is customized.
- A limit on the number users sessions is configured.
- The context is enabled.

## Context Defaults

The **ssl authenticate verify all** command is enabled by default when a context configuration is created. The context cannot be removed from the router configuration while an SSL VPN gateway is in an enabled state (in service).

## Configuring a Virtual Host

A virtual hostname is specified when multiple virtual hosts are mapped to the same IP address on the SSL VPN gateway (similar to the operation of a canonical domain name). The virtual hostname differentiates host requests on the gateway. The host header in the HTTP message is modified to direct traffic to the virtual host. The virtual hostname is configured with the **gateway** command in webvpn context configuration mode.

## Prerequisites

The SSL VPN gateway configuration has been completed.

## SUMMARY STEPS

### Required Steps

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*

### Optional Steps

4. **aaa authentication** { **domain** *name* | **list** *name* }
5. **policy group** *name*
6. **exit**
7. **default-group-policy** *name*
8. **exit**
9. **gateway** *name* [**domain** *name* | **virtual-host** *name*]
10. **inservice**
11. **login-message** [*message-string*]
12. **logo** [**file** *filename* | **none**]
13. **max-users** *number*
14. **secondary-color** *color*
15. **secondary-text-color** { **black** | **white** }
16. **title** [*title-string*]
17. **title-color** *color*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
	<b>Example:</b> Router> enable	
Step 2	<b>configure terminal</b>	Enters global configuration mode.
	<b>Example:</b> Router# configure terminal	

	Command or Action	Purpose
Step 3	<b>webvpn context</b> <i>name</i>  <b>Example:</b> Router(config)# webvpn context context1	Enters webvpn context configuration mode to configure the SSL VPN context.  <b>Tip</b> The context can be optionally named using the domain or virtual hostname. This is recommended as a best practice. It simplifies the management of multiple context configurations.
Step 4	<b>aaa authentication</b> { <i>domain name</i>   <b>list</b> <i>name</i> }  <b>Example:</b> Router(config-webvpn-context)# aaa authentication domain SERVER_GROUP	Specifies a list or method for SSL VPN remote-user authentication.  <b>Tip</b> If this command is not configured, the SSL VPN gateway will use global authentication, authorization, and accounting (AAA) parameters (if configured) for remote-user authentication.
Step 5	<b>policy group</b> <i>name</i>  <b>Example:</b> Router(config-webvpn-context)# policy group ONE	Creates a policy group within the SSL VPN context and enters webvpn group policy configuration mode.  <ul style="list-style-type: none"> <li>Used to define a policy that can be applied to the user.</li> </ul>
Step 6	<b>exit</b>  <b>Example:</b> Router(webvpn-group-policy)# exit	Exits webvpn group policy configuration mode.
Step 7	<b>default-group-policy</b> <i>name</i>  <b>Example:</b> Router(webvpn-group-policy)# default-group-policy ONE	Associates a a group policy with an SSL VPN context configuration.  <ul style="list-style-type: none"> <li>This command is configured to attach the policy group to the SSL VPN context when multiple group policies are defined under the context.</li> <li>This policy will be used as default, unless a AAA server pushes an attribute that specifically requests another group policy.</li> </ul>
Step 8	<b>exit</b>  <b>Example:</b> Router(webvpn-group-policy)# exit	Exits webvpn group policy configuration mode.
Step 9	<b>gateway</b> <i>name</i> [ <i>domain name</i>   <b>virtual-host</b> <i>name</i> ]  <b>Example:</b> Router(config-webvpn-context)# gateway GW_1 domain cisco.com	Associates an SSL VPN gateway with an SSL VPN context.  <ul style="list-style-type: none"> <li>The gateway configured in the first configuration task table is associated with the SSL VPN context in this configuration step.</li> </ul>
Step 10	<b>inservice</b>  <b>Example:</b> Router(config-webvpn-gateway)# inservice	Enables an SSL VPN context configuration.  <ul style="list-style-type: none"> <li>The context is put “in service” by entering this command. However, the context is not operational until it is associated with an enabled SSL VPN gateway.</li> </ul>

	Command or Action	Purpose
Step 11	<b>login-message</b> <i>[message-string]</i>  <b>Example:</b> Router(config-webvpn-context)# login-message "Please enter your login credentials"	Configures a message for the user login text box displayed on the login page.
Step 12	<b>logo</b> [ <b>file</b> <i>filename</i>   <b>none</b> ]  <b>Example:</b> Router(config-webvpn-context)# logo file flash:/mylogo.gif	Configures a custom logo to be displayed on the login and portal pages of an SSL VPN. <ul style="list-style-type: none"> <li>The source image file for the logo is a gif, jpg, or png file that is up to 255 characters in length (filename) and up to 100 KB in size.</li> <li>The file is referenced from a local file system, such as flash memory. An error message will be displayed if the file is not referenced from a local file system.</li> <li>No logo will be displayed if the image file is removed from the local file system.</li> </ul>
Step 13	<b>max-users</b> <i>number</i>  <b>Example:</b> Router(config-webvpn-context)# max-users 500	Limits the number of connections to an SSL VPN that will be permitted.
Step 14	<b>secondary-color</b> <i>color</i>  <b>Example:</b> Router(config-webvpn-context)# secondary-color darkseagreen Router(config-webvpn-context)# secondary-color #8FBC8F Router(config-webvpn-context)# secondary-color 143,188,143	Configures the color of the secondary title bars on the login and portal pages of an SSL VPN. <ul style="list-style-type: none"> <li>The value for the <i>color</i> argument is entered as a comma-separated red, green, blue (RGB) value, an HTML color value (beginning with a pound sign [#]), or the name of the color that is recognized in HTML (no spaces between words or characters). The value is limited to 32 characters. The value is parsed to ensure that it matches one of the following formats (using Perl regex notation): <ul style="list-style-type: none"> <li><code>\#/x{6}</code></li> <li><code>\d{1,3},\d{1,3},\d{1,3}</code> (and each number is from 1 to 255)</li> <li><code>\w+</code></li> </ul> </li> <li>The default color is purple.</li> <li>The example shows the three forms that the color can be configured.</li> </ul>
Step 15	<b>secondary-text-color</b> { <b>black</b>   <b>white</b> }  <b>Example:</b> Router(config-webvpn-context)# secondary-text-color white	Configures the color of the text on the secondary bars of an SSL VPN. <ul style="list-style-type: none"> <li>The color of the text on the secondary bars must be aligned with the color of the text on the title bar.</li> <li>The default color is black.</li> </ul>

Command or Action	Purpose
<p><b>Step 16</b> <code>title [title-string]</code></p> <p><b>Example:</b>  Router(config-webvpn-context)# title "Secure  Access: Unauthorized users prohibited"</p>	<p>Configures the HTML title string that is shown in the browser title and on the title bar of an SSL VPN.</p> <ul style="list-style-type: none"> <li>The optional form of the <b>title</b> command is entered to configure a custom text string. If this command is issued without entering a text string, a title will not be displayed in the browser window. If the <b>no</b> form of this command is used, the default title string "WebVPN Service" is displayed.</li> </ul>
<p><b>Step 17</b> <code>title-color color</code></p> <p><b>Example:</b>  Router(config-webvpn-context)# title-color  darkseagreen  Router(config-webvpn-context)# title-color #8FBC8F  Router(config-webvpn-context)# title-color  143,188,143</p>	<p>Specifies the color of the title bars on the login and portal pages of an SSL VPN.</p> <ul style="list-style-type: none"> <li>The value for the <i>color</i> argument is entered as a comma-separated red, green, blue (RGB) value, an HTML color value (beginning with a pound sign [#]), or the name of the color that is recognized in HTML (no spaces between words or characters). The value is limited to 32 characters. The value is parsed to ensure that it matches one of the following formats (using Perl regex notation): <ul style="list-style-type: none"> <li><code>\#/x{6}</code></li> <li><code>\d{1,3},\d{1,3},\d{1,3}</code> (and each number is from 1 to 255)</li> <li><code>\w+</code></li> </ul> </li> <li>The default color is purple.</li> <li>The example shows the three forms that can be used to configure the title color.</li> </ul>

## What to Do Next

an SSL VPN policy group configuration must be defined before an SSL VPN gateway can be operationally deployed. Proceed to the next section to see information on SSL VPN policy group configuration.

## Configuring an SSL VPN Policy Group

The policy group is a container that defines the presentation of the portal and the permissions for resources that are configured for a group of remote users. Entering the **policy group** command places the router in webvpn group policy configuration mode. After it is configured, the group policy is attached to the SSL VPN context configuration by configuring the **default-group-policy** command. The following tasks are accomplished in this configuration:

- The presentation of the SSL VPN portal page is configured.
- A NetBIOS server list is referenced.
- A port-forwarding list is referenced.
- The idle and session timers are configured.
- A URL list is referenced.



## Outlook Web Access 2003

OWA 2003 is supported by the SSL VPN gateway upon completion of this task. The Outlook Exchange Server must be reachable by the SSL VPN gateway via TCP/IP.

## URL-List Configuration

A URL list can be configured under the SSL VPN context configuration and then separately for each individual policy group configuration. Individual URL list configurations must have unique names.

### SUMMARY STEPS

#### Required Steps

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **policy group** *name*

#### Optional Steps

5. **banner** *string*
6. **hide-url-bar**
7. **nbns-list** *name*
8. **port-forward** *name* [**auto-download**] | [**http-proxy** [**proxy-url** {*homepage-url*}]]
9. **timeout** {**idle** *seconds* | **session** *seconds*}
10. **url-list** *name*

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>webvpn context</b> <i>name</i>  <b>Example:</b> Router(config)# webvpn context context1	Enters webvpn context configuration mode to configure the SSL VPN context.
Step 4	<b>policy group</b> <i>name</i>  <b>Example:</b> Router(config-webvpn-context)# policy group ONE	Enters webvpn group policy configuration mode to configure a group policy.

	Command or Action	Purpose
Step 5	<b>banner</b> <i>string</i>  <b>Example:</b> Router(config-webvpn-group)# banner "Login Successful"	Configures a banner to be displayed after a successful login.
Step 6	<b>hide-url-bar</b>  <b>Example:</b> Router(config-webvpn-group)# hide-url-bar	Prevents the URL bar from being displayed on the SSL VPN portal page.
Step 7	<b>nbns-list</b> <i>name</i>  <b>Example:</b> Router(config-webvpn-group)# nbns-list SERVER_LIST	Attaches a NetBIOS Name Service (NBNS) server list to a policy group configuration. <ul style="list-style-type: none"> <li>The NBNS server list is first defined in SSL VPN NBNS list configuration mode.</li> </ul>
Step 8	<b>port-forward</b> <i>name</i> [ <b>auto-download</b> ]   [ <b>http-proxy</b> [ <b>proxy-url</b> { <i>homepage-url</i> }]]  <b>Example:</b> Router(config-webvpn-group)# port-forward EMAIL auto-download http-proxy proxy-url "http://www.example.com"	Attaches a port-forwarding list to a policy group configuration. <ul style="list-style-type: none"> <li><b>auto-download</b>—(Optional) Allows for automatic download of the port-forwarding Java applet on the portal page of a website.</li> <li><b>http-proxy</b>—(Optional) Allows the Java applet to act as a proxy for the browser of the user.</li> <li><b>proxy-url</b>—(Optional) Page at this URL address opens as the portal (home) page of the user.</li> <li><i>homepage-url</i>—URL of the homepage.</li> </ul>
Step 9	<b>timeout</b> { <b>idle</b> <i>seconds</i>   <b>session</b> <i>seconds</i> }  <b>Example:</b> Router(config-webvpn-group)# timeout idle 1800 Router(config-webvpn-group)# timeout session 36000	Configures the length of time that a remote user session can remain idle or the total length of time that the session can remain connected. <ul style="list-style-type: none"> <li>Upon expiration of either timer, the remote user connection is closed. The remote user must login (reauthenticate) to access the SSL VPN.</li> </ul>
Step 10	<b>url-list</b> <i>name</i>  <b>Example:</b> Router(config-webvpn-group)# url-list ACCESS	Attaches a URL list to policy group configuration.

## What to Do Next

At the completion of this task, the SSL VPN gateway and context configurations are operational and enabled (in service), and the policy group has been defined. The SSL VPN gateway is operational for clientless remote access (HTTPS only). Proceed to the next section to see information about configuring AAA for remote-user connections.

## Configuring Local AAA Authentication for SSL VPN User Sessions

The steps in this task show how to configure a local AAA database for remote-user authentication. AAA is configured in global configuration mode. In this task, the **aaa authentication** command is not configured under the SSL VPN context configuration. Omitting this command from the SSL VPN context configuration causes the SSL VPN gateway to use global authentication parameters by default.

### Prerequisites

SSL VPN gateway and context configurations are enabled and operational.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **username {name secret [0 | 5] password}**
5. **aaa authentication login default local**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>aaa new-model</b>  <b>Example:</b> Router(config)# aaa new-model	Enables the AAA access control model.
Step 4	<b>username {name secret [0   5] password}</b>  <b>Example:</b> Router(config)# username USER1 secret 0 PsW2143	Establishes a username based authentication system. <ul style="list-style-type: none"><li>• Entering <b>0</b> configures the password as clear text.</li><li>• Entering <b>5</b> encrypts the password.</li></ul>
Step 5	<b>aaa authentication login default local</b>  <b>Example:</b> Router(config)# aaa authentication login default local	Configures local AAA authentication.

## What to Do Next

The database that is configured for remote-user authentication on the SSL VPN gateway can be a local database, as shown in this task, or the database can be accessed through any RADIUS or TACACS+ AAA server.

It is recommended that you use a separate AAA server, such as a Cisco ACS. A separate AAA server provides a more robust security solution. It allows you to configure unique passwords for each remote user and accounting and logging for remote-user sessions. Proceed to the next section to see more information.

## Configuring AAA for SSL VPN Users Using a Secure Access Control Server

The steps in this task show how to configure AAA using a separate RADIUS or TACACS+ server. AAA is configured in global configuration mode. The authentication list/method is referenced in the SSL VPN context configuration with the **aaa authentication** command. The steps in this task configure AAA using a RADIUS server.

### Prerequisites

- SSL VPN gateway and context configurations are enabled and operational.
- A RADIUS or TACACS+ AAA server is operational and reachable from the SSL VPN gateway.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server** {*radius group-name* | *tacacs+ group-name*}
5. **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
6. **exit**
7. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
8. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias**{*hostname* | *ip-address*}]
9. **webvpn context** *name*
10. **aaa authentication** {**domain** *name* | **list** *name*}

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>aaa new-model</b>  <b>Example:</b> Router(config)# aaa new-model	Enables the AAA access control model.
Step 4	<b>aaa group server</b> {radius group-name   tacacs+ group-name}  <b>Example:</b> Router(config)# aaa group server radius myServer	Configures a RADIUS or TACACS+ server group and specifies the authentication list or method, and enters server-group configuration mode.
Step 5	<b>server ip-address</b> [auth-port port-number] [acct-port port-number]  <b>Example:</b> Router(config-sg-radius)# server 10.1.1.20 auth-port 1645 acct-port 1646	Configures the IP address of the AAA group server.
Step 6	<b>exit</b>  <b>Example:</b> Router(config-sg-radius)# exit	Exits server-group configuration mode.
Step 7	<b>aaa authentication login</b> {default   list-name} method1 [method2...]  <b>Example:</b> Router(config)# aaa authentication login default local group myServer	Sets AAA login parameters.
Step 8	<b>radius-server host</b> {hostname   ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string] [alias {hostname   ip-address}]  <b>Example:</b> Router(config)# radius-server host 10.1.1.20 auth-port 1645 acct-port 1646	Specifies a host as the group server.

	Command or Action	Purpose
Step 9	<b>webvpn context</b> <i>name</i>  <b>Example:</b> Router(config)# webvpn context context1	Enters SSL VPN configuration mode to configure the SSL VPN context.
Step 10	<b>aaa authentication</b> { <b>domain</b> <i>name</i>   <b>list</b> <i>name</i> }  <b>Example:</b> Router(config-webvpn-context)# aaa authentication domain myServer	Configures AAA authentication for SSL VPN sessions.

## What to Do Next

Proceed to the section “[Configuring RADIUS Attribute Support for SSL VPN](#)” to see RADIUS attribute-value pair information introduced to support this feature.

## Configuring RADIUS Accounting for SSL VPN User Sessions

To configure RADIUS accounting for SSL VPN user sessions, perform the following steps.

### Prerequisites

- Before configuring RADIUS accounting for SSL VPN user sessions, you should first have configured AAA-related commands (in global configuration mode) and have set the accounting list.

### SUMMARY STEPS

- enable**
- configure terminal**
- aaa new-model**
- webvpn aaa accounting list** *aaa-list*

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<b>aaa new-model</b>  <b>Example:</b> Router(config)# aaa new-model	Enables the AAA access control model.
Step 4	<b>webvpn aaa accounting-list aaa-list</b>  <b>Example:</b> Router(config)# webvpn aaa accounting-list SSL VPNaaa	Enables AAA accounting when you are using RADIUS for SSL VPN sessions.

## Monitoring and Maintaining RADIUS Accounting for an SSL VPN Session

To monitor and maintain your RADIUS accounting configuration, perform the following steps (the **debug** commands can be used together or individually).

### SUMMARY STEPS

1. **enable**
2. **debug webvpn aaa**
3. **debug aaa accounting**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>debug webvpn aaa</b>  <b>Example:</b> Router# debug webvpn aaa	Enables SSL VPN session monitoring for AAA.
Step 3	<b>debug aaa accounting</b>  <b>Example:</b> Router# debug aaa accounting	Displays information on accountable events as they occur.

## Configuring RADIUS Attribute Support for SSL VPN

This section lists RADIUS attribute-value (AV) pair information introduced to support SSL VPN. For information on using RADIUS AV pairs with Cisco IOS software, see the “Configuring RADIUS” chapter in the *Cisco IOS Security Configuration Guide, Release 12.4* at the following URL:

[http://www.cisco.com/en/US/customer/products/ps6350/products\\_configuration\\_guide\\_chapter09186a00804ec61e.html](http://www.cisco.com/en/US/customer/products/ps6350/products_configuration_guide_chapter09186a00804ec61e.html)

Table 5 shows information about SSL VPN RADIUS attribute-value pairs.



**Note**

All SSL VPN attributes (except for the standard IETF RADIUS attributes) start with **webvpn:** as follows:

```
webvpn:urllist-name=cisco
webvpn:nbnslist-name=cifs
webvpn:default-domain=cisco.com
```

**Table 5** *SSL VPN RADIUS Attribute-Value Pairs*

Attribute	Type of Value	Values	Default
addr (Framed-IP-Address <sup>1</sup> )	ipaddr	<i>IP_address</i>	
addr-pool	string	<i>name</i>	
auto-applet-download	integer	0 (disable) 1 (enable) <sup>2</sup>	0
banner	string		
citrix-enabled	integer	0 (disable) 1 (enable) <sup>3</sup>	0
default-domain	string		
dns-servers	ipaddr	<i>IP_address</i>	
dpd-client-timeout	integer (seconds)	0 (disabled)–3600	300
dpd-gateway-timeout	integer (seconds)	0 (disabled)–3600	300
file-access	integer	0 (disable) 1 (enable) <sup>3</sup>	0
file-browse	integer	0 (disable) 1 (enable) <sup>3</sup>	0
file-entry	integer	0 (disable) 1 (enable) <sup>3</sup>	0
hide-urlbar	integer	0 (disable) 1 (enable) <sup>3</sup>	0
home-page	string		
idletime (Idle-Timeout <sup>1</sup> )	integer (seconds)	0–3600	2100
ie-proxy-exception	string	<i>DNS_name</i>	
	ipaddr	<i>IP_address</i>	
ie-proxy-server	ipaddr	<i>IP_address</i>	
inacl	integer	1–199, 1300–2699	
	string	<i>name</i>	
keep-svc-installed	integer	0 (disable) 1 (enable) <sup>3</sup>	1
nbnslist-name	string	<i>name</i>	



**Table 5** *SSL VPN RADIUS Attribute-Value Pairs (continued)*

Attribute	Type of Value	Values	Default
netmask (Framed-IP-Netmask <sup>1</sup> )	ipaddr	<i>IP_address_mask</i>	
port-forward-auto	integer	0 (disable) 1 (enable)	If this AV pair is not configured, the default is whatever was configured for the group policy.  If this AV pair is configured with an integer of 1, the 1 will override a group policy value of 0.
port-forward-http-proxy	integer	0 (disable) 1 (enable)	HTTP proxy is not enabled.  If this AV pair is configured with an integer of 1, the 1 will override a group policy value of 0.
port-forward-http-proxy-url	string	URL address (for example, <i>http://example.com</i> )	
port-forward-name	string	<i>name</i>	
primary-dns	ipaddr	<i>IP_address</i>	
rekey-interval	integer (seconds)	0–43200	21600
secondary-dns	ipaddr	<i>IP_address</i>	
split-dns	string		
split-exclude <sup>4</sup>	ipaddr ipaddr	<i>IP_address</i> <i>IP_address_mask</i>	
	word	local-lans	
split-include <sup>4</sup>	ipaddr ipaddr	<i>IP_address</i> <i>IP_address_mask</i>	
sso-server-name	string	<i>name</i>	

**Table 5**      **SSL VPN RADIUS Attribute-Value Pairs (continued)**

Attribute	Type of Value	Values	Default
svc-enabled <sup>5</sup>	integer	0 (disable) 1 (enable) <sup>3</sup>	0
svc-ie-proxy-policy	word	none, auto, bypass-local	
svc-required <sup>5</sup>	integer	0 (disable) 1 (enable) <sup>3</sup>	0
timeout (Session-Timeout <sup>1</sup> )	integer (seconds)	1–1209600	43200
urllist-name	string	<i>name</i>	
user-vpn-group	string	<i>name</i>	
wins-server-primary	ipaddr	<i>IP_address</i>	
wins-servers	ipaddr	<i>IP_address</i>	
wins-server-secondary	ipaddr	<i>IP_address</i>	

1. Standard IETF RADIUS attributes.
2. Any integer other than 0 enables this feature.
3. Any integer other than 0 enables this feature.
4. You can specify either split-include or split-exclude, but you cannot specify both options.
5. You can specify either svc-enable or svc-required, but you cannot specify both options.

## What to Do Next

Proceed to the next section to see information about customizing the URL list configured in Step 10 of the section “[Configuring an SSL VPN Policy Group](#).”

## Configuring a URL List for Clientless Remote Access

The steps in this configuration task show how to configure a URL list. The URL list, as the name implies, is a list of HTTP URLs that are displayed on the portal page after a successful login. The URL list is configured in webvpn context configuration and webvpn group policy configuration modes.

## Prerequisites

SSL VPN gateway and context configurations are enabled and operational.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **url-list** *name*
5. **heading** *text-string*
6. **url-text** {*name* **url-value** *url*}

7. **exit**
8. **policy group** *name*
9. **url-list** *name*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>webvpn context</b> <i>name</i>  <b>Example:</b> Router(config)# webvpn context context1	Enters webvpn context configuration mode to configure the SSL VPN context.
Step 4	<b>url-list</b> <i>name</i>  <b>Example:</b> Router(config-webvpn-context)# url-list ACCESS	Enters enter webvpn URL list configuration mode to configure the list of URLs to which a user has access on the portal page of an SSL VPN.
Step 5	<b>heading</b> <i>text-string</i>  <b>Example:</b> Router(config-webvpn-url)# heading "Quick Links"	Configures the heading that is displayed above URLs listed on the portal page of an SSL VPN. <ul style="list-style-type: none"> <li>The URL list heading entered as a text string. The heading must be entered inside of quotation marks if it contains spaces.</li> </ul>
Step 6	<b>url-text</b> { <i>name</i> <b>url-value</b> <i>url</i> }  <b>Example:</b> Router(config-webvpn-url)# url-text "Human Resources" url-value hr.mycompany.com	Adds an entry to a URL list.
Step 7	<b>exit</b>  <b>Example:</b> Router(config-webvpn-url)# exit	Exits webvpn URL list configuration mode, and enters SSL VPN context configuration mode.
Step 8	<b>policy group</b> <i>name</i>  <b>Example:</b> Router(config-webvpn-context)# policy group ONE	Enters webvpn group policy configuration mode to configure a group policy.
Step 9	<b>url-list</b> <i>name</i>  <b>Example:</b> Router(config-webvpn-group)# url-list ACCESS	Attaches the URL list to the policy group configuration.

## What to Do Next

Proceed to the next section to see information about configuring clientless remote access to file shares.

## Configuring Microsoft File Shares for Clientless Remote Access

In clientless remote access mode, files and directories created on Microsoft Windows servers can be accessed by the remote client through the HTTPS-enabled browser. When enabled, a list of file server and directory links are displayed on the portal page after login. The administrator can customize permissions on the SSL VPN gateway to provide limited read-only access for a single file or full-write access and network browsing capabilities. The following access capabilities can be configured:

- Network browse (listing of domains)
- Domain browse (listing of servers)
- Server browse (listing of shares)
- Listing files in a share
- Downloading files
- Modifying files
- Creating new directories
- Creating new files
- Deleting files

## Common Internet File System Support

CIFS is the protocol that provides access to Microsoft file shares and support for common operations that allow shared files to be accessed or modified.

## NetBIOS Name Service Resolution

Windows Internet Name Service (WINS) uses NetBIOS name resolution to map and establish connections between Microsoft servers. A single server must be identified by its IP address in this configuration. Up to three servers can be added to the configuration. If multiple servers are added, one server should be configured as the master browser.

## Samba Support

Microsoft file shares can be accessed through the browser on a Linux system that is configured to run Samba.

## Prerequisites

- SSL VPN gateway and context configurations are enabled and operational.
- A Microsoft file server is operational and reachable from the SSL VPN gateway over TCP/IP.

## Restrictions

- Only file shares configured on Microsoft Windows 2000 or XP servers are supported.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **nbns-list** *name*
5. **nbns-server** *ip-address* [**master**] [**timeout** *seconds*] [**retries** *number*]
6. **exit**
7. **policy group** *name*
8. **nbns-list** *name*
9. **functions** { **file-access** | **file-browse** | **file-entry** | **svc-enabled** | **svc-required** }

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>webvpn context</b> <i>name</i>  <b>Example:</b> Router(config)# webvpn context context1	Enters webvpn context configuration mode to configure the SSL VPN context.
Step 4	<b>nbns-list</b> <i>name</i>  <b>Example:</b> Router(config-webvpn-context)# nbns-list SERVER_LIST	Enters webvpn nbnslist configuration mode to configure an NBNS server list for CIFS name resolution.
Step 5	<b>nbns-server</b> <i>ip-address</i> [ <b>master</b> ] [ <b>timeout</b> <i>seconds</i> ] [ <b>retries</b> <i>number</i> ]  <b>Example:</b> Router(config-webvpn-nbnslist)# nbns-server 172.16.1.1 master Router(config-webvpn-nbnslist)# nbns-server 172.16.2.2 timeout 10 retries 5 Router(config-webvpn-nbnslist)# nbns-server 172.16.3.3 timeout 10 retries 5	Adds a server to an NBNS server list and enters webvpn nbnslist configuration mode. <ul style="list-style-type: none"><li>The server specified with the <i>ip-address</i> argument can be a primary domain controller (PDC) in a Microsoft network.</li><li>When multiple NBNS servers are specified, a single server is configured as master browser.</li><li>Up to three NBNS server statements can be configured.</li></ul>

	Command or Action	Purpose
Step 6	<b>exit</b>  <b>Example:</b> Router(config-webvpn-nbnslist)# exit	Exits webvpn nbnslist configuration mode and enters webvpn context configuration mode.
Step 7	<b>policy group</b> <i>name</i>  <b>Example:</b> Router(config-webvpn-context)# policy group ONE	Enters webvpn group policy configuration mode to configure a group policy.
Step 8	<b>nbns-list</b> <i>name</i>  <b>Example:</b> Router(config-webvpn-group)# nbns-list SERVER_LIST	Attaches a NBNS server list to a policy group configuration.
Step 9	<b>functions</b> { <b>file-access</b>   <b>file-browse</b>   <b>file-entry</b>   <b>svc-enabled</b>   <b>svc-required</b> }  <b>Example:</b> Router(config-webvpn-group)# functions file-access Router(config-webvpn-group)# functions file-browse Router(config-webvpn-group)# functions file-entry	Configures access for Microsoft file shares. <ul style="list-style-type: none"> <li>Entering the <b>file-access</b> keyword enables network file share access. File servers in the server list are listed on the SSL VPN portal page when this keyword is enabled.</li> <li>Entering the <b>file-browse</b> keyword enables browse permissions for server and file shares. The file-access function must be enabled in order to also use this function.</li> <li>Entering the <b>file-entry</b> keyword enables “modify” permissions for files in the shares listed on the SSL VPN portal page.</li> </ul>

## Examples

### NBNS Server List Example

The following example, starting in global configuration mode, configures a server list for NBNS resolution:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# nbns-list SERVER_LIST
Router(config-webvpn-nbnslist)# nbns-server 172.16.1.1 master
Router(config-webvpn-nbnslist)# nbns-server 172.16.2.2 timeout 10 retries 5
Router(config-webvpn-nbnslist)# nbns-server 172.16.3.3 timeout 10 retries 5
Router(config-webvpn-nbnslist)# exit
```

### File Share Permissions Example

The following example attaches the server list to and enables full file and network access permissions for policy group ONE:

```
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# nbns-list SERVER_LIST
Router(config-webvpn-group)# functions file-access
Router(config-webvpn-group)# functions file-browse
Router(config-webvpn-group)# functions file-entry
Router(config-webvpn-group)# end
```

## What to Do Next

Proceed to the next section to see information about configuring clientless remote access for Citrix-enabled applications.

## Configuring Citrix Application Support for Clientless Remote Access

Clientless Citrix support allows the remote user to run Citrix-enabled applications through the SSL VPN as if the application were locally installed (similar to traditional thin-client computing). Citrix applications run on a MetaFrame XP server (or server farm). The SSL VPN gateway provides access to the remote user. The applications run in real time over the SSL VPN. This task shows how to enable Citrix support for policy group remote users.

### ICA Client

The Independent Computing Architecture (ICA) client carries keystrokes and mouse clicks from the remote user to the MetaFrame XP server. ICA traffic is carried over TCP port number 1494. This port is opened when a Citrix application is accessed. If multiple application are accessed, the traffic is carried over a single TCP session.

### Prerequisites

- A Citrix Metaframe XP server is operational and reachable from the SSL VPN gateway over TCP/IP.
- SSL VPN gateway and context configurations are enabled and operational.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**permit** | **deny**} *protocol source destination*
4. **webvpn context** *name*
5. **policy group** *name*
6. **citrix enabled**
7. **filter citrix** *extended-acl*

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>	Enables privileged EXEC mode.
	<b>Example:</b> Router> enable	<ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>	Enters global configuration mode.
	<b>Example:</b> Router# configure terminal	

	Command or Action	Purpose
Step 3	<b>access-list</b> <i>access-list-number</i> { <b>permit</b>   <b>deny</b> } <i>protocol source destination</i>  <b>Example:</b> Router(config)# access-list 100 permit ip 192.168.1.0 0.255.255.255 any	Configures the access list mechanism for filtering frames by protocol type or vendor code.
Step 4	<b>webvpn context</b> <i>name</i>  <b>Example:</b> Router(config)# webvpn context context1	Enters webvpn context configuration mode to configure the SSL VPN context.
Step 5	<b>policy group</b> <i>name</i>  <b>Example:</b> Router(config-webvpn-context)# policy group ONE	Enters webvpn group policy configuration mode to configure a group policy.
Step 6	<b>citrix enabled</b>  <b>Example:</b> Router(config-webvpn-group)# citrix enabled	Enables Citrix application support for remote users in a policy group.
Step 7	<b>filter citrix</b> <i>extended-acl</i>  <b>Example:</b> Router(config-webvpn-group)# filter citrix 100	Configures a Citrix Thin Client filter. <ul style="list-style-type: none"> <li>An extended access list is configured to define the Thin Client filter. This filter is used to control remote user access to Citrix applications.</li> </ul>

## Examples

The following example, starting in global configuration mode, enables Citrix application support for remote users with a source IP address in the 192.168.1.0/24 network:

```
Router(config)# access-list 100 permit ip 192.168.1.0 0.255.255.255 any
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# citrix enabled
Router(config-webvpn-group)# filter citrix 100
```

## What to Do Next

Support for standard applications that use well-known port numbers, such as e-mail and Telnet, can be configured using the port forwarding feature. Proceed to the next section to see more information.

## Configuring Application Port Forwarding

Application port forwarding is configured for thin client mode SSL VPN. Port forwarding extends the cryptographic functions of the SSL-protected browser to provide remote access to TCP and UDP-based applications that use well-known port numbers, such as POP3, SMTP, IMAP, Telnet, and SSH.

When port forwarding is enabled, the hosts file on the SSL VPN client is modified to map the application to the port number configured in the forwarding list. The application port mapping is restored to default when the user terminates the SSL VPN session.



## Administrative Privileges on the Remote Client

When enabling port forwarding, the SSL VPN gateway will modify the hosts file on the PC of the remote user. Some software configurations and software security applications will detect this modification and prompt the remote user to select “Yes” to permit. To permit the modification, the remote user must have local administrative privileges.



### Note

There is a known compatibility issue with the encryption type and Java. If the Java port-forwarding applet does not download properly and the configuration line **ssl encryption 3des-sha1 aes-sha1** is present, you should remove the line from the webvpn gateway subconfiguration.

## Prerequisites

SSL VPN gateway and SSL VPN context configurations are enabled and operational.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **port-forward** *name*
5. **local-port** {*number* **remote-server** *name* **remote-port** *number* **description** *text-string*}
6. **exit**
7. **policy group** *name*
8. **port-forward** *name*

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>webvpn context</b> <i>name</i>  <b>Example:</b> Router(config)# webvpn context context1	Enters webvpn context configuration mode to configure the SSL VPN context.

	Command or Action	Purpose
Step 4	<b>port-forward</b> <i>name</i>  <b>Example:</b> Router(config-webvpn-context)# port-forward EMAIL	Enters webvpn port-forward list configuration mode to configure a port forwarding list.
Step 5	<b>local-port</b> { <i>number</i> <b>remote-server</b> <i>name</i> <b>remote-port</b> <i>number</i> <b>description</b> <i>text-string</i> }  <b>Example:</b> Router(config-webvpn-port-fwd)# local-port 30016 remote-server mail.company.com remote-port 110 description POP3	Remaps (forwards) an application port number in a port forwarding list. <ul style="list-style-type: none"> <li>The remote port number is the well-known port to which the application listens. The local port number is the entry configured in the port forwarding list. A local port number can be configured only once in a given port forwarding list.</li> </ul>
Step 6	<b>exit</b>  <b>Example:</b> Router(config-webvpn-port-fwd)# exit	Exits webvpn port-forward list configuration mode, and enters webvpn context configuration mode.
Step 7	<b>policy group</b> <i>name</i>  <b>Example:</b> Router(config-webvpn-context)# policy group ONE	Enters webvpn group policy configuration mode to configure a group policy.
Step 8	<b>port-forward</b> <i>name</i>  <b>Example:</b> Router(config-webvpn-group)# port-forward EMAIL	Attaches a port forwarding list to a policy group configuration.

## Examples

The following example, starting in global configuration mode, configures port forwarding for well-known e-mail application port numbers:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# port-forward EMAIL
Router(config-webvpn-port-fwd)# local-port 30016 remote-server mail1.company.com
remote-port 110 description POP3
Router(config-webvpn-port-fwd)# local-port 30017 remote-server mail2.company.com
remote-port 25 description SMTP
Router(config-webvpn-port-fwd)# local-port 30018 remote-server mail3.company.com
remote-port 143 description IMAP
Router(config-webvpn-port-fwd)# exit
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# port-forward EMAIL
Router(config-webvpn-group)# end
```

## Configuring the SSL VPN Gateway to Distribute CSD and Cisco AnyConnect VPN Client Package Files

The SSL VPN gateway is preconfigured to distribute Cisco Secure Desktop (CSD) and/or Cisco AnyConnect VPN Client software package files to remote users. The files are distributed only when CSD or Cisco AnyConnect VPN Client support is needed. The administrator performs the following tasks to prepare the gateway:

- The current software package is downloaded from [www.cisco.com](http://www.cisco.com).
- The package file is copied to a local file system.
- The package file is installed for distribution by configuring the **webvpn install** command.

**Note**

---

Effective with Cisco IOS Release 12.4(20)T, multiple packages can be downloaded to a gateway.

---

### Remote Client Software Installation Requirements

The remote user must have administrative privileges, and the JRE for Windows version 1.4 or later must be installed before the CSD client package can be installed.

For Cisco AnyConnect VPN Client software installation, the remote user must have either the Java Runtime Environment for Windows (version 1.4 or later), or the browser must support or be configured to permit Active X controls.

### Software Package Download

The latest versions of the CSD and Cisco AnyConnect VPN Client software packages should be installed for distribution on the SSL VPN gateway.

The CSD software package can be downloaded at the following URL:

- <http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop>

The Cisco AnyConnect VPN Client software package can be downloaded at the following URL:

- <http://www.cisco.com/cgi-bin/tablebuild.pl/anyconnect>

The Cisco SSL VPN Client software package can be downloaded at the following URL:

- <http://www.cisco.com/cgi-bin/tablebuild.pl/sslvpnclient>

**Note**

---

You will be prompted to enter your login name and password to download these files from Cisco.com.

---

### Prerequisites

- SSL VPN gateway and context configurations are enabled and operational.
- Software installation packages are copied to a local files system, such as flash memory.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn install** [*csd location-name* | *svc location-name* [**sequence** *sequence-number*]]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>webvpn install</b> [ <i>csd location-name</i>   <i>svc location-name</i> [ <b>sequence</b> <i>sequence-number</i> ]]  <b>Example:</b> Router(config)# webvpn install svc flash:/webvpn/svc.pkg	Installs a CSD or Cisco AnyConnect VPN Client package file to an SSL VPN gateway for distribution to remote users. <ul style="list-style-type: none"><li>• The CSD and Cisco AnyConnect VPN Client software packages are pushed to remote users as access is needed.</li><li>• The <b>sequence</b> keyword and <i>sequence-number</i> argument are used to install multiple packages to a gateway.</li></ul>

## Examples

The following example, starting in global configuration mode, installs the Cisco AnyConnect VPN Client package to an SSL VPN gateway:

```
Router(config)# webvpn install svc flash:/webvpn/svc.pkg
SSL VPN Package SSL-VPN-Client : installed successfully
```

The following example, starting in global configuration mode, installs the CSD package to an SSL VPN gateway:

```
Router(config)# webvpn install csd flash:/securedesktop_10_1_0_9.pkg
SSL VPN Package Cisco-Secure-Desktop : installed successfully
```

The following example shows that Package B is being installed to an SSL VPN gateway:

```
Router (config)# webvpn install svc flash:/webvpn/packageB sequence 2
```

## What to Do Next

Support for CSD and Cisco AnyConnect VPN Client can be enabled for remote users after the gateway has been prepared to distribute CSD or Cisco AnyConnect VPN Client software.

## Configuring Cisco Secure Desktop Support

CSD provides a session-based interface where sensitive data can be shared for the duration of an SSL VPN session. All session information is encrypted. All traces of the session data are removed from the remote client when the session is terminated, even if the connection is terminated abruptly. CSD support for remote clients is enabled in this task.

### Java Runtime Environment

The remote user (PC or device) must have administrative privileges, and the JRE for Windows version 1.4 or later must be installed before the CSD client packages can be installed.

### Prerequisites

- SSL VPN gateway and context configurations are enabled and operational.
- The CSD software package is installed for distribution on the SSL VPN gateway.  
See the “[Configuring the SSL VPN Gateway to Distribute CSD and Cisco AnyConnect VPN Client Package Files](#)” section if you have not already prepared the SSL VPN gateway to distribute CSD software.

### Restrictions

- Only Microsoft Windows 2000, Windows XP, Windows Vista, Apple-Mac, and Linux are supported on the remote client.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **csd enable**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
	<b>Example:</b> Router> enable	
Step 2	<b>configure terminal</b>	Enters global configuration mode.
	<b>Example:</b> Router# configure terminal	

	Command or Action	Purpose
Step 3	<b>webvpn context</b> <i>name</i>  <b>Example:</b> Router(config)# webvpn context context1	Enters webvpn context configuration mode to configure the SSL VPN context.
Step 4	<b>csd enable</b>  <b>Example:</b> Router(config-webvpn-context)# csd enable	Enables CSD support for SSL VPN sessions.

## What to Do Next

Upon completion of this task, the SSL VPN gateway has been configured to provide clientless and thin client support for remote users. The SSL VPN feature also has the capability to provide full VPN access (similar to IPsec). Proceed to the next section to see more information.

## Configuring Cisco AnyConnect VPN Client Full Tunnel Support

The Cisco AnyConnect VPN Client is an application that allows a remote user to establish a full VPN connection similar to the type of connection that is established with an IPsec VPN. Cisco AnyConnect VPN Client software is pushed (downloaded) and installed automatically on the PC of the remote user. The Cisco AnyConnect VPN Client uses SSL to provide the security of an IPsec VPN without the complexity required to install IPsec in your network and on remote devices. The following tasks are completed in this configuration:

- An access list is applied to the tunnel to restrict VPN access.
- Cisco AnyConnect VPN Client tunnel support is enabled.
- An address pool is configured for assignment to remote clients.
- The default domain is configured.
- DNS is configured for Cisco AnyConnect VPN Client tunnel clients.
- Dead peer timers are configured the SSL VPN gateway and remote users.
- The login home page is configured.
- The Cisco AnyConnect VPN Client software package is configured to remain installed on the remote client.
- Tunnel key refresh parameters are defined.

## Remote Client Software from the SSL VPN Gateway

The Cisco AnyConnect VPN Client software package is pushed from the SSL VPN gateway to remote clients when support is needed. The remote user (PC or device) must have either the Java Runtime Environment for Windows (version 1.4 later), or the browser must support or be configured to permit Active X controls. In either scenario, the remote user must have local administrative privileges.

## The Address Pool

The address pool is first defined with the **ip local pool** command in global configuration mode. The standard configuration assumes that the IP addresses in the pool are reachable from a directly connected network.

### Address Pools for Nondirectly Connected Networks

If you need to configure an address pool for IP addresses from a network that is not directly connected, perform the following steps:

1. Create a local loopback interface and configure it with an IP address and subnet mask from the address pool.
2. Configure the address pool with the **ip local pool** command. The range of addresses must fall under the subnet mask configured in Step 1.
3. Set up the route. If you are using the Routing Information Protocol (RIP), configure the **router rip** command and then the **network** command, as usual, to specify a list of networks for the RIP process. If you are using the Open Shortest Path First (OSPF) protocol, configure the **ip ospf network point-to-point** command in the loopback interface. As a third choice (instead of using the RIP or OSPF protocol), you can set up static routes to the network.
4. Configure the **svc address-pool** command with the name configured in Step 2.

See the examples in this section for a complete configuration example.

## A Manual Entry to the IP Forwarding Table

If the SSL VPN software client is unable to update the IP forwarding table on the PC of the remote user, the following error message will be displayed in the router console or syslog:

```
Error : SSL VPN client was unable to Modify the IP forwarding table
```

This error can occur if the remote client does not have a default route. You can work around this error by performing the following steps:

1. Open a command prompt (DOS shell) on the remote client.
2. Enter the **route print** command.
3. If a default route is not displayed in the output, enter the **route** command followed by the **add** and **mask** keywords. Include the default gateway IP address at the end of the route statement. See the following example:

```
C:\>route ADD 0.0.0.0 MASK 0.0.0.0 10.1.1.1
```

## Prerequisites

- SSL VPN gateway and context configurations are enabled and operational.
- The Cisco AnyConnect VPN Client software package is installed for distribution on the SSL VPN gateway.
- The remote client has administrative privileges. Administrative privileges are required to download the SSL VPN software client.

See the “[Configuring the SSL VPN Gateway to Distribute CSD and Cisco AnyConnect VPN Client Package Files](#)” section if you have not already prepared the SSL VPN gateway to distribute SSL VPN software.

## Restrictions

Only Microsoft Windows 2000, Windows XP, Windows Vista, Apple-Mac, and Linux are supported on the remote client.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **policy group** *name*
5. **filter tunnel** *extended-acl*
6. **functions** {file-access | file-browse | file-entry | svc-enabled | svc-required }
7. **svc address-pool** *name*
8. **svc default-domain** *name*
9. **svc dns-server** {primary | secondary } *ip-address*
10. **svc dpd-interval** {client | gateway } *seconds*
11. **svc homepage** *string*
12. **svc keep-client-installed**
13. **svc rekey** {method {new-tunnel | ssl } | time *seconds*}

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>webvpn context</b> <i>name</i>  <b>Example:</b> Router(config)# webvpn context context1	Enters webvpn context configuration mode to configure the SSL VPN context.
Step 4	<b>policy group</b> <i>name</i>  <b>Example:</b> Router(config-webvpn-context)# policy group ONE	Enters webvpn group policy configuration mode to configure a group policy.
Step 5	<b>filter tunnel</b> <i>extended-acl</i>  <b>Example:</b> Router(config-webvpn-group)# filter tunnel 101	Configures an SSL VPN tunnel access filter. <ul style="list-style-type: none"><li>• The tunnel access filter is used control network and application level access. The tunnel filter is also defined in an extended access list.</li></ul>



	Command or Action	Purpose
Step 6	<p><b>functions</b> {<b>file-access</b>   <b>file-browse</b>   <b>file-entry</b>   <b>svc-enabled</b>   <b>svc-required</b>}</p> <p><b>Example:</b>  Router(config-webvpn-group)# functions  svc-enabled  Router(config-webvpn-group)# functions  svc-required</p>	<p>Configures Cisco AnyConnect VPN Client tunnel mode support.</p> <ul style="list-style-type: none"> <li>Entering the <b>svc-enabled</b> keyword enables tunnel support for the remote user. If the Cisco AnyConnect VPN Client software package fails to install, the remote user can continue to use clientless mode or thin-client mode.</li> <li>Entering the <b>svc-required</b> keyword enables only tunnel support for the remote user. If the Cisco AnyConnect VPN Client software package fails to install (on the PC of the remote user), the other access modes cannot be used.</li> </ul>
Step 7	<p><b>svc address-pool</b> <i>name</i></p> <p><b>Example:</b>  Router(config-webvpn-group)# svc address-pool  ADDRESSES</p>	<p>Configures configure a pool of IP addresses to assign to remote users in a policy group.</p> <ul style="list-style-type: none"> <li>The address pool is first defined with the <b>ip local pool</b> command in global configuration mode.</li> <li>If you are configuring an address pool for a network that is not directly connected, an address from the pool must be configured on a locally loopback interface. See the third example at the end of this section.</li> </ul>
Step 8	<p><b>svc default-domain</b> <i>name</i></p> <p><b>Example:</b>  Router(config-webvpn-group)# svc default-domain  cisco.com</p>	<p>Configures the default domain for a policy group.</p>
Step 9	<p><b>svc dns-server</b> {<b>primary</b>   <b>secondary</b>} <i>ip-address</i></p> <p><b>Example:</b>  Router(config-webvpn-group)# svc dns-server  primary 192.168.3.1  Router(config-webvpn-group)# svc dns-server  secondary 192.168.4.1</p>	<p>Configures DNS servers for policy group remote users.</p>
Step 10	<p><b>svc dpd-interval</b> {<b>client</b>   <b>gateway</b>} <i>seconds</i></p> <p><b>Example:</b>  Router(config-webvpn-group)# svc dpd-interval  gateway 30  Router(config-webvpn-group)# svc dpd-interval  client 300</p>	<p>Configures the dead peer detection (DPD) timer value for the gateway or client.</p> <ul style="list-style-type: none"> <li>The DPD timer is reset every time a packet is received over the SSL VPN tunnel from the gateway or remote user.</li> </ul>
Step 11	<p><b>svc homepage</b> <i>string</i></p> <p><b>Example:</b>  Router(config-webvpn-group)# svc homepage  www.cisco.com</p>	<p>Configures configure the URL of the web page that is displayed upon successful user login.</p> <ul style="list-style-type: none"> <li>The <i>string</i> argument is entered as an HTTP URL. The URL can be up to 255 characters in length.</li> </ul>

	Command or Action	Purpose
Step 12	<b>svc keep-client-installed</b>  <b>Example:</b> Router(config-webvpn-group)# svc keep-client-installed	Configures the remote user to keep Cisco AnyConnect VPN Client software installed when the SSL VPN connection is not enabled.
Step 13	<b>svc rekey {method {new-tunnel   ssl}   time seconds}</b>  <b>Example:</b> Router(config-webvpn-group)# svc rekey method new-tunnel Router(config-webvpn-group)# svc rekey time 3600	Configures the time and method that a tunnel key is refreshed for policy group remote users. <ul style="list-style-type: none"> <li>The tunnel key is refreshed by renegotiating the SSL connection or initiating a new tunnel connection.</li> <li>The time interval between tunnel refresh cycles is configured in seconds.</li> </ul>

## Examples

### Tunnel Filter Configuration

The following example, starting in global configuration mode, configures a deny access filter for any host from the 172.16.2/24 network:

```
Router(config)# access-list 101 deny ip 172.16.2.0 0.0.0.255 any
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# filter tunnel 101
Router(config-webvpn-group)# end
```

### Address Pool (Directly Connected Network) Configuration

The following example, starting in global configuration mode, configures the 192.168.1/24 network as an address pool:

```
Router(config)# ip local pool ADDRESSES 192.168.1.1 192.168.1.254
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc address-pool ADDRESSES
Router(config-webvpn-group)# end
```

### Address Pool (Nondirectly Connected Network) Configuration

The following example, starting in global configuration mode, configures the 172.16.1/24 network as an address pool. Because the network is not directly connected, a local loopback interface is configured.

```
Router(config)# interface loopback 0
Router(config-int)# ip address 172.16.1.126 255.255.255.0
Router(config-int)# no shutdown
Router(config-int)# exit
Router(config)# ip local pool ADDRESSES 172.16.1.1 172.16.1.254
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc address-pool ADDRESSES
Router(config-webvpn-group)# end
```

### Full Tunnel Configuration

The following example, starting in global configuration mode, configures full Cisco AnyConnect VPN Client tunnel support on an SSL VPN gateway:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# functions svc-enabled
Router(config-webvpn-group)# functions svc-required
Router(config-webvpn-group)# svc default-domain cisco.com
Router(config-webvpn-group)# svc dns-server primary 192.168.3.1
Router(config-webvpn-group)# svc dns-server secondary 192.168.4.1
Router(config-webvpn-group)# svc dpd-interval gateway 30
Router(config-webvpn-group)# svc dpd-interval client 300
Router(config-webvpn-group)# svc homepage www.cisco.com
Router(config-webvpn-group)# svc keep-client-installed
Router(config-webvpn-group)# svc rekey method new-tunnel
Router(config-webvpn-group)# svc rekey time 3600
Router(config-webvpn-group)# end
```

## What to Do Next

Proceed to the next section to see advanced Cisco AnyConnect VPN Client tunnel configuration information.

## Configuring Advanced SSL VPN Tunnel Features

This section describes advanced Cisco AnyConnect VPN Client tunnel configurations. The following configuration steps are completed in this task:

- Split tunnel support and split DNS resolution are enabled on the SSL VPN gateway.
- SSL VPN gateway support for Microsoft Internet Explorer proxy settings is configured.
- WINS resolution is configured for Cisco AnyConnect VPN Client tunnel clients.

### Microsoft Internet Explorer Proxy Configuration

The SSL VPN gateway can be configured to pass or bypass Microsoft Internet Explorer (MSIE) proxy settings. Only HTTP proxy settings are supported by the SSL VPN gateway. MSIE proxy settings have no effect on any other supported browser.

### Split Tunneling

Split tunnel support allows you to configure a policy that permits specific traffic to be carried outside of the Cisco AnyConnect VPN Client tunnel. Traffic is either included (resolved in tunnel) or excluded (resolved through the Internet Service Provider [ISP] or WAN connection). Tunnel resolution configuration is mutually exclusive. An IP address cannot be both included and excluded at the same time. Entering the **local-lans** keyword permits the remote user to access resources on a local LAN, such as network printer.

### Prerequisites

- SSL VPN gateway and context configurations are enabled and operational.

- The Cisco AnyConnect VPN Client software package is installed for distribution on the SSL VPN gateway.

## Restrictions

- Only Microsoft Windows 2000, Windows XP, Windows Vista, Apple-Mac, and Linux are supported on the remote client.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **policy group** *name*
5. **svc split exclude** { *ip-address mask* | **local-lans** } | **include** *ip-address mask* }
6. **svc split dns** *name*
7. **svc msie-proxy** { **exception** *host* | **option** { **auto** | **bypass-local** | **none** } }
8. **svc msie-proxy server** *host*
9. **svc wins-server** { **primary** | **secondary** } *ip-address*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>webvpn context</b> <i>name</i>  <b>Example:</b> Router(config)# webvpn context context1	Enters webvpn context configuration mode to configure the SSL VPN context.
Step 4	<b>policy group</b> <i>name</i>  <b>Example:</b> Router(config-webvpn-context)# policy group ONE	Enters webvpn group policy configuration mode to configure a group policy.

	Command or Action	Purpose
Step 5	<b>svc split exclude</b> {{ip-address mask   local-lans}   <b>include</b> ip-address mask}  <b>Example:</b> Router(config-webvpn-group)# <b>svc split exclude</b> 192.168.1.1 0.0.0.255 Router(config-webvpn-group)# <b>svc split include</b> 172.16.1.0 255.255.255.0	Configures split tunneling for policy group remote users. <ul style="list-style-type: none"> <li>Split tunneling is configured to include or exclude traffic in the Cisco AnyConnect VPN Client tunnel. Traffic that is included is sent over the SSL VPN tunnel. Traffic that is excluded is resolved outside of the tunnel.</li> <li>Exclude and include statements are configured with IP address/wildcard mask pairs.</li> </ul>
Step 6	<b>svc split dns</b> name  <b>Example:</b> Router(config-webvpn-group)# <b>svc split dns</b> www.cisco.com Router(config-webvpn-group)# <b>svc split dns</b> my.company.com	Configures the SSL VPN gateway to resolve the specified fully qualified DNS names through the Cisco AnyConnect VPN Client tunnel. <ul style="list-style-type: none"> <li>A default domain was configured in the previous task with the <b>svc default-domain</b> command. DNS names configured with the <b>svc split dns</b> command are configured in addition.</li> <li>Up to 10 split DNS statements can be configured.</li> </ul>
Step 7	<b>svc msie-proxy</b> {exception host   <b>option</b> {auto   bypass-local   none}}  <b>Example:</b> Router(config-webvpn-group)# <b>svc msie-proxy</b> option auto Router(config-webvpn-group)# <b>svc msie-proxy</b> exception www.cisco.com Router(config-webvpn-group)# <b>svc msie-proxy</b> exception 10.20.20.1	Configures MSIE browser proxy settings for policy group remote users. <ul style="list-style-type: none"> <li>Entering the <b>option auto</b> keywords configures the browser of the remote user to auto-detect proxy settings.</li> <li>Entering the <b>option bypass-local</b> keywords configures local addresses to bypass the proxy.</li> <li>Entering the <b>option none</b> keywords configures the browser on the remote client to not use a proxy.</li> </ul>
Step 8	<b>svc msie-proxy server</b> host  <b>Example:</b> Router(config-webvpn-group)# <b>svc msie-proxy</b> server 10.10.10.1:80	Specifies an MSIE proxy server for policy group remote users. <ul style="list-style-type: none"> <li>The proxy server is specified by entering an IP address or a fully qualified domain name.</li> </ul>
Step 9	<b>svc wins-server</b> {primary   secondary} ip-address  <b>Example:</b> Router(config-webvpn-group)# <b>svc wins-server</b> primary 172.31.1.1 Router(config-webvpn-group)# <b>svc wins-server</b> secondary 172.31.2.1	Configures WINS servers for policy group remote users.

## Examples

### Split DNS Configuration

The following example, starting in global configuration mode, configures the following DNS names to be resolved in the Cisco AnyConnect VPN Client tunnel:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc split dns www.example.com
```

```
Router(config-webvpn-group) # svc split dns my.company.com
```

### Including and Excluding IP Prefixes

The following example configures a list of IP addresses to be resolved over the tunnel (included) and a list to be resolved outside of the tunnel (excluded):

```
Router(config-webvpn-group) # svc split exclude 192.168.1.0 255.255.255.0
Router(config-webvpn-group) # svc split include 172.16.1.0 255.255.255.0
```

### MSIE Proxy Configuration

The following example configures MSIE proxy settings:

```
Router(config-webvpn-group) # svc msie-proxy option auto
Router(config-webvpn-group) # svc msie-proxy exception www.example.com
Router(config-webvpn-group) # svc msie-proxy exception 10.20.20.1
Router(config-webvpn-group) # svc msie-proxy server 10.10.10.1:80
```

### WINS Server Configuration

The following example configures primary and secondary WINS servers for the policy group:

```
Router(config-webvpn-group) # svc wins-server primary 172.31.1.1
Router(config-webvpn-group) # svc wins-server secondary 172.31.2.1
Router(config-webvpn-group) # svc wins-server secondary 172.31.3.1
Router(config-webvpn-group) # end
```

## Configuring VRF Virtualization

VRF Virtualization allows you to associate a traditional VRF with an SSL VPN context configuration. This feature allows you to apply different configurations and reuse address space for different groups of users in your organization.

### Prerequisites

- A VRF has been configured in global configuration mode.
- SSL VPN gateway and context configurations are enabled and operational.
- A policy group has been configured and associated with the WebVPN context.

### Restrictions

- Only a single VRF can be configured for each SSL VPN context configuration.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context *name***
4. **vrf-name *name***

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>webvpn context</b> <i>name</i>  <b>Example:</b> Router(config)# webvpn context context1	Enters webvpn context configuration mode to configure the SSL VPN context.
Step 4	<b>vrf-name</b> <i>name</i>  <b>Example:</b> Router(config-webvpn-context)# vrf-name BLUE	Associates a VRF with an SSL VPN context.

## Examples

The following example, starting in global configuration mode, associates the VRF under the SSL VPN context configuration:

```
Router(config)# ip vrf BLUE
Router(config-vrf)# rd 10.100.100.1
Router(config-vrf)# exit
Router(config)# webvpn context BLUE
Router(config-webvpn-context)# policy group BLUE
Router(config-webvpn-group)# exit
Router(config-webvpn-context)# default-group-policy BLUE
Router(config-webvpn-context)# vrf-name BLUE
Router(config-webvpn-context)# end
```

## Configuring ACL Rules

To configure ACL rules on the application layer level for an individual user, perform the following tasks.



### Note

- The ACL rules can be overridden for an individual user when the user logs on to the gateway (using AAA policy attributes).
- If a user session has no ACL attribute configured, all application requests from that user session are permitted by default.

## Prerequisites

Before configuring the ACL rules, you must have first configured the time range using the **time-range** command (this prerequisite is in addition to optionally configuring the time range, in the task table below, as part of the **permit** or **deny** entries).

## Restrictions

There is no limitation on the maximum number of filtering rules that can be configured for each ACL entry, but keeping the number below 50 should have no significant impact on router performance.

## SUMMARY STEPS

### Required Steps

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **acl** *acl-name*
5. **permit** [url [any | *url-string*]] [ip | tcp | udp | http | https | cifs] [any | *source-ip source-mask*] [any | *destination-ip destination-mask*] [**time-range** *time-range-name*] [syslog]  
or  
**deny** [url [any | *url-string*]] [ip | tcp | udp | http | https | cifs] [any | *source-ip source-mask*] [any | *destination-ip destination-mask*] [**time-range** *time-range-name*] [syslog]

### Optional Steps

6. **add position** *acl-entry*
7. **error-url** *access-deny-page-url*
8. **error-msg** *message-string*
9. **list**

## DETAILED STEPS

	Command or Action	Purpose
<b>Required Steps</b>		
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.



	Command or Action	Purpose
Step 3	<b>webvpn context</b> <i>name</i>  <b>Example:</b> Router (config)# webvpn context context1	Enters webvpn context configuration mode to configure the SSL VPN context.
Step 4	<b>acl</b> <i>acl-name</i>  <b>Example:</b> Router (config-webvpn-context)# acl acl1	Defines the ACL and enters webvpn acl configuration modes.
Step 5	<b>permit</b> [ <i>url</i> [ <i>any</i>   <i>url-string</i> ]] [ <i>ip</i>   <i>tcp</i>   <i>udp</i>   <i>http</i>   <i>https</i>   <i>cifs</i> ] [ <i>any</i>   <i>source-ip</i> <i>source-mask</i> ] [ <i>any</i>   <i>destination-ip</i> <i>destination-mask</i> ] <b>time-range</b> { <i>time-range-name</i> } [ <i>syslog</i> ]  or  <b>deny</b> [ <i>url</i> [ <i>any</i>   <i>url-string</i> ]] [ <i>ip</i>   <i>tcp</i>   <i>udp</i>   <i>http</i>   <i>https</i>   <i>cifs</i> ] [ <i>any</i>   <i>source-ip</i> <i>source-mask</i> ] [ <i>any</i>   <i>destination-ip</i> <i>destination-mask</i> ] [ <b>time-range</b> <i>time-range-name</i> ] [ <i>syslog</i> ]  <b>Example:</b> Router (config-webvpn-acl)# permit url any	Sets conditions in a named SSL VPN access list that will permit or deny packets.
<b>Optional Steps</b>		
Step 6	<b>add</b> <i>position acl-entry</i>  <b>Example:</b> Router (config-webvpn-acl)# add 3 permit url any	Adds an ACL entry at a specified position.
Step 7	<b>error-url</b> <i>access-deney-page-url</i>  <b>Example:</b> Router (config-webvpn-acl)# error-url "http://www.example.com"	Defines a URL as an ACL violation page. <ul style="list-style-type: none"> <li>If the <b>error-url</b> command is configured, the user is redirected to a predefined URL for every request that is not allowed. If the <b>error-url</b> command is not configured, the user gets a standard, gateway-generated error page.</li> </ul>
Step 8	<b>error-msg</b> <i>message-string</i>  <b>Example:</b> Router (config-webvpn-acl)# error-msg "If you have any questions, please contact <a href=mailto:employee1@example.com>Employee1</a>."	Displays a specific error message when a user logs on and his or her request is denied.
Step 9	<b>list</b>  <b>Example:</b> Router (config-webvpn-acl)# list	Lists the currently configured ACL entries sequentially and assigns a position number.

## Associating an ACL Attribute with a Policy Group

To associate an ACL attribute with a policy group, perform the following steps.



### Note

- Associating an ACL attribute for an individual user must be performed as part of a AAA operation.
- The ACL rules can be overridden for an individual user when the user logs on to the gateway (using AAA policy attributes).
- If a user session has no ACL attribute configured, all application requests from that user session are permitted by default.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **policy group** *name*
5. **exit**
6. **acl** *acl-name*

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>webvpn context</b> <i>name</i>  <b>Example:</b> Router (config)# webvpn context context1	Configures the SSL VPN context and enters webvpn context configuration mode.
Step 4	<b>policy group</b> <i>name</i>  <b>Example:</b> Router (config-webvpn-context)# policy group group1	Defines a policy that can be applied to the user and enters webvpn policy group configuration mode.

	Command or Action	Purpose
Step 5	<b>exit</b>  <b>Example:</b> Router (config-webvpn-group)# exit	Exits webvpn policy group configuration mode.
Step 6	<b>acl acl-name</b>  <b>Example:</b> Router (config-webvpn-context)# acl acl1	Defines the ACL and enters webvpn acl configuration mode.

## Monitoring and Maintaining ACLs

To monitor and maintain your ACL configuration, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **debug webvpn acl**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>debug webvpn acl</b>  <b>Example:</b> Router# debug webvpn acl	Displays information about ACLs.

## Configuring SSO Netegrity Cookie Support for a Virtual Context

To configure SSO Netegrity cookie support, perform the following steps.

### Prerequisites

- A Cisco plug-in must first be installed on a Netegrity server.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context name**
4. **sso-server name**

5. **web-agent-url** *url*
6. **secret-key** *key-name*
7. **max-retry-attempts** *number-of-retries*
8. **request-timeout** *number-of-seconds*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>webvpn context</b> <i>name</i>  <b>Example:</b> Router (config)# webvpn context context1	Enters webvpn context configuration mode to configure the SSL VPN context.
Step 4	<b>sso-server</b> <i>name</i>  <b>Example:</b> Router (config-webvpn-context)# sso-server "test-sso-server"	Creates a SSO server name under an SSL VPN context and enters webvpn sso server configuration mode
Step 5	<b>web-agent-url</b> <i>url</i>  <b>Example:</b> Router (config-webvpn-sso-server)# web-agent-url http://www.example.comwebvpn/	Configures the Netegrity agent URL to which SSO authentication requests will be dispatched.
Step 6	<b>secret-key</b> <i>key-name</i>  <b>Example:</b> Router (config-webvpn-sso-server)# secret-key "12345"	Configures the policy server secret key that is used to secure authentication requests.
Step 7	<b>max-retry-attempts</b> <i>number-of-retries</i>  <b>Example:</b> Router (config-webvpn-sso-server)# max-retry-attempts 3	Sets the maximum number of retries before SSO authentication fails.
Step 8	<b>request-timeout</b> <i>number-of-seconds</i>  <b>Example:</b> Router (config-webvpn-sso-server)# request-timeout 15	Sets the number of seconds before an authentication request times out.

## Associating an SSO Server with a Policy Group

To associate an SSO server with a policy group, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **policy group** *name*
5. **sso-server** *name*

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>webvpn context</b> <i>name</i>  <b>Example:</b> Router (config)# webvpn context context1	Configures the SSL VPN context and enters webvpn context configuration mode.
Step 4	<b>policy group</b> <i>name</i>  <b>Example:</b> Router (config-webvpn-context)# policy group ONE	Configures a group policy and enters webvpn group policy configuration mode.
Step 5	<b>sso-server</b> <i>name</i>  <b>Example:</b> Router (config-group-webvpn)# sso-server "test-sso-server"	Attaches an SSO server to a policy group.

## Configuring URL Obfuscation (Masking)

To configure URL obfuscation, masking, for a policy group, perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **policy group** *name*
5. **mask-urls**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>webvpn context</b> <i>name</i>  <b>Example:</b> Router (config)# webvpn context context1	Configures the SSL VPN context and enters webvpn context configuration mode.
Step 4	<b>policy group</b> <i>name</i>  <b>Example:</b> Router (config-webvpn-context)# policy group ONE	Configures a group policy and enters group policy configuration mode.
Step 5	<b>mask-urls</b>  <b>Example:</b> Router (config-webvpn-group)# mask-urls	Obfuscates, or masks, sensitive portions of an enterprise URL, such as IP addresses, hostnames, or port numbers.

## Adding a CIFS Server URL List to an SSL VPN Context and Attaching It to a Policy Group

To add a CIFS server URL list to an SSL VPN context and attach it to a policy group, perform the following steps.

### Prerequisites

Before adding a CIFS server URL list to an SSL VPN context, you must have already set up the Web VPN context using the **webvpn context** command, and you must be in webvpn context configuration mode.

## SUMMARY STEPS

1. **cifs-url-list** *name*
2. **heading** *text-string*
3. **url-text** *name*
4. **exit**
5. **policy group** *name*
6. **cifs-url-list** *name*
7. **exit**
8. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>cifs-url-list</b> <i>name</i>  <b>Example:</b> Router (config-webvpn-context) cifs-url-list c1	Enters webvpn URL list configuration mode to configure a list of CIFS server URLs to which a user has access on the portal page of an SSL VPN.
Step 2	<b>heading</b> <i>text-string</i>  <b>Example:</b> Router (config-webvpn-url) heading "cifs-url"	Configures the heading that is displayed above URLs listed on the portal page of an SSL VPN.
Step 3	<b>url-text</b> <i>name</i>  <b>Example:</b> Router (config-webvpn-url)# url-text "SSLVPN-SERVER2" url-value "\\SLVPN-SERVER2"	Adds an entry to a URL list. <ul style="list-style-type: none"><li>• More than one entry can be added by reentering the <b>url-text</b> command for each subsequent entry.</li></ul>
Step 4	<b>exit</b>  <b>Example:</b> Router (config-webvpn-url)# exit	Exits webvpn URL list configuration mode.
Step 5	<b>policy group</b> <i>name</i>  <b>Example:</b> Router (config)# policy group ONE	Enters webvpn group policy configuration mode to configure a group policy.
Step 6	<b>cifs-url-list</b> <i>name</i>  <b>Example:</b> Router (config-webvpn-group)# cifs-url-list "c1"	Attaches a URL list to a policy group.

	Command or Action	Purpose
Step 7	<b>exit</b>  <b>Example:</b> Router (config-webvpn-group)# exit	Exits webvpn group policy configuration mode.
Step 8	<b>exit</b>  <b>Example:</b> Router (config)# exit	Exits global configuration mode.

## Configuring User-Level Bookmarks

To configure user-level bookmarks, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **user-profile location flash:***directory*

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>webvpn context</b> <i>name</i>  <b>Example:</b> Router (config)# webvpn context context1	Configures the SSL VPN context and enters webvpn context configuration mode.
Step 4	<b>user-profile location flash:</b> <i>directory</i>  <b>Example:</b> Router (config-webvpn-context)# user-profile location flash:webvpn/sslvpn/vpn_context/	Stores bookmarks on a directory.



## Configuring FVRF

To configure FVRF so that the SSL VPN gateway is fully integrated into an MPLS network, perform the following steps.

### Prerequisites

As the following configuration task shows, IP VRF must be configured before the FVRF can be associated with the SSL VPN gateway. For more information about configuring IP VRF, see the subsection “Configuring IP VRF (**ip vrf** command)” in the “[Related Documents](#)” section.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **exit**
5. **webvpn gateway** *name*
6. **vrfname** *name*
7. **exit**
8. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip vrf</b> <i>vrf-name</i>  <b>Example:</b> Router (config)# ip vrf vrf_1	Defines a VPN VRF instance and enters VRF configuration mode.  <b>Note</b> The <i>vrf-name</i> argument specified here must be the same as the name argument in Step 6.
Step 4	<b>exit</b>  <b>Example:</b> Router (config-vrf)# exit	Exits VRF configuration mode.

	Command or Action	Purpose
Step 5	<b>webvpn gateway</b> <i>name</i>  <b>Example:</b> Router (config)# webvpn gateway mygateway	Enters webvpn gateway configuration mode to configure an SSL VPN gateway.
Step 6	<b>vrfname</b> <i>name</i>  <b>Example:</b> Router (config-webvpn-gateway)# vrfname vrf_1	Associates a VPN FVRF with an SSL VPN gateway.  <b>Note</b> The <i>name</i> argument here must be the same as the <i>vrf-name</i> argument in Step 3.
Step 7	<b>exit</b>  <b>Example:</b> Router (config-webvpn-gateway)# exit	Exits webvpn gateway configuration mode.
Step 8	<b>exit</b>  <b>Example:</b> Router (config)# exit	Exits global configuration mode.

## Disabling Full-Tunnel CEF

To disable full-tunnel CEF support, perform the following tasks:



**Note** The command **no webvpn cef** disables all Web VPN CEF support, not just full-tunnel CEF support.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no webvpn cef**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<b>no webvpn cef</b>	Disables full-tunnel CEF support.
	<b>Example:</b> Router (config)# no webvpn cef	<b>Note</b> The <b>webvpn cef</b> command is enabled by default.

## Configuring Automatic Authentication and Authorization

To configure automatic authentication and authorization so that a user needs to log in only one time, at login, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **aaa authentication auto**
5. **authorization list** *name*

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>	Enables privileged EXEC mode.
	<b>Example:</b> Router> enable	<ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>	Enters global configuration mode.
	<b>Example:</b> Router# configure terminal	
Step 3	<b>webvpn context</b> <i>name</i>	Enters webvpn context configuration mode to configure the SSL VPN context.
	<b>Example:</b> Router (config)# webvpn context context1	
Step 4	<b>aaa authentication auto</b>	Allows automatic authentication for users. Users provide their usernames and passwords via the gateway page URL and do not have to again enter their usernames and passwords from the login page.
	<b>Example:</b> Router (config-webvpn-context)# aaa authentication auto	
Step 5	<b>aaa authorization list</b> <i>name</i>	Allows user attributes to get “pushed” during authentication.
	<b>Example:</b> Router (config-webvpn-context)# aaa authorization list 11	<ul style="list-style-type: none"> <li>• <i>name</i>—Name of the list to be automatically authorized.</li> </ul>

## Configuring a URL Rewrite Splitter

To configure a URL rewrite splitter, perform the following tasks.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **url rewrite**
5. **host** *host-name*
6. **ip** *ip-address*
7. **unmatched-action** [**direct-access** | **redirect**]

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>webvpn context</b> <i>name</i>  <b>Example:</b> Router (config)# webvpn context context1	Enters webvpn context configuration mode to configure the SSL VPN context.
Step 4	<b>url rewrite</b>  <b>Example:</b> Router (config-webvpn-context)# url rewrite	Allows you to mangle selective URL requests and enters URL rewrite mode. <b>Note</b> One of the commands <b>host</b> or <b>ip</b> is required. The <b>unmatched-action</b> command is optional.
Step 5	<b>host</b> <i>host-name</i>  <b>Example:</b> Router (config-webvpn-url-rewrite)# host www.examplecompany.com	Hostname of the site to be mangled. <b>Note</b> One of the commands <b>host</b> or <b>ip</b> is required. The <b>unmatched-action</b> command is optional.

	Command or Action	Purpose
Step 6	<b>ip</b> <i>ip-address</i>  <b>Example:</b> Router (config-webvpn-url-rewrite)# ip 10.1.1.0 255.255.0.0	IP address of the site to be mangled.  <b>Note</b> One of the commands <b>host</b> or <b>ip</b> is required. The <b>unmatched-action</b> command is optional.
Step 7	<b>unmatched-action</b> [ <b>direct-access</b>   <b>redirect</b> ]  <b>Example:</b> Router (config-webvpn-url-rewrite)# unmatched-action direct-access	(Optional) Defines the action for the request to the public website.  <ul style="list-style-type: none"> <li><b>direct-access</b>—Provides the user with direct access to the URL. In addition, the user receives an information page stating that he or she can access the URL directly.</li> <li><b>redirect</b>—Provides the user with direct access to the URL, but the user does not receive the information page.</li> </ul>

## Configuring a Backend HTTP Proxy

To configure a backend HTTP proxy, perform the following tasks.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **webvpn context** *name*
4. **policy group** *name*
5. **http proxy-server** {*ip-address* | *dns-name*} **port** *port-number*

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>webvpn context</b> <i>name</i>  <b>Example:</b> Router (config)# webvpn context context1	Enters webvpn context configuration mode to configure the SSL VPN context.

	Command or Action	Purpose
Step 4	<b>policy group</b> <i>name</i>  <b>Example:</b> Router (config-webvpn-context)# <b>policy group</b> g1	Enters webvpn group policy configuration mode to configure a group policy.
Step 5	<b>http proxy-server</b> { <i>ip-address</i>   <i>dns-name</i> } <b>port</b> <i>port-number</i>  <b>Example:</b> Router (config-webvpn-context)# <b>http proxy-server</b> 10.1.1.1 <b>port</b> 2034	Allows user requests to go through a backend HTTP proxy. <ul style="list-style-type: none"> <li><i>ip-address</i>—IP address of the proxy server.</li> <li><i>dns-name</i>—Domain Name System (DNS) of the proxy server.</li> <li><b>port</b> <i>port-number</i>—Proxy port number.</li> </ul>

## Configuring Stateless High Availability with HSRP for SSL VPN

To configure stateless High Availability with HSRP for SSL VPN, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **standby number ip** *ip-address*
5. **standby number name** *standby-name*
6. **exit**
7. **webvpn gateway** *name*
8. **ip address number port** *port-number* **standby** *name*

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# <b>configure terminal</b>	Enters global configuration mode.
Step 3	<b>interface</b> <i>type slot/port</i>  <b>Example:</b> Router (config)# <b>interface</b> gateway 0/0	Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 4	<b>standby</b> <i>number</i> <b>ip</b> <i>ip-address</i>  <b>Example:</b> Router (config-if)# standby 0 ip 10.1.1.1	Configures a standby IP address.
Step 5	<b>standby</b> <i>number</i> <b>name</b> <i>standby-name</i>  <b>Example:</b> Router (config-if)# standby 0 name SSLVPN	Configures a standby name.
Step 6	<b>exit</b>  <b>Example:</b> Router (config-if)# exit	Exits interface configuration mode.
Step 7	<b>webvpn gateway</b> <i>name</i>  <b>Example:</b> Router (config)# webvpn gateway Gateway1	Enters webvpn gateway configuration mode to configure an SSL VPN gateway.
Step 8	<b>ip address</b> <i>ip-address</i> <b>port</b> <i>port-number</i> <b>standby</b> <i>name</i>  <b>Example:</b> Router (config)# ip address 10.1.1.1 port 443 standby SSLVPN	Configures a standby IP address as the proxy IP address on an SSL VPN gateway.  <b>Note</b> The IP address configured here must be the same as the IP address that was configured as the standby IP address ( <b>standby number ip ip-address</b> ).

## Using SSL VPN Clear Commands

This section describes **clear** commands that are used to perform the following tasks:

- Clear NBNS cache information
- Clear remote user sessions
- Clear (or reset) SSL VPN application and access counters

### SUMMARY STEPS

1. **enable**
2. **clear webvpn nbns** [**context** {*name* | **all**}]
3. **clear webvpn session** [**user** *name*] **context** {*name* | **all**}
4. **clear webvpn stats** [[**cifs** | **citrix** | **mangle** | **port-forward** | **sso** | **tunnel**] [**context** {*name* | **all**}]]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>clear webvpn nbns</b> [ <b>context</b> { <i>name</i>   <b>all</b> }]  <b>Example:</b> Router# clear webvpn nbns context all	Clears the NBNS cache on an SSL VPN gateway.
Step 3	<b>clear webvpn session</b> [ <b>user</b> <i>name</i> ] <b>context</b> { <i>name</i>   <b>all</b> }  <b>Example:</b> Router# clear webvpn session context all	Clears SSL VPN remote user sessions.
Step 4	<b>clear webvpn stats</b> [[ <b>cifs</b>   <b>citrix</b>   <b>mangle</b>   <b>port-forward</b>   <b>sso</b>   <b>tunnel</b> ] [ <b>context</b> { <i>name</i>   <b>all</b> }]]  <b>Example:</b> Router# clear webvpn stats	Clears SSL VPN application and access counters.

## Verifying SSL VPN Configurations

This section describes show commands that are used to verify the following:

- SSL VPN gateway configuration
- SSL VPN context configuration
- CSD and Cisco AnyConnect VPN Client installation status
- NetBIOS name services information
- SSL VPN group policy configuration
- SSL VPN user session information
- SSL VPN application statistics

## SUMMARY STEPS

1. **enable**
2. **show webvpn context** [*name*]
3. **show webvpn gateway** [*name*]
4. **show webvpn install** {**file** *name* | **package** {**csd** | **svc**} | **status** {**csd** | **svc**}}
5. **show webvpn nbns** {**context** {**all** | *name*}}
6. **show webvpn policy group** *name* **context** {**all** | *name*}



7. **show webvpn session** {[*user name*] context {**all** | *name*}}
8. **show webvpn stats** [**cifs** | **citrix** | **mangle** | **port-forward** | **sso** | **tunnel**] [**detail**] [context {**all** | *name*}]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>show webvpn context</b> [ <i>name</i> ]  <b>Example:</b> Router# show webvpn context	Displays the operational status and configuration parameters for SSL VPN context configurations.
Step 3	<b>show webvpn gateway</b> [ <i>name</i> ]  <b>Example:</b> Router# show webvpn gateway	Displays the status of the SSL VPN gateway.
Step 4	<b>show webvpn install</b> { <b>file</b> <i>name</i>   <b>package</b> { <b>csd</b>   <b>svc</b> }   <b>status</b> { <b>csd</b>   <b>svc</b> }}  <b>Example:</b> Router# show webvpn install status csd	Displays the installation status of Cisco AnyConnect VPN Client or CSD client software packages.
Step 5	<b>show webvpn nbns</b> { <b>context</b> { <b>all</b>   <i>name</i> }}  <b>Example:</b> Router# show webvpn nbns context all	Displays information in the NetBIOS Name Service (NBNS) cache.
Step 6	<b>show webvpn policy group</b> <i>name</i> <b>context</b> { <b>all</b>   <i>name</i> }  <b>Example:</b> Router# show webvpn policy group ONE context all	Displays the context configuration associated with a policy group.
Step 7	<b>show webvpn session</b> {[ <i>user name</i> ] <b>context</b> { <b>all</b>   <i>name</i> }}  <b>Example:</b> Router# show webvpn session context all	Displays SSL VPN user session information.
Step 8	<b>show webvpn stats</b> [ <b>cifs</b>   <b>citrix</b>   <b>mangle</b>   <b>port-forward</b>   <b>sso</b>   <b>tunnel</b> ] [ <b>detail</b> ] [context { <b>all</b>   <i>name</i> }]  <b>Example:</b> Router# show webvpn stats tunnel detail context all	Displays SSL VPN application and network statistics.

## Using SSL VPN Debug Commands

To monitor and manage your SSL VPN configurations, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **debug webvpn** [verbose] [aaa | acl | cifs | citrix [verbose] | cookie [verbose] | count | csd | data | dns | emweb [state] | entry context-name [source ip [network-mask] | user username] | http [authentication | trace | verbose] | package | sdps [level number] | sock [flow] | sso | timer | trie | tunnel [traffic acl-number | verbose] | url-disp | webservice [verbose]]

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>debug webvpn</b> [verbose] [aaa   acl   cifs   citrix [verbose]   cookie [verbose]   count   csd   data   dns   emweb [state]   entry context-name [source ip [network-mask]   user username]   http [authentication   trace   verbose]   package   sdps [level number]   sock [flow]   sso   timer   trie   tunnel [traffic acl-number   verbose]   url-disp   webservice [verbose]]  <b>Example:</b> Router# debug webvpn	Enables the display of debug information for SSL VPN applications and network activity.

## Remote User Guide

For information specifically for the remote user, see the document *SSL VPN Remote User Guide*.

## Configuration Examples for SSL VPN

This section includes the following configuration examples:

- [Configuring a Generic SSL VPN Gateway: Example, page 85](#)
- [Configuring an ACL: Example, page 85](#)
- [Configuring HTTP Proxy: Example, page 86](#)
- [RADIUS Accounting for SSL VPN Sessions: Example, page 86](#)
- [URL Obfuscation \(Masking\): Example, page 87](#)
- [Adding a CIFS Server URL List and Attaching It to a Policy List: Example, page 87](#)
- [Typical SSL VPN Configuration: Example, page 88](#)

- [CEF-Processed Packets: Example, page 90](#)
- [Multiple AnyConnect VPN Client Package Files: Examples, page 90](#)
- [Local Authorization: Example, page 91](#)
- [URL Rewrite Splitter: Example, page 91](#)
- [Backend HTTP Proxy: Example, page 92](#)
- [Stateless High Availability with HSRP: Example, page 92](#)
- [debug Command Output: Examples, page 93](#)
- [show Command Output: Examples, page 93](#)

## Configuring a Generic SSL VPN Gateway: Example

The following output example shows that a generic SSL VPN gateway has been configured in privileged EXEC mode:

```
Router# show running-config

webvpn gateway SSL_gateway2
 ip address 10.1.1.1. port 442
 ssl trustpoint TP_self_signed _4138349635
 inservice
!
webvpn context SSL_gateway2
 ssl authenticate verify all
!
!
policy group default
default-group-policy default
 gateway SSL_gateway2
inservice
```

## Configuring an ACL: Example

The following output example shows the ACL is “acl1.” It has been associated with policy group “default.”

```
Router# show running-config

webvpn context context1
 ssl authenticate verify all
!
acl "acl1"
 error-msg "warning!!!..."
 permit url "http://www.example1.com"
 deny url "http://www.example2.com"
 permit http any any
!
nbns-list l1
 nbns-server 10.1.1.20
!
cifs-url-list "c1"
 heading "cifs-url"
 url-text "SSL VPN-SERVER2" url-value "\\SSL VPN-SERVER2"
 url-text "SSL-SERVER2" url-value "\\SSL-SERVER2"
!
```

```

policy group default
 acl "acl1"
 cifs-url-list "c1"
 nbns-list "l1"
 functions file-access
 functions file-browse
 functions file-entry
default-group-policy default
gateway public
inservice
!

```

## Configuring HTTP Proxy: Example

The following output example shows that HTTP proxy has been configured and that the portal (home) page from URL “http://www.example.com” will automatically download the home page of the user:

Router# **show running-config**

```

webvpn context myContext
 ssl authenticate verify all
 !
 !
 port-forward "email"
 local-port 20016 remote-server "ssl-server1.SSL VPN-ios.com" remote-port 110
 description "POP-ssl-server1"
 !
 policy group myPolicy
 port-forward "email" auto-download http-proxy proxy-url "http://www.example.com"
 inservice

```

## RADIUS Accounting for SSL VPN Sessions: Example

The following output example shows that RADIUS accounting has been configured for SSL VPN user sessions:

Router# **show running-config**

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname host1
!
aaa new-model
!
!
aaa accounting network SSL VPNaaa start-stop group radius
aaa accounting update periodic 1
aaa session-id common
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name cisco.com
ip name-server 172.16.2.133
ip name-server 172.16.11.48
!

```

```

line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
!
webvpn gateway GW1
 ip address 172.19.216.141 port 443
 inservice
!
webvpn gateway SSL VPN
 no inservice
!
webvpn install svc flash:/webvpn/svc.pkg
webvpn aaa accounting-list SSL VPNaaa
!
webvpn context Default_context
 ssl encryption
 ssl authenticate verify all
!
 no inservice
!
!

```

## URL Obfuscation (Masking): Example

The following output example shows that URL obfuscation (masking) has been configured for policy group “gp\_urlobf.”

Router: **show running-config**

```

!
!
policy group gp_urlobf
 mask-urls
 default-group-policy gp_urlobf
 gateway gw domain dom
 inservice
!
!

```

## Adding a CIFS Server URL List and Attaching It to a Policy List: Example

The following output example shows that the CIFS server URLs “SSLVPN-SERVER2” and “SSL-SERVER2” have been added as portal page URLs to which a user has access. The output also shows that the two servers have been attached to a policy group.

```

webvpn context context_1
 ssl authenticate verify all
!
 acl "acl1"
 error-msg "warning!!!..."
 permit url "http://www.example1.com"
 deny url "http://www.example2.com"
 permit http any any
!
 nbns-list 11
 nbns-server 10.1.1.20

```

```

!
cifs-url-list "c1"
 heading "cifs-url"
 url-text "SSLVPN-SERVER2" url-value "\\SSLVPN-SERVER2"
 url-text "SSL-SERVER2" url-value "\\SSL-SERVER2"
!
policy group default
 acl "acl1"
 cifs-url-list "c1"
 nbns-list "l1"
 functions file-access
 functions file-browse
 functions file-entry
default-group-policy default
gateway public
inservice
!

```

## Typical SSL VPN Configuration: Example

The following output is an example of an SSL VPN configuration that includes most of the features that are available using SSL VPN:

Router# **show running-config**

```

hostname sslvpn
!
!
aaa new-model
!
!
aaa authentication login default local group radius
!
!
crypto pki trustpoint Gateway
 enrollment selfsigned
 ip-address 192.168.22.13
 revocation-check crl
 rsakeypair keys 1024 1024
!
!
crypto pki certificate chain Gateway
 certificate self-signed 02
!
!
interface Loopback0
 ip address 10.10.10.1 255.255.255.0
!
!
interface GigabitEthernet0/1
 ip address 192.168.22.14 255.255.255.0 secondary
 ip address 192.168.22.13 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
!
!
ip local pool svc-pool 10.10.10.100 10.10.10.110
!
!
ip radius source-interface FastEthernet1/1
!

```

```

!
webvpn gateway ssl-vpn
 ip address 192.168.22.13 port 443
 http-redirect port 80
 ssl trustpoint Gateway
 inservice
!
! The following line is required for SSLVPN Client.
webvpn install svc flash:/webvpn/svc.pkg
!
! The following line is required for Cisco Secure Desktop.
webvpn install csd flash:/webvpn/sdesktop.pkg
!
webvpn context ssl-vpn
 ssl authenticate verify all
!
 url-list "sslvpn-dt"
 url-text "sslvpn-dt" url-value "http://10.1.1.40"
 url-text "Exchange Server" url-value "http://10.1.1.40/exchange"
!
 sso-server "netegrity"
 web-agent-url "http://10.1.1.37/vpnauth/"
 secret-key "sslvpn1"
 retries 3
 timeout 15
!
 nbns-list cifs
 nbns-server 10.1.1.40
!
 port-forward "mail_test"
 local-port 30016 remote-server "mail.sslvpn-dt.com" remote-port 143 description
"IMAP-test"
 local-port 30017 remote-server "mail.sslvpn-dt.com" remote-port 110 description
"POP3-test"
 local-port 30018 remote-server "mail.sslvpn-dt.com" remote-port 25 description
"SMTP-test"
!
 policy group default
! The following line applies the URL list.
 url-list "sslvpn-dt"
! The following line applies TCP port forwarding.
 port-forward "mail_test"
! The following line applies CIFS.
 nbns-list "cifs"
! The following line enables CIFS functionality.
 functions file-access
! The following line enables CIFS functionality.
 functions file-browse
! The following line enables CIFS functionality.
 functions file-entry
! The following line enables SSLVPN Client.
 functions svc-enabled
! The following line enables clientless Citrix.
 citrix enabled
 default-group-policy default
! The following line maps this context to the virtual gateway and defines the domain to
use.
 gateway ssl-vpn domain sslvpn
! The following line enables Cisco Secure Desktop.
 csd enable
 inservice

```

```
!
!
end
```

## CEF-Processed Packets: Example

The following output example from the **show webvpn stats** command shows information about CEF-processed packets:

```
Router# show webvpn stats
```

```
User session statistics:
 Active user sessions : 56 AAA pending reqs : 0
 Peak user sessions : 117 Peak time : 00:13:19
 Active user TCP conns : 0 Terminated user sessions : 144
 Session alloc failures : 0 Authentication failures : 0
 VPN session timeout : 0 VPN idle timeout : 0
 User cleared VPN sessions : 0 Exceeded ctx user limit : 0
 Exceeded total user limit : 0
 Client process rcvd pkts : 1971 Server process rcvd pkts : 441004
 Client process sent pkts : 921291 Server process sent pkts : 2013
 Client CEF received pkts : 1334 Server CEF received pkts : 951610
 Client CEF rcv punt pkts : 0 Server CEF rcv punt pkts : 779
 Client CEF sent pkts : 1944439 Server CEF sent pkts : 0
 Client CEF sent punt pkts : 21070 Server CEF sent punt pkts : 0
```

## Multiple AnyConnect VPN Client Package Files: Examples

The following example shows that three AnyConnect VPN Client packages have been installed to a gateway and shows the resulting **show webvpn install** command output:

```
Router (config)# webvpn install svc vpn-Darwin_i386-Release-2.0.0077-k9.pkg sequence 6
Router (config)# webvpn install svc vpn-Darwin_powerpc-Release-2.0.0077-k9.pkg sequence 8
Router (config)# webvpn install svc svc_1.pkg sequence 4
```

```
Router# show webvpn install status svc
```

```
SSLVPN Package SSL-VPN-Client version installed:
```

```
CISCO STC win2k+
```

```
2,0,0148
```

```
Fri 12/29/2006 19:13:56.37
```

```
SSLVPN Package SSL-VPN-Client version installed:
```

```
CISCO STC Darwin_i386
```

```
2,0,0
```

```
Wed Nov 8 04:01:57 MST 2006
```

```
SSLVPN Package SSL-VPN-Client version installed:
```

```
CISCO STC Darwin_powerpc
```

```
2,0,0
```

```
Wed Nov 8 03:54:50 MST 2006
```



The following example shows (1) that three AnyConnect VPN client packages have been configured and (2) typical output from the **show-running config** command:

```
Router# show running-config | begin webvpn

webvpn install svc flash:/webvpn/svc_4.pkg sequence 4
!
webvpn install svc flash:/webvpn/svc_6.pkg sequence 6
!
webvpn install svc flash:/webvpn/svc_9.pkg sequence 9
```

## Local Authorization: Example

The following example shows that local authorization has been configured:

```
aaa new-model
!
aaa authentication login default local
aaa authorization network default local
!
aaa attribute list 12
 attribute type banner "user2"
!
aaa attribute list 11
 attribute type banner "user1"
 attribute type urllist-name "my-url-list"
!
username user1 password 0 passwd1
username user1 aaa attribute list 11
username user2 password 0 passwd2
username user2 aaa attribute list 12
!
webvpn context best
 ssl authenticate verify all
 !
 url-list "my-url-list"
 heading "external url"
 url-text "google" url-value "http://www.google.com"
 !
 policy group default
 default-group-policy default
 aaa authorization list default
 gateway public domain d1
 inservice
```

## URL Rewrite Splitter: Example

The following example shows that URL mangling has been configured for a specific host and IP address. The unmatched action has been defined as direct access.

```
webvpn context e1
!
url rewrite
 host "www.examplecompany.com"
 ip 10.1.0.0 255.255.0.0
 unmatched-action direct-access
!
```

## Backend HTTP Proxy: Example

The following example shows that a backend HTTP proxy has been configured:

```
webvpn context e1
!
 policy group g1
 http proxy-server "1.1.1.1" port 2034
 default-group-policy g1
```

## Stateless High Availability with HSRP: Example

Figure 13 shows the topology of a typical stateless High Availability with HSRP setup. Router 1 and Router 2 are configured for HSRP on Gateway Webvpn. The example below Figure 11 shows the actual configuration.

**Figure 13**      *Stateless High Availability with HSRP Setup*



### Router 1 Configuration

```
Router# configure terminal
Router (config)# interface gateway 0/1
Router (config-if)# standby 0 ip 10.1.1.1
Router (config-if)# standby 0 name SSLVPN
Router (config-if)# exit
Router (config)# webvpn gateway Webvpn
Router (config-webvpn-gateway)# ip address 10.1.1.1 port 443 standby SSLVPN
```

### Router 2 Configuration

```
Router# configure terminal
Router (config)# interface gateway 0/0
Router (config-if)# standby 0 ip 10.1.1.1
Router (config-if)# standby 0 name SSLVPN2
Router (config-if)# exit
Router (config)# webvpn gateway Webvpn
Router (config-webvpn-gateway)# ip address 10.1.1.1 port 443 standby SSLVPNhigh2
```

## debug Command Output: Examples

### Configuring SSO: Example

The following output example displays ticket creation, session setup, and response handling information for an SSO configuration:

Router# **debug webvpn sso**

```
*Jun 12 20:37:01.052: WV-SSO: Redirect to SSO web agent URL -
http://example.examplecompany.com/vpnauth/
*Jun 12 20:37:01.052: WV-SSO: Set session cookie with SSO redirect
*Jun 12 20:37:01.056: WV-SSO: Set SSO auth flag
*Jun 12 20:37:01.056: WV-SSO: Attach credentials - building auth ticket
*Jun 12 20:37:01.060: WV-SSO: user: [user11], secret: [secret123], version: [1.0], login
time: [BCEFC86D], session key: [C077F97A], SHA1 hash :
[B07D0A924DB33988D423AE9F937C1C5A66404819]
*Jun 12 20:37:01.060: WV-SSO: auth_ticket :
user11:1.0@C077F97A@BCEFC86D@B07D0A924DB33988D423AE9F937C1C5A66404819
*Jun 12 20:37:01.060: WV-SSO: Base64 credentials for the auth_ticket:
dXNlcjExOjEuMEBDMDc3Rjk3QUBCQ0VGQzg2REBCMDdEMEE5MjREQjMzOTg4RDQyM0FFOUY5MzdDMUM1QTY2NDA0OD
E5
*Jun 12 20:37:01.060: WV-SSO: Decoded credentials =
user11:1.0@C077F97A@BCEFC86D@B07D0A924DB33988D423AE9F937C1C5A66404819
*Jun 12 20:37:01.060: WV-SSO: Starting SSO request timer for 15-second

*Jun 12 20:37:01.572: WV-SSO: SSO auth response rcvd - status[200]
*Jun 12 20:37:01.572: WV-SSO: Parsed non-SM cookie: SMCHALLENGE
*Jun 12 20:37:01.576: WV-SSO: Parsed SMSESSION cookie
*Jun 12 20:37:01.576: WV-SSO: Sending logon page after SSO auth success
```

## show Command Output: Examples

The following examples display information about various SSL VPN features and scenarios:

- [show webvpn context Example, page 94](#)
- [show webvpn context name Example, page 94](#)
- [show webvpn gateway Example, page 94](#)
- [show webvpn gateway name Example, page 94](#)
- [show webvpn install file Example, page 94](#)
- [show webvpn install package svc Example, page 95](#)
- [show webvpn install status svc Example, page 95](#)
- [show webvpn nbns context all Example, page 95](#)
- [show webvpn policy Example, page 95](#)
- [show webvpn policy Example \(with NTLM disabled\), page 96](#)
- [show webvpn session Example, page 96](#)
- [show webvpn session user Example, page 96](#)
- [show webvpn stats Example, page 97](#)
- [show webvpn stats sso Examples, page 99](#)
- [F VRF show Command Output Example, page 99](#)

**show webvpn context Example**

The following is sample output from the **show webvpn context** command:

```
Router# show webvpn context
```

```
Codes: AS - Admin Status, OS - Operation Status
 VHost - Virtual Host
```

Context Name	Gateway	Domain/VHost	VRF	AS	OS
-----	-----	-----	-----	-----	-----
Default_context	n/a	n/a	n/a	down	down
con-1	gw-1	one	-	up	up
con-2	-	-	-	down	down

**show webvpn context name Example**

The following is sample output from the **show webvpn context** command, entered with the name of a specific SSL VPN context:

```
Router# show webvpn context context1
```

```
Admin Status: up
Operation Status: up
CSD Status: Disabled
Certificate authentication type: All attributes (like CRL) are verified
AAA Authentication List not configured
AAA Authentication Domain not configured
Default Group Policy: PG_1
Associated WebVPN Gateway: GW_ONE
Domain Name: DOMAIN_ONE
Maximum Users Allowed: 10000 (default)
NAT Address not configured
VRF Name not configured
```

**show webvpn gateway Example**

The following is sample output from the **show webvpn gateway** command:

```
Router# show webvpn gateway
```

Gateway Name	Admin	Operation
-----	-----	-----
GW_1	up	up
GW_2	down	down

**show webvpn gateway name Example**

The following is sample output from the **show webvpn gateway** command, entered with a specific SSL VPN gateway name:

```
Router# show webvpn gateway GW_1
```

```
Admin Status: up
Operation Status: up
IP: 10.1.1.1, port: 443
SSL Trustpoint: TP-self-signed-26793562
```

**show webvpn install file Example**

The following is sample output from the **show webvpn install** command, entered with the **file** keyword:

```
Router# show webvpn install file \webvpn\stc\version.txt
```

```
SSL VPN File \webvpn\stc\version.txt installed:
CISCO STC win2k+ 1.0.0
```

```
1,1,0,116
Fri 06/03/2005 03:02:46.43
```

### show webvpn install package svc Example

The following is sample output from the **show webvpn install** command, entered with the **package svc** keywords:

```
Router# show webvpn install package svc

SSL VPN Package SSL-VPN-Client installed:
File: \webvpn\stc\1\binaries\detectvm.class, size: 555
File: \webvpn\stc\1\binaries\java.htm, size: 309
File: \webvpn\stc\1\binaries\main.js, size: 8049
File: \webvpn\stc\1\binaries\ocx.htm, size: 244
File: \webvpn\stc\1\binaries\setup.cab, size: 176132
File: \webvpn\stc\1\binaries\stc.exe, size: 94696
File: \webvpn\stc\1\binaries\stcjava.cab, size: 7166
File: \webvpn\stc\1\binaries\stcjava.jar, size: 4846
File: \webvpn\stc\1\binaries\stcweb.cab, size: 13678
File: \webvpn\stc\1\binaries\update.txt, size: 11
File: \webvpn\stc\1\empty.html, size: 153
File: \webvpn\stc\1\images\alert.gif, size: 2042
File: \webvpn\stc\1\images\buttons.gif, size: 1842
File: \webvpn\stc\1\images\loading.gif, size: 313
File: \webvpn\stc\1\images\title.gif, size: 2739
File: \webvpn\stc\1\index.html, size: 4725
File: \webvpn\stc\2\index.html, size: 325
File: \webvpn\stc\version.txt, size: 63
Total files: 18
```

### show webvpn install status svc Example

The following is sample output from the **show webvpn install** command, entered with the **status svc** keywords:

```
Router# show webvpn install status svc

SSL VPN Package SSL-VPN-Client version installed:
CISCO STC win2k+ 1.0.0
1,0,2,127
Fri 07/22/2005 12:14:45.43
```

### show webvpn nbns context all Example

The following sample output from the **show webvpn nbns** command, entered with the **context all** keywords:

```
Router# show webvpn nbns context all

NetBIOS name IP Address Timestamp

0 total entries
NetBIOS name IP Address Timestamp

0 total entries
NetBIOS name IP Address Timestamp

0 total entries
```

### show webvpn policy Example

The following is sample output from the **show webvpn policy** command:

```
Router# show webvpn policy group ONE context all
```

```

WEBVPN: group policy = ONE ; context = SSL VPN
 idle timeout = 2100 sec
 session timeout = 43200 sec
 citrix disabled
 dpd client timeout = 300 sec
 dpd gateway timeout = 300 sec
 keep SSL VPN client installed = disabled
 rekey interval = 3600 sec
 rekey method =
 lease duration = 43200 sec
WEBVPN: group policy = ONE ; context = SSL VPN_TWO
 idle timeout = 2100 sec
 session timeout = 43200 sec
 citrix disabled
 dpd client timeout = 300 sec
 dpd gateway timeout = 300 sec
 keep SSL VPN client installed = disabled
 rekey interval = 3600 sec
 rekey method =
 lease duration = 43200 sec

```

### show webvpn policy Example (with NTLM disabled)

The following is sample output from the **show webvpn policy** command. NTLM authentication has been disabled.

```
Router# show webvpn policy group ntlm context ntlm
```

```

WEBVPN: group policy = ntlm; context = ntlm
 url list name = "ntlm-server"
 idle timeout = 2100 sec
 session timeout = 43200 sec
 functions =
 httpauth-disabled
 file-access
 svc-enabled

 citrix disabled
 dpd client timeout = 300 sec
 dpd gateway timeout = 300 sec
 keep SSL VPN client installed = disabled
 rekey interval = 3600 sec
 rekey method =
 lease duration = 43200 sec

```

### show webvpn session Example

The following is sample output from the **show webvpn session** command. The output is filtered to display user session information for only the specified context.

```
Router# show webvpn session context SSL VPN
```

```

WebVPN context name: SSL VPN
Client_Login_Name Client_IP_Address No_of_Connections Created Last_Used
user1 10.2.1.220 2 04:47:16 00:01:26
user2 10.2.1.221 2 04:48:36 00:01:56

```

### show webvpn session user Example

The following is sample output from the **show webvpn session** command. The output is filtered to display session information for a specific user.

```
Router# show webvpn session user user1 context all
```

```

WebVPN user name = user1 ; IP address = 10.2.1.220; context = SSL VPN
No of connections: 0
Created 00:00:19, Last-used 00:00:18
CSD enabled
CSD Session Policy
 CSD Web Browsing Allowed
 CSD Port Forwarding Allowed
 CSD Full Tunneling Disabled
 CSD FILE Access Allowed
User Policy Parameters
 Group name = ONE
Group Policy Parameters
 url list name = "Cisco"
 idle timeout = 2100 sec
 session timeout = 43200 sec
 port forward name = "EMAIL"
 tunnel mode = disabled
 citrix disabled
 dpd client timeout = 300 sec
 dpd gateway timeout = 300 sec
 keep stc installed = disabled
 rekey interval = 3600 sec
 rekey method = ssl
 lease duration = 3600 sec

```

### show webvpn stats Example

The following is sample output from the **show webvpn stats** command entered with the **detail** and **context** keywords:

```
Router# show webvpn stats detail context SSL VPN
```

```
WebVPN context name : SSL VPN
```

```
User session statistics:
```

Active user sessions	: 0	AAA pending reqs	: 0
Peak user sessions	: 0	Peak time	: never
Active user TCP conns	: 0	Terminated user sessions	: 0
Session alloc failures	: 0	Authentication failures	: 0
VPN session timeout	: 0	VPN idle timeout	: 0
User cleared VPN sessions:	0	Exceeded ctx user limit	: 0
CEF switched packets - client:	0		, server: 0
CEF punted packets - client:	0		, server: 0

```
Mangling statistics:
```

Relative urls	: 0	Absolute urls	: 0
Non-http(s) absolute urls:	0	Non-standard path urls	: 0
Interesting tags	: 0	Uninteresting tags	: 0
Interesting attributes	: 0	Uninteresting attributes	: 0
Embedded script statement:	0	Embedded style statement	: 0
Inline scripts	: 0	Inline styles	: 0
HTML comments	: 0	HTTP/1.0 requests	: 0
HTTP/1.1 requests	: 0	Unknown HTTP version	: 0
GET requests	: 0	POST requests	: 0
CONNECT requests	: 0	Other request methods	: 0
Through requests	: 0	Gateway requests	: 0
Pipelined requests	: 0	Req with header size >1K	: 0
Processed req hdr bytes	: 0	Processed req body bytes	: 0
HTTP/1.0 responses	: 0	HTTP/1.1 responses	: 0
HTML responses	: 0	CSS responses	: 0
XML responses	: 0	JS responses	: 0
Other content type resp	: 0	Chunked encoding resp	: 0
Resp with encoded content:	0	Resp with content length	: 0
Close after response	: 0	Resp with header size >1K:	0
Processed resp hdr size	: 0	Processed resp body bytes:	0

```

Backend https response : 0 Chunked encoding requests: 0

CIFS statistics:
SMB related Per Context:
 TCP VC's : 0 UDP VC's : 0
 Active VC's : 0 Active Contexts : 0
 Aborted Conns : 0
NetBIOS related Per Context:
 Name Queries : 0 Name Replies : 0
 NB DGM Requests : 0 NB DGM Replies : 0
 NB TCP Connect Fails : 0 NB Name Resolution Fails : 0
HTTP related Per Context:
 Requests : 0 Request Bytes RX : 0
 Request Packets RX : 0 Response Bytes TX : 0
 Response Packets TX : 0 Active Connections : 0
 Active CIFS context : 0 Requests Dropped : 0

Socket statistics:
 Sockets in use : 0 Sock Usr Blocks in use : 0
 Sock Data Buffers in use : 0 Sock Buf desc in use : 0
 Select timers in use : 0 Sock Select Timeouts : 0
 Sock Tx Blocked : 0 Sock Tx Unblocked : 0
 Sock Rx Blocked : 0 Sock Rx Unblocked : 0
 Sock UDP Connects : 0 Sock UDP Disconnects : 0
 Sock Premature Close : 0 Sock Pipe Errors : 0
 Sock Select Timeout Errs : 0

Port Forward statistics:
 Connections serviced : 0 Server Aborts (idle) : 0
Client
 in pkts : 0 Server
 in bytes : 0 out pkts : 0
 out pkts : 0 out bytes : 0
 out bytes : 0 in pkts : 0
 out bytes : 0 in bytes : 0

WEBVPN Citrix statistics:
Connections serviced : 0

Server
Packets in : 0
Packets out : 0
Bytes in : 0
Bytes out : 0

Client
0
0
0
0

Tunnel Statistics:
 Active connections : 0 Peak time : never
 Peak connections : 0 Connect failed : 0
 Connect succeed : 0 Reconnect failed : 0
 Reconnect succeed : 0 SVCIP install IOS failed : 0
 SVCIP install IOS succeed : 0 SVCIP clear IOS failed : 0
 SVCIP clear IOS succeed : 0 SVCIP install TCP failed : 0
 SVCIP install TCP succeed : 0
 DPD timeout : 0
Client
 in CSTP frames : 0 Server
 in CSTP data : 0 out IP pkts : 0
 in CSTP control : 0 out stitched pkts : 0
 in CSTP Addr Reqs : 0 out copied pkts : 0
 in CSTP DPD Reqs : 0 out bad pkts : 0
 in CSTP DPD Resps : 0 out filtered pkts : 0
 in CSTP Msg Reqs : 0 out non fwded pkts : 0
 in CSTP bytes : 0 out forwarded pkts : 0
 out CSTP frames : 0 out IP bytes : 0
 out CSTP data : 0 in IP pkts : 0
 out CSTP data : 0 in invalid pkts : 0

```



```

out CSTP control : 0 in congested pkts : 0
out CSTP Addr Resps : 0 in bad pkts : 0
out CSTP DPD Reqs : 0 in nonfwded pkts : 0
out CSTP DPD Resps : 0 in forwarded pkts : 0
out CSTP Msg Reqs : 0
out CSTP bytes : 0 in IP bytes : 0

```

### show webvpn stats sso Examples

The following output example displays statistics for an SSO server:

```
webvpn# show webvpn stats sso
```

Single Sign On statistics:

```

Auth Requests : 4 Pending Auth Requests :0
Successful Requests : 1 Failed Requests :3
Retranmissions : 0 DNS Errors :0
Connection Errors : 0 Request Timeouts :0
Unknown Responses :

```

The following output example displays extra information about SSO servers that are configured for the SSL VPN context:

```
Router# show webvpn context test_sso
```

```

Context SSO server: sso-server
Web agent URL : "http://example1.examplecompany.com/vpnauth/"
Policy Server Secret : "Secret123"
Request Re-tries : 5, Request timeout: 15-second

```

The following output example displays extra information about a SSO server that is configured for the policy group of the SSL VPN context:

```
Router# show webvpn policy group sso context test_sso
```

```

WV: group policy = sso ; context = test_sso
idle timeout = 2100 sec
session timeout = 43200 sec
sso server name = "server1"
citrix disabled
dpd client timeout = 300 sec
dpd gateway timeout = 300 sec
keep SSL VPN client installed = disabled
rekey interval = 3600 sec
rekey method =
lease duration = 43200 sec

```

### F VRF show Command Output Example

The following output example shows that FVRF has been configured:

```
Router# show webvpn gateway mygateway
```

```

Admin Status: down
Operation Status: down
Error and Event Logging: Disabled
GW IP address not configured
SSL Trustpoint: TP-self-signed-788737041
FVRF Name: vrf_1

```

# Additional References

The following sections provide references related to SSL VPN.

## Related Documents

Related Topic	Document Title
Cisco AnyConnect VPN Client	Cisco SSL VPN Client Home Page <ul style="list-style-type: none"> <li><a href="http://www.cisco.com/en/US/partner/products/ps6496/tsd_products_support_series_home.html">http://www.cisco.com/en/US/partner/products/ps6496/tsd_products_support_series_home.html</a></li> <li><i>Cisco AnyConnect VPN Client Administrator Guide, Release 2.2</i></li> <li><i>Release Notes for Cisco AnyConnect VPN Client, Version 2.0</i></li> </ul>
Cisco Secure Desktop	Cisco Secure Desktop Home Page <ul style="list-style-type: none"> <li><a href="http://www.cisco.com/en/US/partner/products/ps6742/tsd_products_support_series_home.html">http://www.cisco.com/en/US/partner/products/ps6742/tsd_products_support_series_home.html</a></li> </ul>
Configuring IP VRF ( <b>ip vrf</b> command)	<i>Cisco IOS IP Application Services Command Reference</i>
IANA Application Port Numbers	Port Numbers <ul style="list-style-type: none"> <li><a href="http://www.iana.org/assignments/port-numbers">http://www.iana.org/assignments/port-numbers</a></li> </ul>
RADIUS accounting	“Configuring RADIUS” chapter of the <i>Cisco IOS Security Configuration Guide</i>
Security commands	<i>Cisco IOS Security Command Reference</i>
SSL VPN platforms	<i>Cisco IOS SSL VPN</i> (“Feature Availability” section)
SSL VPN remote users guide	<i>SSL VPN Remote User Guide</i>

## Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

## MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature.	—

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

- **aaa accounting-list**
- **aaa authentication (WebVPN)**
- **aaa authentication auto (WebVPN)**
- **aaa authorization list**
- **acl (WebVPN)**
- **add (WebVPN)**
- **banner (WebVPN)**
- **cifs-url-list**
- **citrix enabled**
- **clear webvpn nbns**
- **clear webvpn session**
- **clear webvpn stats**

- **csd enable**
- **debug webvpn**
- **default-group-policy**
- **deny (WebVPN)**
- **error-msg**
- **error-url**
- **filter citrix**
- **filter tunnel**
- **functions**
- **gateway (WebVPN)**
- **heading**
- **hide-url-bar**
- **host (webvpn url rewrite)**
- **hostname (WebVPN)**
- **http proxy-server**
- **http-redirect**
- **inservice (WebVPN)**
- **ip (webvpn url rewrite)**
- **ip address (WebVPN)**
- **list (WebVPN)**
- **local-port (WebVPN)**
- **login-message**
- **login-photo**
- **logo**
- **mask-urls**
- **max-retry-attempts**
- **max-users (WebVPN)**
- **nbns-list**
- **nbns-list (policy group)**
- **nbns-server**
- **permit (webvpn acl)**
- **policy group**
- **port-forward**
- **port-forward (policy group)**
- **request-timeout**
- **secondary-color**
- **secondary-text-color**
- **secret-key**

- **show webvpn context**
- **show webvpn gateway**
- **show webvpn nbns**
- **show webvpn policy**
- **show webvpn session**
- **show webvpn stats**
- **ssl encryption**
- **ssl trustpoint**
- **sso-server**
- **svc address-pool**
- **svc default-domain**
- **svc dns-server**
- **svc dpd-interval**
- **svc homepage**
- **svc keep-client-installed**
- **svc msie-proxy**
- **svc rekey**
- **svc split**
- **svc split dns**
- **svc wins-server**
- **text-color**
- **timeout (policy group)**
- **time-range**
- **title**
- **title-color**
- **unmatched-action**
- **url-list**
- **url rewrite**
- **url-text**
- **user-profile location**
- **vrfname**
- **vrf-name**
- **web-agent-url**
- **webvpn cef**
- **webvpn context**
- **webvpn enable (Privileged EXEC)**
- **webvpn gateway**
- **webvpn install**

# Feature Information for SSL VPN

Table 6 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 6 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 6** Feature Information for SSL VPN

Feature Name	Release	Feature Information
SSL VPN	12.4(6)T	<p>This feature enhances SSL VPN support in Cisco IOS software. This feature provides a comprehensive solution that allows easy access to a broad range of web resources and web-enabled applications using native HTTP over SSL (HTTPS) browser support. SSL VPN introduced three modes of SSL VPN access: clientless, thin-client, and full-tunnel client support.</p> <p>The following command was introduced in Cisco IOS Release 12.4(15)T: <b>cifs-url-list</b>.</p>
Access Control Enhancements	12.4(20)T	<p>This feature allows administrators to configure automatic authentication and authorization for users. Users provide their usernames and passwords via the gateway page URL and do not have to reenter their usernames and passwords from the login page. Authorization is enhanced to support more generic authorization, including local authorization.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Access Control Enhancements, page 10</a></li> <li>• <a href="#">Configuring Automatic Authentication and Authorization, page 77</a></li> <li>• <a href="#">Local Authorization: Example, page 91</a></li> </ul> <p>The following commands were introduced by this feature: <b>aaa authentication auto</b> and <b>aaa authorization list</b></p>

**Table 6**      **Feature Information for SSL VPN (continued)**

Application ACL Support	12.4(11)T	<p>This feature provides administrators with the flexibility to fine tune access control on the Application Layer level.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Application ACL Support, page 11</a></li> <li>• <a href="#">Configuring ACL Rules, page 65</a></li> <li>• <a href="#">Associating an ACL Attribute with a Policy Group, page 68</a></li> <li>• <a href="#">Configuring an ACL: Example, page 85</a></li> </ul> <p>The following commands were introduced by this feature: <b>acl</b>, <b>add</b>, <b>error-msg</b>, <b>error-url</b>, and <b>list</b>.</p>
Auto Applet Download	12.4(9)T	<p>This feature provides administrators with the option of automatically downloading the port-forwarding applet under the policy group.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Options for Configuring HTTP Proxy and the Portal Page, page 8</a></li> </ul> <p>The following command was modified by this feature: <b>port-forward (policy group)</b></p>
Backend HTTP Proxy	12.4(20)T	<p>This feature allows administrators to route user requests through a backend HTTP proxy, providing more flexibility and controllability than routing through internal web servers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Backend HTTP Proxy, page 11</a></li> <li>• <a href="#">Configuring a Backend HTTP Proxy, page 79</a></li> <li>• <a href="#">Backend HTTP Proxy: Example, page 92</a></li> </ul> <p>The following command was added by this feature: <b>http proxy-server</b></p>

**Table 6**      **Feature Information for SSL VPN (continued)**

Cisco AnyConnect VPN Client	12.4(15)T	<p>This feature is the next-generation SSL VPN Client. The feature provides remote users with secure VPN connections to the router platforms supported by SSL VPN and to the Cisco 5500 Series Adaptive Security Appliances.</p> <p>Users having Cisco IOS software releases before Release 12.4(15)T see SSL VPN Client GUI. Users having Release 12.4(15)T and later releases see Cisco AnyConnect VPN Client GUI.</p> <p>The task configurations in this document for tunnel mode apply to SVC and AnyConnect VPN Client.</p> <p>For more information about the Cisco AnyConnect VPN Client feature, see the documents <a href="#">Cisco AnyConnect VPN Client Administrator Guide</a> and <a href="#">Release Notes for Cisco AnyConnect VPN Client, Version 2.0</a>.</p> <p><b>Note</b> Many of the features listed in the documents <i>Cisco AnyConnect VPN Client Administrator Guide</i> and <i>Release Notes for Cisco AnyConnect VPN Client, Version 2.0</i> apply only to the Cisco ASA 5500 Series Adaptive Security Appliances. For a list of features that do not currently apply to other Cisco platforms, see the restriction in the “<a href="#">Cisco AnyConnect VPN Client</a>” section on page 3 of this document.</p>
AnyConnect Client Support	12.4(20)T	<p>Effective with this release, AnyConnect Client adds support for several client-side platforms, such as Microsoft Windows, Apple-Mac, and Linux. The ability to install AnyConnect in a standalone mode is also added. In addition, this feature allows multiple SSL VPN client package files to be configured on a gateway.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">AnyConnect Client Support, page 10</a></li> <li>• <a href="#">Configuring the SSL VPN Gateway to Distribute CSD and Cisco AnyConnect VPN Client Package Files, page 53</a></li> <li>• <a href="#">Multiple AnyConnect VPN Client Package Files: Examples, page 90</a></li> </ul> <p>The following command was modified by this feature: <b>webvpn install</b></p>



**Table 6**      **Feature Information for SSL VPN (continued)**

Debug Infrastructure	12.4(11)T	<p>Updates to the <b>webvpn debug</b> command provide administrators with the ability to turn debugging on for any one user or group.</p> <p>The following keywords were introduced by this feature: <b>acl</b>, <b>entry</b>, <b>sso</b>, and <b>verbose</b>.</p> <p>The following keyword options were added for the <b>http</b> keyword: <b>authentication</b>, <b>trace</b>, and <b>verbose</b>.</p> <p>The <b>verbose</b> keyword option was added for the <b>citrix</b>, <b>cookie</b>, <b>tunnel</b>, and <b>webservice</b> keywords.</p> <p>The <b>port-forward</b> keyword was deleted effective with this release, and the <b>detail</b> keyword option for the <b>tunnel</b> keyword was deleted.</p>
Front-Door VRF Support	12.4(15)T	<p>Coupled with the already supported internal VRF, this feature allows the SSL VPN gateway to be fully integrated into an MPLS network.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Front-Door VRF Support, page 11</a></li> <li>• <a href="#">Configuring FVRF, page 75</a></li> </ul>
Full-Tunnel CEF Support	12.4(20)T	<p>This feature provides better performance for full-tunnel packets.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Full-Tunnel CEF Support, page 12</a></li> <li>• <a href="#">Disabling Full-Tunnel CEF, page 76</a></li> <li>• <a href="#">CEF-Processed Packets: Example, page 90</a></li> </ul>
GUI Enhancements	12.4(15)T	<p>These enhancements provide updated examples and explanation of the Web VPN GUIs.</p> <p>The following section provides information about these updates:</p> <ul style="list-style-type: none"> <li>• <a href="#">GUI Enhancements, page 12</a></li> </ul>

**Table 6**      **Feature Information for SSL VPN (continued)**

Netegrity Cookie-Based Single SignOn (SSO) Support	12.4(11)T	<p>This feature allows administrators to configure a SSO server that sets a SiteMinder cookie in the browser of a user when the user initially logs on. The benefit of this feature is that users are prompted to log on only a single time</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Netegrity Cookie-Based Single SignOn Support, page 18</a></li> <li>• <a href="#">Configuring SSO Netegrity Cookie Support for a Virtual Context, page 69</a></li> <li>• <a href="#">Associating an SSO Server with a Policy Group, page 71</a></li> </ul> <p>The following commands were modified for this feature: <b>clear webvpn stats</b>, <b>debug webvpn</b>, <b>show webvpn policy</b>, <b>show webvpn context</b>, and <b>show webvpn stats</b>.</p> <p>The following commands were added for this feature: <b>max-retry-attempts</b>, <b>request-timeout</b>, <b>secret-key</b>, <b>sso-server</b>, and <b>web-agent-url</b>.</p>
NTLM Authentication	12.4(9)T	<p>This feature provides NT LAN Manager (NTLM) authentication support.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">NTLM Authentication, page 18</a></li> </ul> <p>The following command was modified by this feature: <b>functions</b></p>
Port-Forward Enhancements	12.4(11)T	<p>This feature provides administrators with more options for configuring HTTP proxy and portal pages.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Options for Configuring HTTP Proxy and the Portal Page, page 8</a></li> </ul> <p>The following commands were added for this feature: <b>acl</b>, <b>add</b>, <b>deny</b>, <b>error-msg</b>, <b>error-url</b>, <b>list</b>, and <b>permit</b>.</p>

**Table 6**      **Feature Information for SSL VPN (continued)**

RADIUS Accounting	12.4(9)T	<p>This feature provides for RADIUS accounting for SSL VPN sessions.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">RADIUS Accounting, page 18</a></li> <li>• <a href="#">Configuring RADIUS Accounting for SSL VPN User Sessions, page 40</a></li> <li>• <a href="#">RADIUS Accounting for SSL VPN Sessions: Example, page 86</a></li> </ul> <p>The following command was added by this feature: <b>webvpn aaa accounting-list</b></p>
Stateless High Availability with Hot Standby Router Protocol (HSRP)	12.4(20)T	<p>This feature allows stateless failover to be applied to VPN routers by using HSRP.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Stateless High Availability with Hot Standby Router Protocol, page 19</a></li> <li>• <a href="#">Configuring Stateless High Availability with HSRP for SSL VPN, page 80</a></li> <li>• <a href="#">Stateless High Availability with HSRP: Example, page 92</a></li> </ul> <p>The following command was modified by this feature: <b>ip address</b></p>
URL Obfuscation	12.4(11)T	<p>This feature provides administrators with the ability to obfuscate, or mask, sensitive portions of an enterprise URL, such as IP addresses, hostnames, or port numbers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">URL Obfuscation, page 22</a></li> <li>• <a href="#">Configuring URL Obfuscation (Masking), page 71</a></li> <li>• <a href="#">URL Obfuscation (Masking): Example, page 87</a></li> </ul> <p>The following command was added by this feature: <b>mask-urls</b></p>

**Table 6**      **Feature Information for SSL VPN (continued)**

URL Rewrite Splitter	12.4(20)T	<p>This feature allows administrators to selectively mangle requests to the gateway.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">URL Rewrite Splitter, page 22</a></li> <li>• <a href="#">Configuring a URL Rewrite Splitter, page 78</a></li> <li>• <a href="#">URL Rewrite Splitter: Example, page 91</a></li> </ul> <p>The following commands were added by this feature: <b>host</b>, <b>ip</b>, <b>unmatched-action</b>, and <b>url rewrite</b></p>
User-Level Bookmarking	12.4(15)T	<p>This feature allows a user to bookmark URLs while connected through an SSL VPN tunnel.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">User-Level Bookmarking, page 22</a></li> <li>• <a href="#">Configuring User-Level Bookmarks, page 74</a></li> </ul> <p>The following command was added by this feature: <b>user-profile location</b></p>

## Notices

The following notices pertain to this software license.

### OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

### License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

#### OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)".
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

**Original SSLeay License:**

Copyright © 1995-1998 Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). All rights reserved.

This package is an SSL implementation written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

---

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0805R)

---

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007–2008 Cisco Systems, Inc. All rights reserved.



# SSL VPN Remote User Guide

---

**First Published: February 27, 2006**

**Last Updated: March 6, 2008**

The SSL VPN feature (also known as WebVPN) provides support, in Cisco IOS software, for remote user access to enterprise networks from anywhere on the Internet. Remote access is provided through a Secure Socket Layer- (SSL-) enabled SSL Virtual Private Network (VPN) gateway. The SSL VPN gateway allows remote users to establish a secure VPN tunnel using a web browser. This feature provides a comprehensive solution that allows easy access to a broad range of web resources and web-enabled applications using native HTTP over SSL (HTTPS) browser support.

This document describes how a remote user, whose enterprise network is configured for SSL VPN, can access the network by launching a browser and connecting to the SSL VPN gateway.

For information about SSL VPN from the point of view of a system administrator, see the document [SSL VPN](#).



**Note**

The Cisco AnyConnect VPN Client is introduced in Cisco IOS Release 12.4(15)T. This feature is the next-generation SSL VPN Client. If you are using Cisco software before Cisco IOS Release 12.4(15)T, you should use SSL VPN Client and see GUI for the SSL VPN Client when you are web browsing. However, if you are using Cisco software Release 12.4(15)T or later, you should use Cisco AnyConnect VPN Client and see GUI for Cisco AnyConnect VPN Client when you are web browsing.

For “What’s New” information about SSL VPN features by release, see the [“Feature Information for SSL VPN for Remote Users” section on page 23](#).

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for SSL VPN for Remote Users” section on page 23](#).*

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007–2008 Cisco Systems, Inc. All rights reserved.

# Contents:

- [SSL VPN Prerequisites for the Remote User, page 2](#)
- [Restrictions for SSL VPN Remote User Guide, page 3](#)
- [Usernames and Passwords, page 3](#)
- [Remote User Interface, page 4](#)
- [Security Tips, page 17](#)
- [Troubleshooting Guidelines, page 20](#)
- [Additional References, page 21](#)
- [Feature Information for SSL VPN for Remote Users, page 23](#)
- [Notices, page 24](#)

## SSL VPN Prerequisites for the Remote User

The following prerequisites are required to start SSL VPN on a PC or device:

- Connection to the Internet—Any Internet connection is supported, including:
  - Home DSL, cable, or dial-ups
  - Public kiosks
  - Hotel connections
  - Airport wireless nodes
  - Internet cafes
- Operating system support




---

**Note** Later versions of the following software are also supported.

---

- Microsoft Windows 2000, Windows XP, or Windows Vista
- Macintosh OS X 10.4.6
- Linux (Redhat RHEL 3.0 +, FEDORA 5, or FEDORA 6)
- SSL VPN-supported browser—The following browsers have been verified for SSL VPN. Other browsers might not fully support SSL VPN features.




---

**Note** Later versions of the following software are also supported.

---

- Internet Explorer 6.0 or 7.0
- Firefox 2.0 (Windows and Linux)
- Safari 2.0.3
- Cookies enabled—Cookies must be enabled on the browser to access applications through port forwarding.



- Pop-ups enabled—Pop-ups should be enabled on the browser to display the floating SSL VPN toolbar and timeout warnings. If pop-ups are blocked, change the browser setting and click the SSL VPN floating toolbar icon on the in-page toolbar to display the floating toolbar.  
If pop-ups are disabled on the browser, SSL VPN does not warn you before disconnecting because of an idle timeout or a maximum connect time.
- URL for SSL VPN—An HTTPS address in the following form:  
`https://address`  
where *address* is the IP address or Domain Name System (DNS) hostname of an interface of the SSL VPN gateway, for example `https://10.89.192.163` or `https://vpn.company.com`.
- SSL VPN username and password

## Restrictions for SSL VPN Remote User Guide

### Cisco AnyConnect VPN Client

CiscoAnyConnect VPN Client does not support the following:

- Adaptive Security Appliance (ASA) and Adaptive Security Device Manager (ASDM) and any command-line interface (CLI) associated with the them
- Adjusting Maximum Transmission Unit (MTU) size
- Client-side authentication
- Compression support
- Datagram Transport Layer Security (DTLS) with SSL connections
- IPv6 VPN access
- Language Translation (localization)
- (Optional) Local printer—SSL VPN does not support printing in clientless mode from a web browser to a network printer. However, printing to a local printer is supported.
- Sequencing
- Standalone Mode

## Username and Passwords

[Table 1](#) lists the type of usernames and passwords that SSL VPN users might have to know.

**Table 1** *Usernames and Passwords for SSL VPN Users*

Login Username/ Password Type	Purpose	Entered When
Computer	Access the computer	Starting the computer
Internet Provider	Access the Internet	Connecting to an Internet provider
SSL VPN	Access the remote network	Starting SSL VPN
File Server	Access the remote file server	Using the SSL VPN file browsing feature to access a remote file server

**Table 1**      *Username and Passwords for SSL VPN Users (continued)*

<b>Login Username/ Password Type</b>	<b>Purpose</b>	<b>Entered When</b>
Corporate Application Login	Access the firewall-protected internal server	Using the SSL VPN web browsing feature to access an internal protected website
Mail Server	Access the remote mail server via SSL VPN	Sending or receiving e-mail messages

## Remote User Interface

If your enterprise network has been configured for SSL VPN, you can access the network by launching a browser and connecting to the SSL VPN gateway. Present your credentials and authenticate, and then a portal page (home page) of the enterprise site is displayed. The portal page displays SSL VPN features (for example, e-mail and web browsing) to which you have access on the basis of your credentials. If you have access to all features enabled on the SSL VPN gateway, the home page will provide access links.

The following sections explain the remote user interface in more detail:

- [Page Flow, page 4](#)
- [Initial Connection, page 5](#)
- [Login Page, page 5](#)
- [Certificate Authentication, page 6](#)
- [Logout Page, page 6](#)
- [Portal Page, page 7](#)
- [Remote Servers, page 9](#)
- [Toolbar, page 9](#)
- [Session Timeout, page 12](#)
- [TCP Port Forwarding and Thin Client, page 13](#)
- [Tunnel Connection, page 15](#)
- [User-Level Bookmarking, page 15](#)

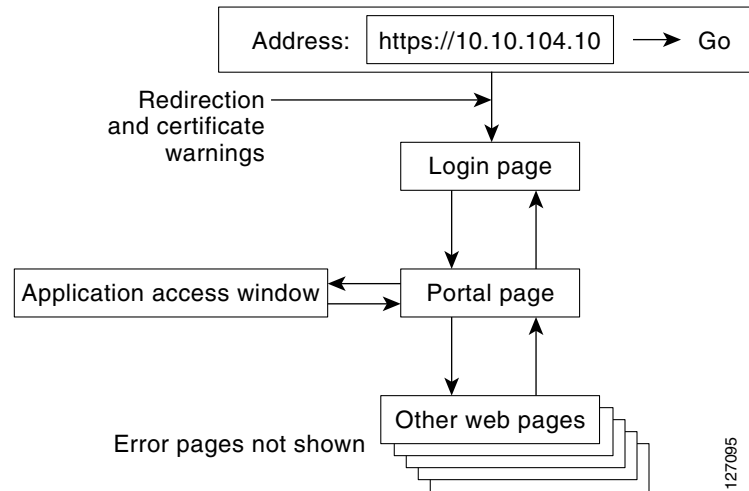
## Page Flow

This section describes the page flow process (see [Figure 1](#)) for a SSL VPN session. When you enter the HTTPS URL (<https://address>) into your browser, you are then redirected to <https://address/index.html>, where the login page is located.



### Note

Depending on the configuration of the browser, this redirection may display a warning message in your browser, which indicates that you are being redirected to a secure connection.

**Figure 1**      **Page Flow**

## Initial Connection

When you connect for the first time, you might be presented with one of the following scenarios:

- [503 Service Unavailable Message, page 5](#)
- [SSL/TLS Certificate, page 5](#)
- [Web Browsing, page 10](#)

### 503 Service Unavailable Message

You might see a “503 Service Unavailable” message if the gateway is experiencing high traffic loads. If you receive this message, try to connect again later.

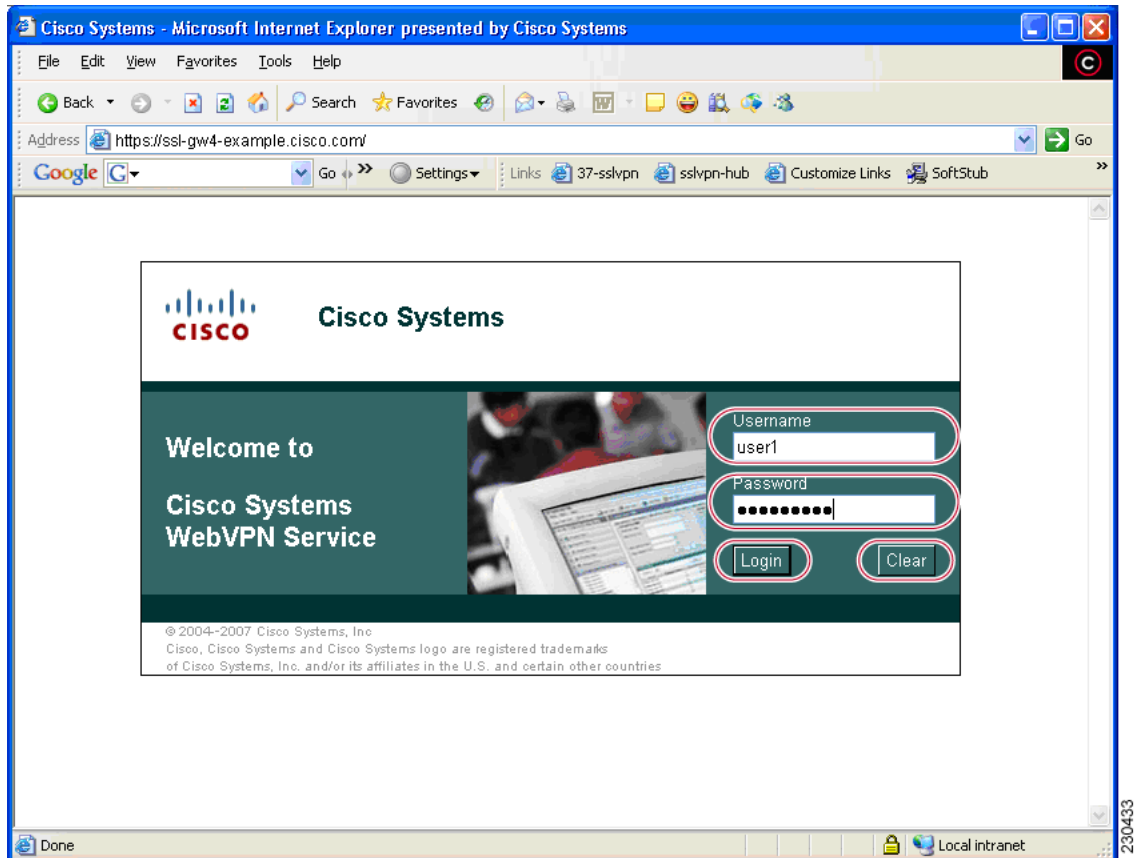
### SSL/TLS Certificate

When the HTTPS connection is established, a warning about the SSL/Transport Layer Security (TLS) certificate may display. If the warning displays, you should install this certificate. If the warning does not display, the system already has a certificate that the browser trusts.

You are then connected to the login page.

## Login Page

The default login page ([Figure 2](#)) prompts you to enter your username and password, which are entered into an HTML form. If an authentication failure occurs, the login page displays an error message.

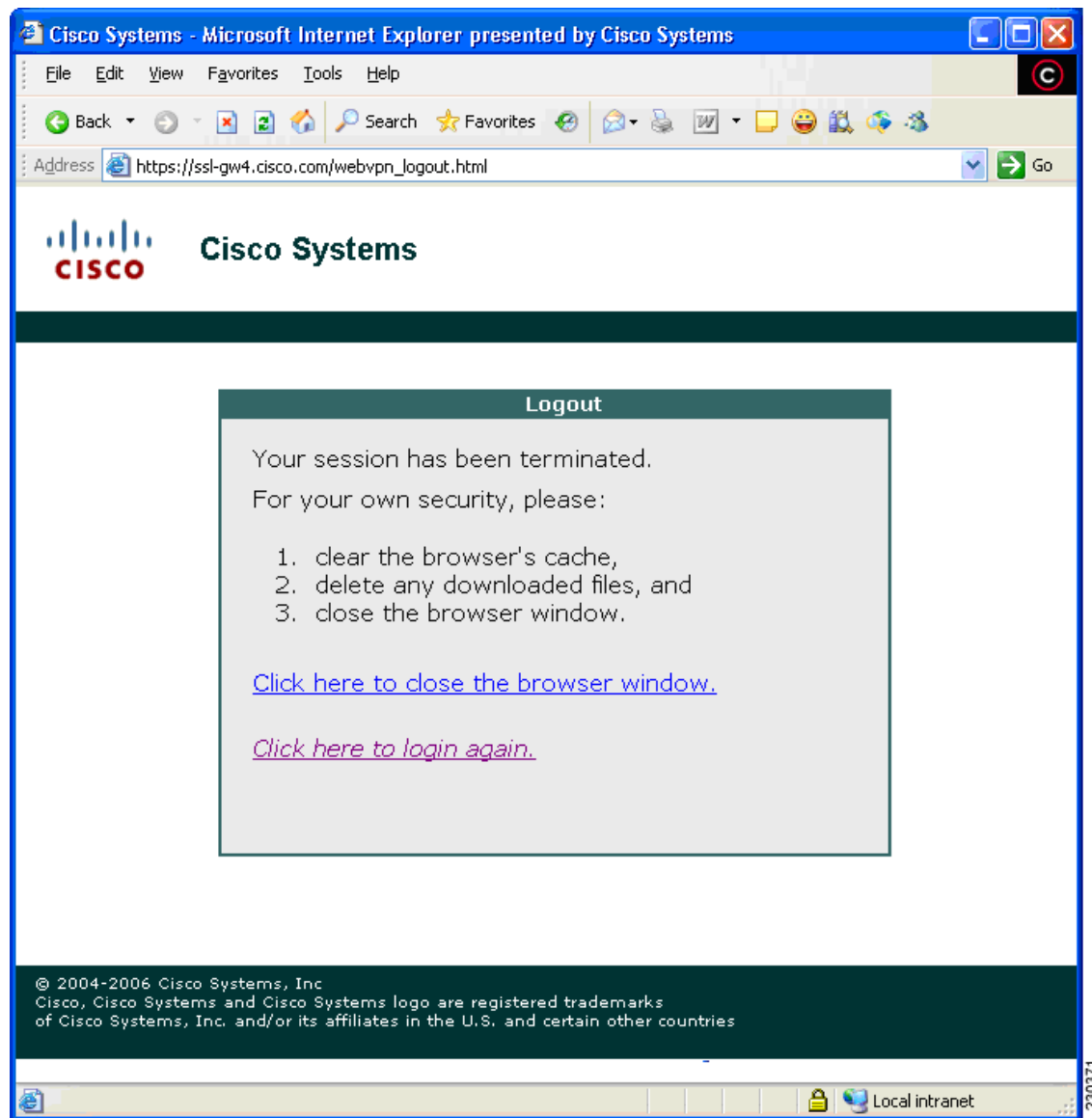
**Figure 2**      **Default Login Page**

## Certificate Authentication

Client certificate authentication is not supported. Only username and password authentication is supported.

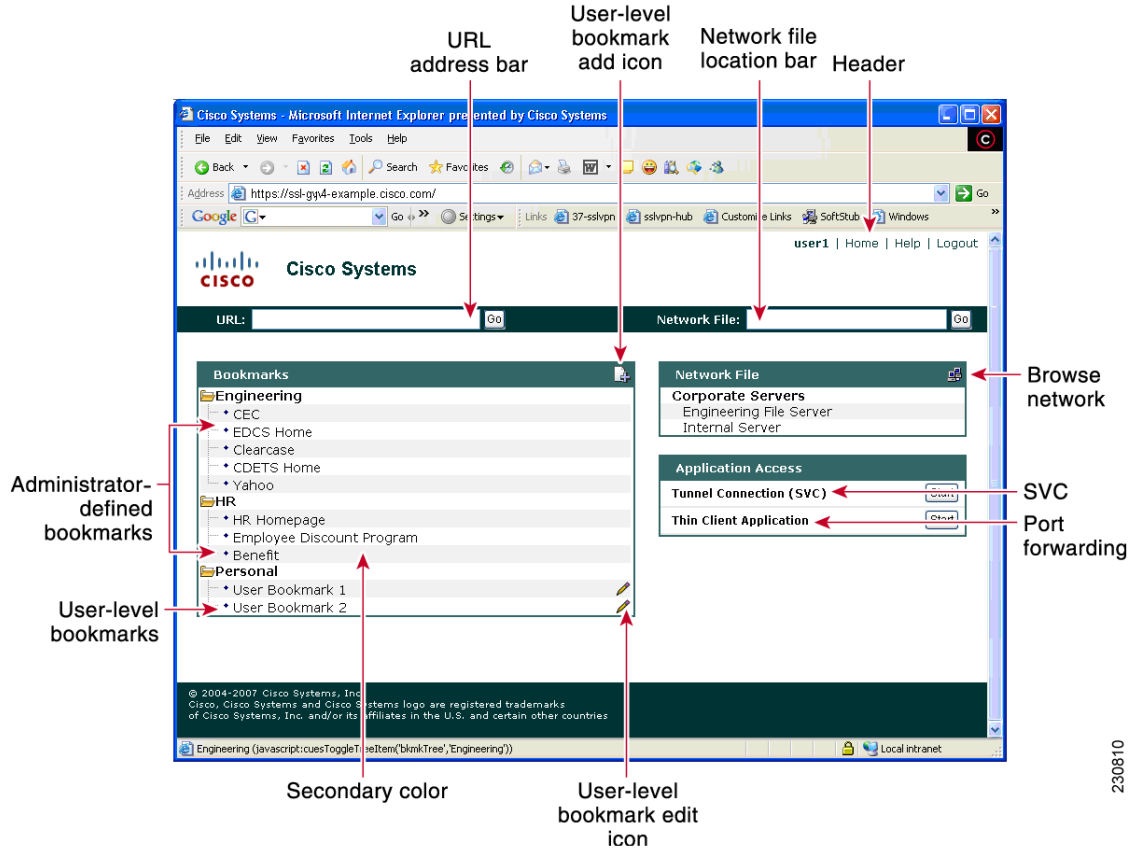
## Logout Page

The logout page ([Figure 3](#)) displays if you click the logout link or if the session terminates because of an idle timeout or a maximum connection time.

**Figure 3 Logout Page**

## Portal Page

The portal page (Figure 4) is the main page for the SSL VPN functionality. See the callouts for functions that exist for administrators and users.

**Figure 4**      **Portal Page**


230810

Table 2 provides information about various fields on the portal page.

**Table 2**      **Information About Fields on the Portal Page**

Field	Description
Administrator-defined bookmarks	Administrator-defined URL lists that cannot be edited by the user.
Browse network	Allows you to browse the file network.
Header	Shares the same color value as the “Title.” Set by the administrator.
Network File location bar	Allows you to access the network share or folder directly by entering \\server\share\folder.
Port forwarding	Downloads the applet and starts port forwarding.
Tunnel connection	Allows you to download the tunnel client and to install tunnel connect.
URL address bar	A new window is opened when you click <b>Go</b> .
User-level bookmark add icon	Clicking the icon opens a dialog box so you can add a new bookmark to the Personal folder.

**Table 2**      **Information About Fields on the Portal Page (continued)**

Field	Description
User-level bookmark edit icon	Allows you to edit or delete an existing bookmark.
User-level bookmarks	<p>You can add a bookmark by using the plus icon (see below)</p> <div data-bbox="862 428 924 493" data-label="Image"></div> <p>on the bookmark panel or toolbar. See the <a href="#">“Toolbar” section on page 9</a> for information about the toolbar. A new window is opened when the link is clicked.</p>

## Remote Servers

You may enter an address or URL path of a website that you want to visit in the text box on the portal page. Pages from the remote server are displayed in the browser window. You can then browse to other links on the page.

## Toolbar

A toolbar has been introduced to help you access the SSL VPN functionalities that are outside the portal page. The toolbar is in the upper right corner of [Figure 5](#) and is outlined in red.

**Figure 5** Website with a Toolbar

The toolbar is expanded below in [Figure 6](#). The sections that follow it explain how to use the toolbar icons.

**Figure 6** Toolbar

## Web Browsing

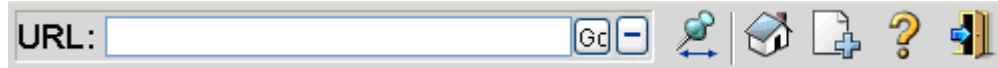
The web browser is the plus icon (see [Figure 7](#)).

**Figure 7** Web Browsing Icon

If you click the web browsing icon (see [Figure 7](#)), the toolbar expands so that you can enter a URL (see [Figure 8](#)).



**Figure 8** *URL Bar*



When a remote user goes to a URL through the URL address bar, the window that is already open is used for display.

## Moving the Toolbar

The push-pin icon (see [Figure 9](#)) allows you to move the toolbar to the right or left side of the portal page.

**Figure 9** *Toolbar Repositioning*



## Returning to the Portal Page

The house icon allows you to return to the portal page (see [Figure 10](#)).

**Figure 10** *Return to the Portal Page*



If the portal page is present in the parent window and you click to return to the portal page, your screen jumps back (sets the focus) to that window; otherwise, the current page is loaded with the portal page.

## Adding the Current Page to the Personal Bookmark Folder

You can add the current page to your personal bookmark folder by clicking the page-with-a-plus icon (see [Figure 11](#)).

**Figure 11** *Adding Current Page to Personal Bookmark Folder*



## Displaying the Help Page

You can display the help page by clicking the question mark icon (see [Figure 12](#)).

**Figure 12**      **Help Page**

## Logging Out

The door icon (see [Figure 13](#)) allows you to log out.

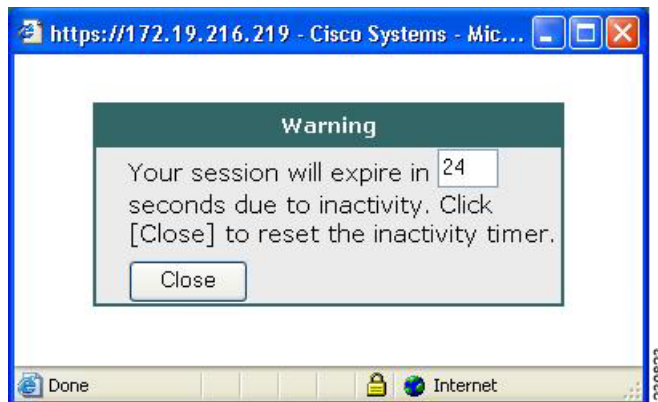
**Figure 13**      **Log Out**

## Session Timeout

You receive a warning message approximately 1 minute before the session is set to expire, and you receive another message when the session expires. On the workstation, the local time indicates when the message was displayed.

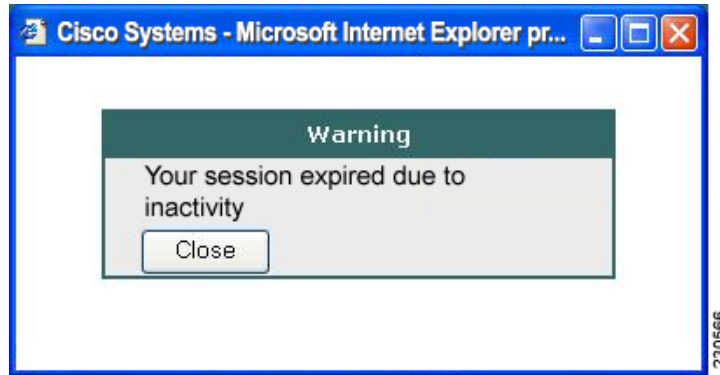
The first message will be similar to the following:

“Your session will expire in x seconds due to inactivity. Click Close to reset the inactivity timer. (browser time and date)” (See [Figure 14](#) below.)

**Figure 14**      **Session Expiration Message**

The last message, as shown below in [Figure 15](#), displays when the time runs out (depending on whether the reason of the session termination is known):

**Figure 15**      *Session Inactivity or Timeout Window*



## TCP Port Forwarding and Thin Client



**Note**

This feature requires the Java Runtime Environment (JRE) version 1.4 or later releases to properly support SSL connections.



**Note**

Because this feature requires installing JRE and configuring the local clients, and because doing so requires administrator permissions on the local system, it is unlikely that you can use applications when you connect from public remote systems.

When you click the Start button of the Thin Client application (under Application Access), a new window is displayed. This window initiates the downloading of a port-forwarding applet. Another window is then displayed. This window asks you to verify the certificate with which this applet is signed. When you accept the certificate, the applet starts running, and port-forwarding entries are displayed (see [Figure 16](#)). The number of active connections and bytes that are sent and received is also listed on this window.

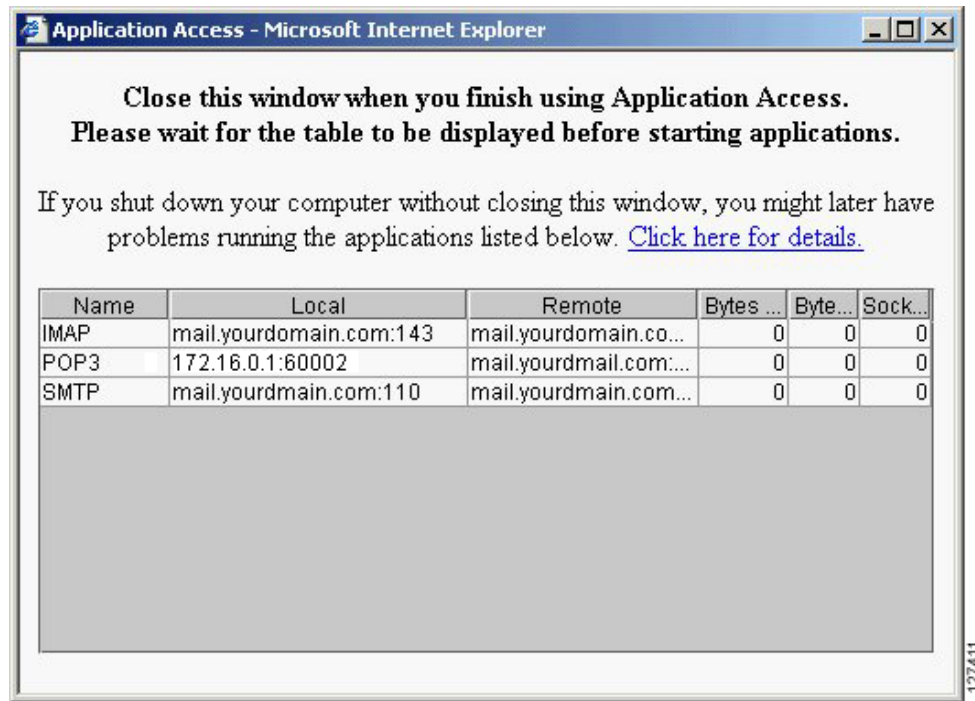


**Note**

When you click the Thin Client link, your system may display a dialog box regarding digital certificates, and this dialog box may appear behind other browser windows. If your connection hangs, minimize the browser windows to find this dialog box.

The administrator should have configured IP addresses, DNS names, and port numbers for the e-mail servers. If they are configured, you can launch the e-mail client, which is configured to contact these e-mail servers and send and receive e-mails. Point of Presence3 (POP3), Internet Message Access Protocol (IMAP), and Simple Mail Transfer Protocol (SMTP) protocols are supported.

The window attempts to close automatically if you are logged out using JavaScript. If the session terminated and a new port forwarding connection is established, the applet displays an error message.

**Figure 16** TCP Port Forwarding Page**Caution**

You should always close the Thin Client window when you finish using applications by clicking the close icon. Failure to quit the window properly can cause Thin Client or the applications to be disabled. See the “[Thin Client—Recovering from Hosts File Error](#)” section on page 18 for details.

Table 3 lists the requirements for Thin Client (Port Forwarding) on your PC or device.

**Table 3** SSL VPN Remote System Thin Client Requirements

Remote User System Requirements	Specifications or Use Suggestions
Client applications installed	—
Cookies enabled on browser	—
Administrator privileges	You must be the local administrator on your PC.
Sun Microsystems JRE version 1.4 or later installed	SSL VPN automatically checks for JRE whenever you start Thin Client. If it is necessary to install JRE, a pop-up window displays, directing you to a site where it is available.

**Table 3**      **SSL VPN Remote System Thin Client Requirements (continued)**

Remote User System Requirements	Specifications or Use Suggestions
Client applications configured, if necessary <b>Note</b> The Microsoft Outlook client does not require this configuration step.	To configure the client application, use the locally mapped IP address and port number of the server. To find this information, do the following: <ul style="list-style-type: none"> <li>• Start SSL VPN on the remote system and click the Thin Client link on the SSL VPN home page. The Thin Client window is displayed.</li> <li>• In the Name column, find the name of the server that you want to use, and then identify its corresponding client IP address and port number (in the Local column).</li> <li>• Use this IP address and port number to configure the client application. The configuration steps vary for each client application.</li> </ul>
Windows XP SP2 patch	If you are running Windows XP SP2, you must install a patch from Microsoft that is available at the following address: <a href="http://support.microsoft.com/?kbid=884020">http://support.microsoft.com/?kbid=884020</a> This problem is a known Microsoft issue.

## Tunnel Connection

In a typical clientless remote access scenario, you establish an SSL tunnel to move data to and from the internal networks at the application layer (for example, web and e-mail). In tunnel mode, you use an SSL tunnel to move data at the network (IP) layer. Therefore, tunnel mode supports most IP-based applications. Tunnel mode supports many popular corporate applications (for example, Microsoft Outlook, Microsoft Exchange, Lotus Notes E-mail, and Telnet).

The tunnel connection is determined by the group policy configuration. The Cisco AnyConnect VPN Client (next-generation SSL VPN Client) is downloaded and installed on your PC, and the tunnel connection is established after the installation.

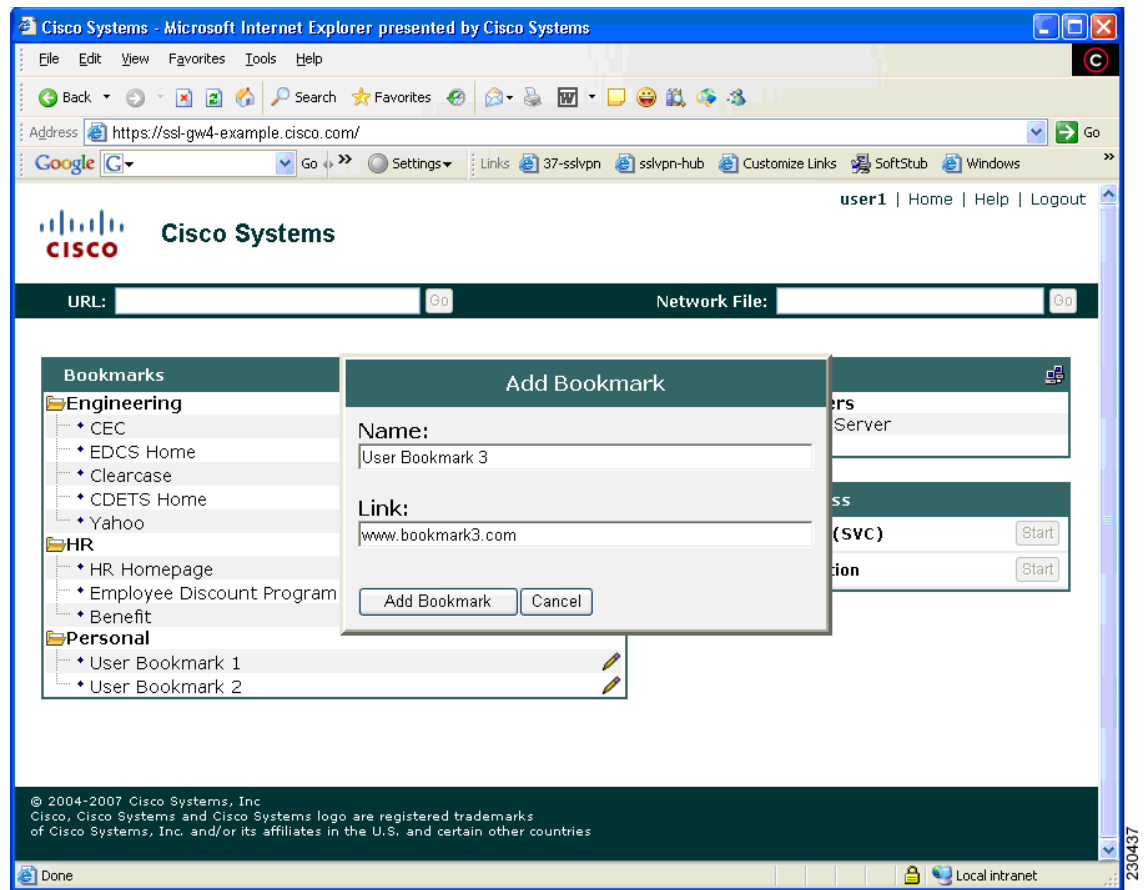
By default, Cisco AnyConnect VPN Client is removed from your PC after the connection is closed. However, you have the option to keep the Cisco AnyConnect VPN Client installed on your PC.

## User-Level Bookmarking

Effective with Cisco IOS Release 12.4(15)T, you can bookmark URLs while connected through an SSL VPN tunnel. You can access the bookmarked URLs by clicking the URL.

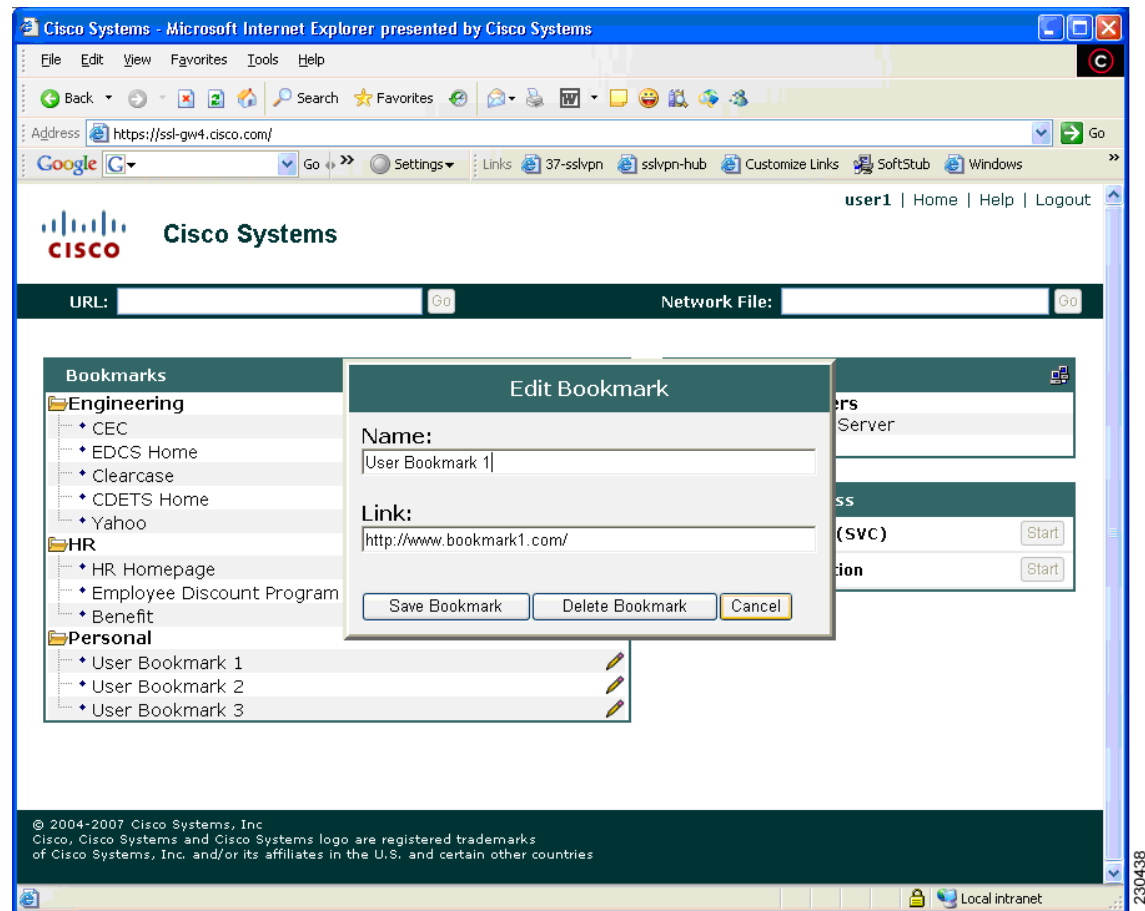
### Adding a Bookmark

Figure 17 shows a typical web page to which a bookmark can be added.

**Figure 17 Add Bookmark**

## Editing a Bookmark

Figure 18 shows a typical web page to which a bookmark can be edited.

**Figure 18**      **Edit Bookmark**

## Security Tips

You should always log out from the SSL VPN session when you are finished. (To log out of SSL VPN, click the logout icon on the SSL VPN toolbar or quit the browser.)

Using SSL VPN does not ensure that communication with every site is secure. SSL VPN ensures the security of data transmission between your PC or workstation and the SSL VPN gateway on the corporate network. If you then access a non-HTTPS web resource (located on the Internet or on the internal network), the communication from the corporate SSL VPN gateway to the destination web server is not secured.

## Browser Caching and Security Implications

If you access SSL VPN through a public or shared Internet system, such as an Internet cafe or kiosk, to ensure the security of your information after terminating or logging out of the SSL VPN session, you must delete all files that you have saved on the PC during the SSL VPN session. These files are not removed automatically upon disconnect.

**Note**

SSL VPN does not save the content of web pages viewed during the session. However, for additional security, we recommend that you clear your browser cache. Deleting content from a PC does not ensure that it cannot be recovered; keep this fact in mind when downloading sensitive data.

## Thin Client—Recovering from Hosts File Error

It is important that you close the Thin Client window properly by clicking the close icon. If you do not close the window properly, the following could occur:

- The next time you try to start Thin Client, it might be disabled; you will receive a “Backup HOSTS File Found” error message.
- The applications might be disabled or might malfunction even when you are running them locally.

These errors can result if you terminate the Thin Client window in any improper way:

- The browser crashes while using Thin Client.
- A power outage or system shutdown occurs while using Thin Client.
- You minimize the Thin Client window and then shut down the computer with the window active (but minimized).

## How SSL VPN Uses the Hosts File

The hosts file on your system maps IP addresses to hostnames. When you start Thin Client, SSL VPN modifies the hosts file by adding SSL VPN-specific entries. When you stop Thin Client by properly closing the Thin Client window, SSL VPN returns the hosts file to its original state. The hosts file goes through the following states:

- Before invoking Thin Client, the hosts file is in its original state.
- When Thin Client starts, SSL VPN does the following:
  1. Copies the hosts file to hosts.webvpn and creates a backup.
  2. Edits the hosts file, inserting SSL VPN-specific information.
- When Thin Client stops, SSL VPN does the following:
  1. Copies the backup file to the hosts file, restoring the hosts file to its original state.
  2. Deletes hosts.webvpn.
- After finishing Thin Client, the hosts file is in its original state.

## What Happens If You Stop Thin Client Improperly

If you improperly terminate Thin Client, the hosts file is left in the SSL VPN-customized state. SSL VPN checks for this possibility the next time you start Thin Client by searching for a hosts.webvpn file. If SSL VPN finds the file, you receive a “Backup HOSTS File Found” error message, and Thin Client is temporarily disabled.

If you improperly shut down Thin Client, you leave the remote access client or server applications in a suspended state. If you start these applications without using SSL VPN, the applications might malfunction. You might find that hosts that you normally connect to are unavailable. This situation could commonly occur if you run applications remotely from home, fail to quit the Thin Client window before shutting down the computer, and then try to run the applications later from the office.



## What to Do

To reenable Thin Client or malfunctioning applications, you should do the following:

- If you can connect to your remote access server, you should follow the steps in the [“Reconfiguring the Hosts File Automatically Using SSL VPN” section on page 19](#).
- If you cannot connect to your remote access server from your current location or if you have made custom edits to the hosts file, you should follow the steps in the [“Reconfiguring the Hosts File Manually” section on page 19](#).

### Reconfiguring the Hosts File Automatically Using SSL VPN

If you can connect to your remote access server, you should follow these steps to reconfigure the hosts file and reenable both Thin Client and the applications:

- 
- Step 1** Start SSL VPN and log in. The portal page opens.
- Step 2** Click the Applications Access link. A “Backup HOSTS File Found” message displays.
- Step 3** Choose one of the following options:
- Restore from backup—SSL VPN forces a proper shutdown. SSL VPN copies the hosts.webvpn backup file to the hosts file, restoring it to its original state, and then deletes the hosts.webvpn backup file. You then have to restart Thin Client.
  - Do nothing—Thin Client does not start. You are returned to the remote access home page.
  - Delete backup—SSL VPN deletes the hosts.webvpn file, leaving the hosts file in its SSL VPN-customized state. The original hosts file settings are lost. Then Thin Client starts, using the SSL VPN-customized hosts file as the new original. Choose this option only if you are unconcerned about losing hosts file settings. If you edited the hosts file after Thin Client has shut down improperly, choose one of the other options, or edit the hosts file manually. (See the [“Reconfiguring the Hosts File Manually” section on page 19](#).)
- 

### Reconfiguring the Hosts File Manually

If you cannot connect to your remote access server from your current location, or if you have customized the hosts file and do not want to lose your edits, you should follow these steps to reconfigure the hosts file and reenable both Thin Client and the applications:

- 
- Step 1** Locate and edit your hosts file.
- Step 2** Check to see if any lines contain the “added by WebVpnPortForward” string.

If any lines contain this string, your hosts file is customized for SSL VPN. If your hosts file is customized, it looks similar to the following example:

```
10.23.0.3 server1 # added by WebVpnPortForward
10.23.0.3 server1.example.com emailxyz.com # added by WebVpnPortForward
10.23.0.4 server2 # added by WebVpnPortForward
10.23.0.4 server2.example.com.emailxyz.com # added by WebVpnPortForward
10.23.0.5 server3 # added by WebVpnPortForward
10.23.0.5 server3.example.com emailxyz.com # added by WebVpnPortForward

Copyright (c) 1993-1999 Microsoft Corp.
#
This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
This file contains the mappings of IP addresses to hostnames. Each
```

```
entry should be kept on an individual line. The IP address should
be placed in the first column followed by the corresponding hostname.
The IP address and the hostname should be separated by at least one
space.
#
Additionally, comments (such as these) may be inserted on individual
lines or following the machine name denoted by a '#' symbol.
#
For example:
#
172.16.102.97 rhino.acme.com # source server
192.168.63.10 x.acme.com # x client host

```

10.23.0.1            localhost

- Step 3**    Delete the lines that contain the “# added by WebVpnPortForward” string.
- Step 4**    Save and close the file.
- Step 5**    Start SSL VPN and log in. Your home page appears.
- Step 6**    Click the Thin Client link. The Thin Client window appears. Thin Client is now enabled.
- 

## Troubleshooting Guidelines

Table 4 provides a list of messages notifying you of various problems, causes, and fixes.

**Table 4**            *Troubleshooting Guidelines*

Message	Cause	Fix
The request to {url} is not allowed. WebVPN has dropped the request. If you have any questions, please ask {...}.	The administrator does not allow you to access a particular URL.	Contact the administrator.
Unable to connect to server {server name}. The server may not exist, or access to it may not be allowed.	Problem with the server.	Check the server name or contact the administrator if it persists.
Unable to find the server {server or url}. The server may not exist, or access to it may not be allowed.	DNS cannot resolve the server name or URL location.	Check the URL address or contact the administrator if it persists.
This (client) machine does not match any identification of a WebVPN user. Please contact your WebVPN provider for assistance.	The client computer does not match any profile of Cisco Secure Desktop (CSD).	Contact the administrator.
This (client) machine does not have the web access privilege. Please contact your WebVPN provider for assistance.	The client computer does not meet the security criteria of having web access functionality through the SSL VPN gateway.	Check the URL to the gateway or contact the administrator if it persists.

**Table 4**      **Troubleshooting Guidelines (continued)**

Message	Cause	Fix
CSD is enabled, but not installed. Please contact your WebVPN provider for assistance.	The CSD has been enabled on the gateway, but it is not available.	Contact the administrator.
The requested information is not available.	Various causes.	Contact the administrator.

## Additional References

The following sections provide references related to SSL VPN.

### Related Documents

Related Topic	Document Title
Security configurations	<i>Cisco IOS Security Configuration Guide</i> , Release 12.4 <a href="http://www.cisco.com/en/US/customer/products/ps6350/products_configuration_guide_book09186a008043360a.html">http://www.cisco.com/en/US/customer/products/ps6350/products_configuration_guide_book09186a008043360a.html</a>
Security commands	<i>Cisco IOS Security Command Reference</i> , Release 12.4T <a href="http://www.cisco.com/en/US/partner/products/ps6441/products_command_reference_book09186a0080497056.html">http://www.cisco.com/en/US/partner/products/ps6441/products_command_reference_book09186a0080497056.html</a>
Cisco Secure Desktop	Cisco Secure Desktop Home Page <a href="http://www.cisco.com/en/US/partner/products/ps6742/tsd_products_support_series_home.html">http://www.cisco.com/en/US/partner/products/ps6742/tsd_products_support_series_home.html</a>
Cisco AnyConnect VPN Client	<ul style="list-style-type: none"> <li><i>Cisco AnyConnect VPN Client Administrator Guide</i></li> <li><i>Release Notes for Cisco AnyConnect VPN Client, Version 2.0</i></li> </ul>
SSL VPN (administrator guide)	<i>SSL VPN</i>

### Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

## MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature.	—

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Feature Information for SSL VPN for Remote Users

Table 5 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 5 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 5** Feature Information for SSL VPN Remote User Guide

Feature Name	Releases	Feature Information
SSL VPN Remote User Guide	12.4(6)T	This section was originally included in the <a href="#">SSL VPN</a> feature document.
Cisco AnyConnect VPN Client	12.4(15)T	<p>This feature is the next-generation SSL VPN Client. The feature provides remote users with secure VPN connections to the router platforms supported by SSL VPN and to the Cisco 5500 Series Adaptive Security Appliances.</p> <p><b>Note</b> Users who are using Cisco IOS software releases before Release 12.4(15)T see the SSL VPN Client GUI interface when they are web browsing. Users who are using Cisco IOS software Release 12.4(15)T and later see the Cisco AnyConnect VPN Client GUI when they are web browsing.</p> <p><b>Note</b> See the restrictions in the “<a href="#">Cisco AnyConnect VPN Client</a>” section on page 3 for features not currently supported by Cisco AnyConnect VPN Client on platforms other than the Cisco ASA 5500 series Adaptive Security Appliance.</p>

**Table 5**      **Feature Information for SSL VPN Remote User Guide (continued)**

Feature Name	Releases	Feature Information
GUI Enhancements	12.4(15)T	<p>These enhancements provide updated examples and explanation of the Web VPN GUIs.</p> <p>The following sections provide information about these updates:</p> <ul style="list-style-type: none"> <li>• <a href="#">Page Flow, page 4</a></li> <li>• <a href="#">Initial Connection, page 5</a></li> <li>• <a href="#">Login Page, page 5</a></li> <li>• <a href="#">Certificate Authentication, page 6</a></li> <li>• <a href="#">Logout Page, page 6</a></li> <li>• <a href="#">Portal Page, page 7</a></li> <li>• <a href="#">Remote Servers, page 9</a></li> <li>• <a href="#">Toolbar, page 9</a></li> <li>• <a href="#">Session Timeout, page 12</a></li> <li>• <a href="#">TCP Port Forwarding and Thin Client, page 13</a></li> <li>• <a href="#">Tunnel Connection, page 15</a></li> <li>• <a href="#">User-Level Bookmarking, page 15</a></li> </ul>

## Notices

The following notices pertain to this software license.

### OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

### License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

#### OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)".
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

**Original SSLeay License:**

Copyright © 1995-1998 Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). All rights reserved.

This package is an SSL implementation written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

---

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)

---

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and



coincidental.

© 2007–2008 Cisco Systems, Inc. All rights reserved.





## **Threat Information Distribution Protocol (TIDP) and TMS**





# Threat Information Distribution Protocol

---

**First Published: February 27, 2006**

**Last Updated: March 20, 2006**

Threat Information Distribution Protocol (TIDP) provides a rapid and secure mechanism to distribute security threat information. TIDP is designed to support large groups of devices throughout the network. TIDP supports peer authentication and message encryption. TIDP is the distribution layer protocol for TIDP-Based Mitigation Services (TMS). TMS provides the framework to rapidly and efficiently distribute threat information to devices across the network. This document describes TIDP configuration. TIDP must be configured before TMS.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all of the features documented in this module.* To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for TIDP” section on page 25](#)

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for TIDP, page 2](#)
- [Restrictions for TIDP, page 2](#)
- [Information About TIDP, page 2](#)
- [How to Configure TIDP, page 4](#)
- [Configuration Examples for TIDP, page 20](#)
- [Additional References, page 22](#)
- [Command Reference, page 24](#)



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

## Prerequisites for TIDP

- You should have a clear understanding of the physical topology and traffic patterns in your network before deploying TIDP and TMS.
- All devices, configured to run TIDP, must be reachable by TIDP peers via TCP/IP.

## Restrictions for TIDP

- In Cisco IOS Release 12.4(6)T, you can configure only a single controller for each TIDP group.
- Only a physical interface with a fixed IP address can be configured with the **tidp source** command.

## Information About TIDP

You should understand the following concepts, before configuring TIDP and TMS:

- [Threat Information Distribution Protocol, page 2](#)
- [TIDP-Based Mitigation Services, page 4](#)

## Threat Information Distribution Protocol

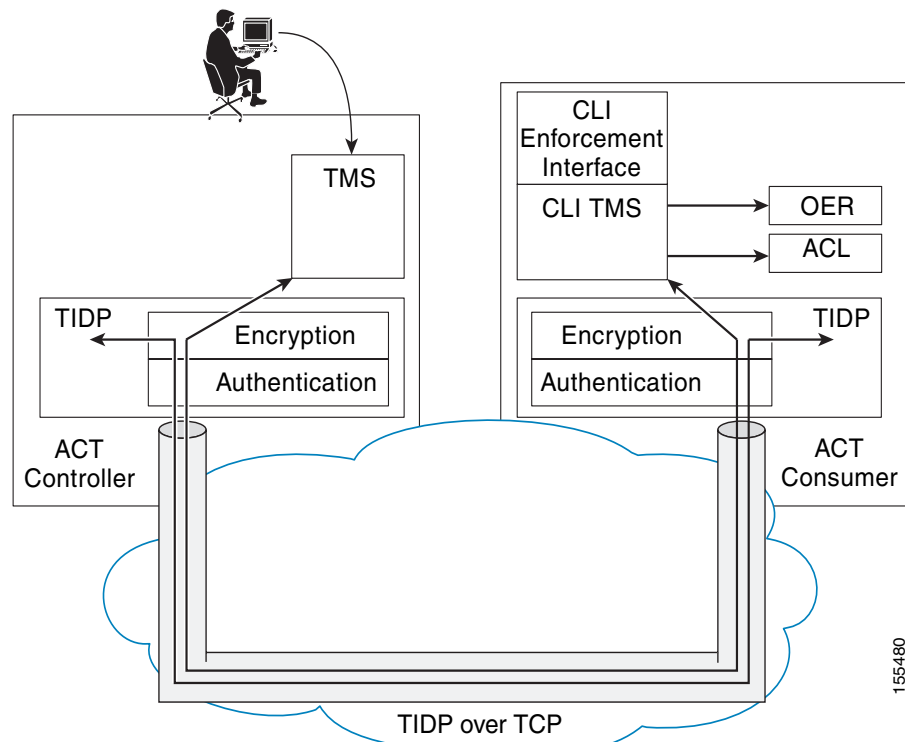
TIDP is a light-weight protocol that provides a rapid, scalable, and secure mechanism to distribute threat information to large groups of devices in the network. TIDP is configured on a per-group basis. Messages are bound to each group but can also be delivered to multiple groups. TIDP is deployed in a star or hub-and-spoke topology, similar to a client/server configuration, in which a controller supports multiple consumers. The controller is configured to peer with all consumers in the group. The consumers peer only with the controller and optionally with each other. [Figure 1](#) shows a sample topology.

**Figure 1**      *The Controller Peers with all Consumers*

## Secure Message Authentication and Encryption

TIDP was designed to be secure. TIDP messages are protected by peer authentication and can be optionally encrypted to prevent the message payload from being viewed or altered. Authentication and encryption are configured with inbound and outbound keys. TIDP can be configured to use AES-128, HMAC-SHA1-160, and RSA key generation. [Figure 2](#) shows TIDP message transport and distribution.

**Figure 2** TMS Service Run Over TIDP



## TIDP-Based Mitigation Services

TIDP is designed to run over only TCP as the transport layer protocol. TIDP is the distribution layer protocol for TIDP-Based Mitigation Services (TMS). TMS provides the framework to rapidly and efficiently distribute threat information to devices across the network.

The TMS framework transports messages that contain specific threat information about suspect traffic and associated mitigation enforcement actions to all devices in the network. Threat Information Messages (TIMs) are distributed throughout the network in near real time. TIMs are distributed from a central device, the TMS controller. TMS consumers are devices configured to receive TIMs. Each consumer can be configured with a unique rule set to locally enforce mitigation actions based on local requirements. Each rule set is customizable and can be modified on demand.



### Note

This document describes TIDP configuration. TIDP must be configured before TMS. For information about TMS, see [TIDP-Based Mitigation Services](#) documentation.

## How to Configure TIDP

This section contains the following tasks:

- [Generating an RSA Key Pair, page 5](#) (optional)



- [Configuring the Remote Peer to Use the RSA Key, page 7](#) (optional)
- [Configuring TIDP Authentication and Encryption Keys, page 9](#) (required)
- [Configuring a TIDP Group, page 13](#) (required)
- [Configuring the Source Interface and Enabling TIDP, page 15](#) (required)
- [Sending a Test Message to Verify that TIDP is Operational, page 17](#) (optional)
- [Using Privileged EXEC Commands to Verify and Troubleshoot TIDP, page 18](#) (optional)

## Generating an RSA Key Pair

This configuration task is optional. The steps in this task show how to generate the RSA key pair and then display the key so that the public key can be copied and input into the remote peer (receiving device).

### Prerequisites

Before configuring the **crypto key generate rsa** command, ensure that your router has a hostname and IP domain name configured (with the **hostname** and **ip domain-name** commands). You will be unable to complete the **crypto key generate rsa** command without a hostname and IP domain name.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto key generate rsa** {general-keys | usage-keys} [label *key-label*] [exportable] [modulus *modulus-size*] [storage *device*:]
4. **exit**
5. **show crypto key mypubkey rsa**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>crypto key generate rsa {general-keys   usage-keys} [label key-label] [exportable] [modulus modulus-size] [storage device:]</b>  <b>Example:</b> Router(config)# crypto key generate rsa general-keys label CRYPTO_KEY_1 modulus 512	Generates an RSA key pair.
Step 4	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits global configuration mode and enters privileged EXEC mode.
Step 5	<b>show crypto key mypubkey rsa</b>  <b>Example:</b> Router# show crypto key mypubkey rsa	Displays the RSA public keys of your router.

## Examples

The following example, starting in global configuration mode, shows how to generate and display an RSA key pair:

```
Router(config)# crypto key generate rsa general-keys label CRYPTO_KEY_1 modulus 512
The name for the keys will be: crypto_key_1
```

```
% The key modulus size is 512 bits
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]
```

```
Router(config)# exit
Router# show crypto key mypubkey rsa
```

```
% Key pair was generated at: 12:45:16 PST Jan 1 2006
Key name: CRYPTO_KEY_1
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00AD3E88 3B3489CB
 A4F77002 97FC4BEC 9AAFE414 973E7B38 B047EACE 5B4857BC 2606EEA3 6704041A
 1F6D9659 89070D18 F4358111 90905012 53EEF5E0 5F41B3FD AB020301 0001
% Key pair was generated at: 12:45:23 PST Jan 9 2006
Key name: CRYPTO_KEY_1.server
Temporary key
Usage: Encryption Key
```

```
Key is not exportable.
Key Data:
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00D13A4D 1A668508
F291D3E3 46500F52 435C3A07 23A66EB0 FA3A0A3B 53DE2DD6 0E24F9B0 825370CB
BFB9E615 97E79BB1 95430760 CB68F399 502B509B 993935B3 A0EBE95C 33BEDD40
471AFCD5 0EB86242 F3F8E741 53C3C14E D20916CF 2BC33422 B5020301 0001
```

## Troubleshooting Tips

See the [Cisco IOS Security Configuration Guide, Release 12.4T](#) for information about crypto key configuration and troubleshooting.

## What to Do Next

The public portion of the key that was generated in this task must be entered on the remote peer. Proceed to the next section for more information.

## Configuring the Remote Peer to Use the RSA Key

This task shows how to enter the senders public RSA key on the remote peer. This task is required if an RSA key is configured for TIDP authentication on the sending device.

## Prerequisites

The IP host statement in this task is optional. The remote peer will attempt to use domain name system (DNS) to resolve the name of the RSA key in the public key chain. If the remote peer is not configured to use DNS resolution, then the sending peer must be identified by configuring the **ip host** command on the remote peer. Configuration of the **ip host** command is optional in this task table.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip host** {rsa-key-name ip-address}
4. **crypto key pubkey-chain rsa**
5. **named-key** key-name [encryption | signature]
6. **address** ip-address
7. **key-string** text-key
8. **quit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip host</b> {rsa-key-name ip-address}  <b>Example:</b> Router(config) ip host CRYPTO_KEY_1 10.1.1.1	(Optional) Configures a static hostname-to-address mapping in the host cache. <ul style="list-style-type: none"><li>This command is required only if DNS resolution is not configured.</li></ul>
Step 4	<b>crypto key pubkey-chain rsa</b>  <b>Example:</b> Router(config)# crypto key pubkey-chain rsa	Enters public key configuration mode to specify an RSA public key for a remote device.
Step 5	<b>named-key</b> key-name [ <b>encryption</b>   <b>signature</b> ]  <b>Example:</b> Router(config-pubkey-chain)# named-key CRYPTO_KEY_1 signature	Places the router in Crypto public key chain configuration mode. <ul style="list-style-type: none"><li>The name of the RSA key configured on the remote peer is entered.</li></ul>
Step 6	<b>address</b> ip-address  <b>Example:</b> Router(config-pubkey-key)# address 10.1.1.1	Specifies the IP address of the remote peer that generated the RSA public key.
Step 7	<b>key-string</b> text-key  <b>Example:</b> Router(config-pubkey-key)# key-string	Specifies the RSA public key of the remote peer. <ul style="list-style-type: none"><li>You will be prompted to enter the public key.</li></ul>
Step 8	<b>quit</b>  <b>Example:</b> Router(config-pubkey) quit	Exits Hex-key input mode, and enters Crypto public key chain configuration mode.

## Examples

The following example, starting in global configuration mode, configures the remote peer to process the RSA key generated in the first configuration task:

```
Router(config)# ip host CRYPTO_KEY_1 10.1.1.1
Router(config)# crypto key pubkey-chain rsa
Router(config-pubkey-chain)# named-key CRYPTO_KEY_1 signature
Router(config-pubkey-key)# address 10.1.1.1
Router(config-pubkey-key)# key-string
Enter a public key as a hexadecimal number
```

```
Router(config-pubkey)# 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00AD3E88
3B3489CB
Router(config-pubkey)# A4F77002 97FC4BEC 9AAFE414 973E7B38 B047EACE 5B4857BC 2606EEA3
6704041A
Router(config-pubkey)# 1F6D9659 89070D18 F4358111 90905012 53EEF5E0 5F41B3FD AB020301 0001
Router(config-pubkey)# quit
```

## Troubleshooting Tips

See the [Cisco IOS Security Configuration Guide, Release 12.4T](#) for information about crypto key configuration and troubleshooting.

## What to Do Next

Proceed to the next section for information on configuring the RSA key for TIDP peer authentication.

## Configuring TIDP Authentication and Encryption Keys

The steps in this task show how to configure TIDP peer authentication and message encryption. Peer authentication is required. Message encryption is optional. TIDP can be configured to use AES-128, HMAC-SHA1-160, and RSA key generation.

### Peer Authentication

TIDP peers are authenticated by configuring an RSA public key or by configuring an authentication string. The authentication string can be encrypted or transmitted as clear text. TIDP performs authentication by signing sent messages and verifying the signature in received messages. Two sets of authentication keys are configured for each TIDP group, a send key and receive key. If a message fails authentication, the invalid message counter is increased incrementally. This counter is displayed in the output of the **show tidp detail** command.

### Message Encryption

TIDP messages can be optionally encrypted to prevent the contents from being viewed or altered. Two sets of encryption keys are configured for each TIDP group, a send key and receive key.

### Locally Encrypting Message and Authentication Strings

A message or authentication string can be encrypted in the router configuration file so that encryption and/or authentication is not compromised for the TIDP group if one peer is compromised. The key string is saved as clear text when the **0** keyword is entered after the **key-string** argument. The key string text is encrypted if the **6** keyword is entered. Configuring the **password encryption aes** command in Global configuration mode will automatically encryption all key-strings in the router configuration file.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **tidp key-set name**

4. **authentication-key send** {**key-string** [0 | 6] *string-text* | **keypair-name** *name*}
5. **authentication-key receive** {**key-string** [0 | 6] *string-text* | **pubkey-name** *name*}
6. **encryption-key receive** {**key-string** [0 | 6] *string-text*}
7. **encryption-key send** {**key-string** [0 | 6] *string-text*}
8. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>tidp key-set name</b>  <b>Example:</b> Router(config)# tidp key-set KEY_1	Enters TIDP key-set configuration mode to configure a key-set for TIDP peer authentication and/or message encryption. <ul style="list-style-type: none"> <li>Authentication and encryption keys are configured in send and receive pairs.</li> <li>Authentication must be configured before a TIDP group can be activated.</li> <li>Encryption key configuration is optional.</li> </ul>
Step 4	<b>authentication-key send {key-string [0   6] string-text   keypair-name name}</b>  <b>Example:</b> Router(config-tidp-ks)# authentication-key send keypair-name CRYPTO_KEY_1	Configures an authentication key for sent TIDP messages. <ul style="list-style-type: none"> <li>The authentication key can be configured as an RSA key, an encrypted text string, or as clear text.</li> <li>There is a 32 character limit for configuring text strings.</li> <li>Entering the <b>0</b> keyword configures a clear text string. Entering the <b>6</b> keyword configures an encrypted text string.</li> <li>In the example, an authentication is configured using the RSA key pair that was generated in the first task.</li> </ul>
Step 5	<b>authentication-key receive {key-string [0   6] string-text   pubkey-name name}</b>  <b>Example:</b> Router(config-tidp-ks)# authentication-key receive key-string 6 Aa1Bb2Cc3	Configures an authentication key for received TIDP messages. <ul style="list-style-type: none"> <li>The receive key must match the send key configured on the remote peer in order for authentication to occur.</li> <li>In the example, the <b>6</b> keyword is entered to encrypt the authentication string.</li> </ul>
Step 6	<b>encryption-key send {key-string [0   6] string-text}</b>  <b>Example:</b> Router(config-tidp-ks)# encryption-key receive Dd4Ee5Ff6	(Optional) Configures an encryption key to encrypt the contents of received TIDP messages. <ul style="list-style-type: none"> <li>Entering the <b>6</b> keyword encrypt the key-string in the router configuration file. The key string is saved as clear text by default.</li> </ul>

	Command or Action	Purpose
Step 7	<b>encryption-key send</b> {key-string [0   6] string-text} <p><b>Example:</b>  Router(config-tidp-ks)# encryption-key send  Gg7Hh8Ii9</p>	Configures an encryption key to decrypt the contents of received TIDP messages. <ul style="list-style-type: none"> <li>The receive key must match the send key configured on the remote peer in order for authentication to occur.</li> </ul>
Step 8	<b>exit</b> <p><b>Example:</b>  Router(config-tidp-ks)# exit</p>	Exits TIDP key-set configuration mode, and enters global configuration mode.

## Examples

The following examples, starting in global configuration mode, configure an encryption key and authentication key between two TIDP peers.

### Sending Peer Key-Set

```
Router(config)# _tidp key-set KEY_1
Router(config-tidp-ks)# authentication-key send keypair-name CRYPTO_KEY_1
Router(config-tidp-ks)# encryption-key send key-string 6 Aa1Bb2Cc3
Router(config-tidp-ks)# exit
```

### Receiving Peer Key-Set

```
Router(config)# _tidp key-set KEY_2
Router(config-tidp-ks)# authentication-key receive pub-key CRYPTO_KEY_1
Router(config-tidp-ks)# encryption-key receive key-string 6 Aa1Bb2Cc3
Router(config-tidp-ks)# exit
```

## Troubleshooting Tips

If a connection has been established, then the existing authentication and/or encryption keys are compatible. If a connection is not established, verify the following:

- The peer is reachable via TCP/IP.
- The authentication key is properly configured on the sender and receiver. Also, verify the encryption key configuration, if one is configured.

If these tips do not resolve the problem, then you should check syslog for CONNFAIL error messages from the peer initiating the connection. The following debug command can also be helpful in troubleshooting a TIDP connection problem:

- Enabling the **debug tidp test** command allows you to send TIDP test messages. This command must be enabled on both the sender and receiver.
- Enabling the **debug tidp registration** command is helpful for troubleshooting authentication/encryption key mismatches.
- Enabling the **debug tidp packets** is helpful for troubleshooting key mismatches and general communication problems.



## What to Do Next

The next task is to configure a TIDP group. Proceed to the next task for more information.

## Configuring a TIDP Group

TIDP groups are designed to manage the distribution of threat information to TIDP consumers. The steps in this task show the following:

- TIDP group creation
- Associating the group with a key set for peer authentication and/or message encryption
- Configuring the time interval at which TIDP registers peers
- TIDP group activation

## TIDP Groups

TIDP is deployed in groups following a star topology. Each group is configured with at least one TIDP controller. The controller is configured to communicate with each TIDP consumer. The consumer is configured to communicate only with the controller. Each group can have a maximum of 250 consumers. Each consumer can be a member of up to 64 groups.

## Prerequisites

Peer authentication is required and must be configured before a TIDP group can be activated. A key-set is first configured with the **tidp key-set** command in global configuration mode. The authentication and encryption keys are associated with the TIDP group by configuring the **key-set** command in Step 4.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **tidp group** *number*
4. **key-set** *name*
5. **peer** *ip-address*
6. **registration retry-interval** {**min** *interval* **max** *interval*}
7. **active**
8. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>tidp group</b> <i>number</i>  <b>Example:</b> Router(config)# tidp group 10	Creates the TIDP group, and enters TIDP group configuration mode.
Step 4	<b>key-set</b> <i>name</i>  <b>Example:</b> Router(config-tidp-grp)# key-set KEY_1	Associates a key-set with a TIDP group. <ul style="list-style-type: none"> <li>A valid key-set must be associated before the group can be activated.</li> </ul>
Step 5	<b>peer</b> <i>ip-address</i>  <b>Example:</b> Router(config-tidp-grp)# peer 10.1.1.2	Configures a TIDP peer as a member of a TIDP group. <ul style="list-style-type: none"> <li>The IP address of the interface that is configured as the TIDP source on the remote peer is entered for the <i>ip-address</i> argument.</li> <li>The TIDP peer must be reachable via TCP/IP before it can be configured to be a member of a TIDP group.</li> </ul>
Step 6	<b>registration retry-interval</b> { <i>min interval max interval</i> }  <b>Example:</b> Router(config-tidp-grp)# registration retry-interval min 30 max 600	Configures the length of time and number of attempts for TIDP group registration. <ul style="list-style-type: none"> <li>By default, TIDP will attempt register group members once every 60 seconds for up to 1 hour or until all group members have been registered.</li> <li>Registration timers are reset to zero when this command is configured or reconfigured.</li> <li>The example configures TIDP to attempt peer registration every 30 seconds for up to 10 minutes.</li> </ul>
Step 7	<b>active</b>  <b>Example:</b> Router(config-tidp-grp)# active	Activates the TIDP group. <ul style="list-style-type: none"> <li>The group cannot be activated until a key-set with valid authentication key is associated with the <b>key-set</b> command.</li> </ul>
Step 8	<b>exit</b>  <b>Example:</b> Router(config-tidp-grp)# exit	Exits TIDP Group configuration mode, and enters global configuration mode.

## Examples

The following examples, starting in global configuration mode, configure TIDP group number 10 on a controller and consumer:

#### Controller (10.1.1.1)

```
Router(config)# tidp key-set KEY_1
Router(config-tidp-ks)# authentication-key receive key-string Aa1Bb2Cc3
Router(config-tidp-ks)# authentication-key send key-string Dd4Ee5Ff6
Router(config-tidp-ks)# exit
Router(config)# tidp group 10
Router(config-tidp-grp)# key-set KEY_1
Router(config-tidp-grp)# registration retry-interval min 30 max 600
Router(config-tidp-grp)# peer 10.1.1.2
Router(config-tidp-grp)# peer 10.1.1.3
Router(config-tidp-grp)# peer 10.1.1.4
Router(config-tidp-grp)# active
Router(config-tidp-grp)# exit
```

#### Consumer (10.1.1.2)

```
Router(config)# tidp-set KEY_2
Router(config-tidp-ks)# authentication-key receive key-string Dd4Ee5Ff6
Router(config-tidp-ks)# authentication-key send key-string Aa1Bb2Cc3
Router(config-tidp-ks)# exit
Router(config)# tidp group 10
Router(config-tidp-grp)# key-set KEY_2
Router(config-tidp-grp)# peer 10.1.1.1
Router(config-tidp-grp)# active
Router(config-tidp-grp)# exit
```

## What to Do Next

An interface must be configured as the source for TIDP communication before TIDP can be enabled. Proceed to the next section for more information.

## Configuring the Source Interface and Enabling TIDP

The steps in this task show how to configure the source interface for TIDP communication and enable TIDP globally on a router.

### Enabling and Disabling TIDP

The source interface must be configured before TIDP can be enabled globally on a router. The source interface cannot be reconfigured while TIDP is enabled. TIDP can be disabled globally on a router by entering the **no** form of the **tidp enable** command. The TIDP configuration is not removed from the router configuration file when the **no** form of this command is entered.

### Prerequisites

A physical interface, configured with a fixed IP address, must be in an enabled state and reachable by TIDP peers via TCP/IP.

## Restrictions

An interface that is configured with a dynamic IP address cannot be configured as the TIDP source interface.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **tidp source *ip-address***
4. **tidp enable**
5. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>tidp source <i>ip-address</i></b>  <b>Example:</b> Router(config)# tidp source 10.1.1.1	Configures the source interface for TIDP communication. <ul style="list-style-type: none"><li>The source interface must be a physical interface with a fixed IP address.</li></ul>
Step 4	<b>tidp enable</b>  <b>Example:</b> Router(config)# tidp enable	Enables TIDP globally on a router. <ul style="list-style-type: none"><li>Entering the <b>no</b> form disables TIDP without removing the TIDP configuration from the router configuration file.</li></ul>
Step 5	<b>end</b>  <b>Example:</b> Router(config)# end	Exits global configuration mode, and enters privileged EXEC mode.

## Examples

The following example, starting in global configuration mode, configures interface Ethernet 0/0 as the source interface for communication with TIDP peers:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# tidp source 10.1.1.1
Router(config)# end
```

## What to Do Next

Configuring the source interface and enabling TIDP completes TIDP configuration. Proceed to the next sections to see information about verifying and troubleshooting TIDP. For information on configuring TMS, see [TIDP-Based Mitigation Services](#) documentation.

## Sending a Test Message to Verify that TIDP is Operational

The steps in this task show how to verify the operational status of TIDP.

### Enabling the TIDP Test CLI

The **test tidp** command is used to transmit a text message to a TIDP group or peer. The **test tidp** command is not visible or configurable until the **debug tidp** command has been entered with the **test** keyword. TIDP test debugging must be enabled on the source and destination devices.

#### SUMMARY STEPS

1. **enable**
2. **debug tidp test**
3. **test tidp send group** *number* [**peer** *ip-address*] *message-string*

#### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>debug tidp test</b>  <b>Example:</b> Router# debug tidp test	Enables the TIDP test CLI.
Step 3	<b>test tidp send group</b> <i>number</i> [ <b>peer</b> <i>ip-address</i> ] <i>message-string</i>  <b>Example:</b> Router# test tidp send group 10 Group_Message	Sends a test message to a TIDP group or peer. <ul style="list-style-type: none"> <li>• An alphanumeric text message up to 35 characters in length can be sent. White space is not permitted in the message string.</li> </ul>

## Examples

The following example shows a test message sent to the 10.1.1.2 peer in TIDP group 10:

#### Sender (10.1.1.1)

```
Router1# debug tidp test
```

```
TIDP test debugging is on
```

```
Router1# test tidp send group 10 peer 10.1.1.2 Unicast_Test_Message
```

**Receiver (10.1.1.2)**

```
Router2# debug tidp test
TIDP test debugging is on
Router2#
03:36:03: TIDP msg from 10.1.1.1, group 10: 'Unicast_Test_Message'
```

## Troubleshooting Tips

If a test message is not received by a group or peer, you should verify the following:

- The **debug tidp test** command has been enabled on the sender and receiver.
- The source interface on each device is enabled and reachable via TCP/IP.
- There are no errors or inconsistencies in sending and receiving authentication and/or encryption keys.

## What to Do Next

Proceed to the next section to see information about verifying and troubleshooting TIDP.

## Using Privileged EXEC Commands to Verify and Troubleshoot TIDP

This section describes **clear**, **debug**, and **show** commands that are used to verify the operational status and configuration of TIDP. All commands in this section are optional.

### SUMMARY STEPS

1. **enable**
2. **clear tidp counters** [group {*number* | **all**}]
3. **debug tidp** {errors | events | packets | registration | test}
4. **show tidp** [detail]
5. **show tidp group** {*number* | **all**} [detail]
6. **show tidp key-set** [*name*]
7. **show tidp peer** {*ip-address* | **all**}

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>clear tidp counters</b> [ <b>group</b> { <i>number</i>   <b>all</b> }]  <b>Example:</b> Router# clear tidp counters	Clears TIDP counters and message statistics. <ul style="list-style-type: none"> <li>The example clears all counters and messages statistics.</li> </ul>
Step 3	<b>debug tidp</b> { <b>errors</b>   <b>events</b>   <b>packets</b>   <b>registration</b>   <b>test</b> }  <b>Example:</b> Router# debug tidp events	Enables TIDP debugging.
Step 4	<b>show tidp</b> [ <b>detail</b> ]  <b>Example:</b> Router# show tidp	Displays the status of TIDP. <ul style="list-style-type: none"> <li>This command displays the operational status, source interface, and groups of which this device is a member.</li> <li>Entering the <b>detail</b> keyword displays the same information but also includes message statistics.</li> </ul>
Step 5	<b>show tidp group</b> { <i>number</i>   <b>all</b> } [ <b>detail</b> ]  <b>Example:</b> Router# show tidp group all	Displays information about TIDP groups. <ul style="list-style-type: none"> <li>This command displays the active status, total number of registered and unregistered peer, registration timer values, and associated key-set.</li> <li>Entering the <b>detail</b> keyword displays group message statistics.</li> </ul>
Step 6	<b>show tidp key-set</b> [ <i>name</i> ]  <b>Example:</b> Router# show tidp key-set	Displays information about locally configured key-sets. <ul style="list-style-type: none"> <li>The group associated with the key-set is displayed in the output.</li> <li>The example displays all locally configured key-sets.</li> </ul>
Step 7	<b>show tidp peer</b> { <i>ip-address</i>   <b>all</b> }  <b>Example:</b> Router# show tidp peer all	Displays information about TIDP peers. <ul style="list-style-type: none"> <li>The output of this command displays connection status, group membership, and message statistics for a single TIDP peer or all peers.</li> </ul>

## Examples

The following is sample output from the **show tidp** command:

```
Router# show tidp

Global TIDP information:
TIDP status: enabled
TIDP source: 10.1.1.1
```

TIDP groups: 1 (1 active, 0 inactive)

The following is sample output from the **show tidp group** command:

```
Router# show tidp group 10
```

```
TIDP Group 10:
 Group status: active
 Total registered peers: 2
 Total unregistered peers: 1
 Registration retry interval - min: 60, max: 3600
 Key-set: KEY_1
```

The following is sample output for the **show tidp key-set** command:

```
Router# show tidp key-set KEY_1
```

```
TIDP keyset KEY_1:
 Groups:
 10
```

The following is sample output for the **show tidp peer** command:

```
Router# show tidp peer 10.1.1.3
```

```
TIDP Peer 10.1.1.3:
 Peer state: Connected
 Configured in groups:
 10
 Total messages received: 1
 Total messages transmitted: 1
 Total messages transmit dropped: 0
 Duplicate messages received: 0
 Replayed messages received: 0
```

## Configuration Examples for TIDP

This section provides TIDP controller and consumer examples. These configurations are similar to each other. The main difference is that TIDP peering is configured between the controller and each peer. However, the TIDP consumers are configured to peer only with the controller and not other peers.

- [TIDP Controller: Example, page 20](#)
- [TIDP Consumer: Example, page 21](#)

### TIDP Controller: Example

Ethernet 0/0 is configured as the source interface for TIDP communication.

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# tidp source 10.1.1.1
```

An RSA key named CRYPTO\_KEY\_1 is generated.

```
Router(config)# crypto key generate rsa general-keys label CRYPTO_KEY_1 modulus 512
The name for the keys will be: crypto_key_1
```



```
% The key modulus size is 512 bits
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]
```

```
Router(config)# exit
```

Key-set KEY\_1 is configured with an authentication and encryption key-set. The RSA key in generated in the previous step is configured as the sender authentication key.

```
Router(config)# tidp key-set KEY_1
Router(config-tidp-ks)# authentication-key send keypair-name CRYPTO_KEY_1
Router(config-tidp-ks)# authentication-key receive key-string 6 Aa1Bb2Cc3
Router(config-tidp-ks)# encryption-key receive key-string 6 Dd4Ee5Ff6
Router(config-tidp-ks)# encryption-key send key-string 6 Gg7Hh8Ii9
Router(config-tidp-ks)# exit
```

TIDP group 10 is configured and activated. KEY\_1 is associated with group 10. The peer registration timers are configured to register unregistered peer at 30 second intervals for up to 10 minutes. Remote peers in the 10.1.1/24 network are configured as TIDP peers.

```
Router(config)# tidp group 10
Router(config-tidp-grp)# key-set KEY_1
Router(config-tidp-grp)# registration retry-interval min 30 max 600
Router(config-tidp-grp)# peer 10.1.1.2
Router(config-tidp-grp)# peer 10.1.1.3
Router(config-tidp-grp)# peer 10.1.1.4
Router(config-tidp-grp)# active
Router(config-tidp-grp)# exit
```

TIDP is enabled globally on the router. This is the final step of the TIDP configuration.

```
Router(config)# tidp enable
```

## TIDP Consumer: Example

Ethernet 0/0 is configured as the source interface for TIDP communication.

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ip address 10.1.1.2 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# tidp source 10.1.1.2
```

The TIDP consumer is configured to process the RSA key generated on the controller. An IP host statement is entered to configure a static hostname-to-IP-address mapping.

```
Router(config)# ip host CRYPTO_KEY_1 10.1.1.1
Router(config)# crypto key pubkey-chain rsa
Router(config-pubkey-chain)# named-key CRYPTO_KEY_1 signature
Router(config-pubkey-key)# address 10.1.1.1
Router(config-pubkey-key)# key-string
Enter a public key as a hexadecimal number

Router(config-pubkey)# 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00AD3E88
3B3489CB
Router(config-pubkey)# A4F77002 97FC4BEC 9AAFE414 973E7B38 B047EACE 5B4857BC 2606EEA3
6704041A
Router(config-pubkey)# 1F6D9659 89070D18 F4358111 90905012 53EEF5E0 5F41B3FD AB020301 0001
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(config-pubkey-chain)# exit
```

Key-set KEY\_2 is configured with an authentication and encryption key-set. The RSA key in processed in the previous step is configured as the receiving authentication key.

```
Router(config)# tidp key-set KEY_2
Router(config-tidp-ks) # authentication-key receive pubkey-name CRYPTO_KEY_1
Router(config-tidp-ks) # authentication-key send key-string 6 Aa1Bb2Cc3
Router(config-tidp-ks) # encryption-key receive key-string 6 Dd4Ee5Ff6
Router(config-tidp-ks) # encryption-key send key-string 6 Gg7Hh8Ii9
Router(config-tidp-ks) # exit
```

TIDP group 10 is configured and activated. KEY\_2 is associated with group 10. Peering is established only with the TIDP controller.

```
Router(config)# tidp group 10
Router(config-tidp-grp) # key-set KEY_2
Router(config-tidp-grp) # peer 10.1.1.1
Router(config-tidp-grp) # active
Router(config-tidp-grp) # exit
```

TIDP is enabled globally on the router.

```
Router(config)# tidp enable
```

## Where to Go Next

This document describes the configuration of TIDP. After TIDP is up and running, see TIDP-Based Mitigation Services (TMS) documentation for information about configuring TMS.

## Additional References

The following sections provide references related to TIDP:

### Related Documents

Related Topic	Document Title
Cisco IOS Security Configuration Guide	<i>Cisco IOS Security Configuration Guide</i> , Release 12.4T <a href="http://www.cisco.com/en/US/partner/products/ps6441/products_configuration_guide_book09186a008049e249.html">http://www.cisco.com/en/US/partner/products/ps6441/products_configuration_guide_book09186a008049e249.html</a>
Cisco IOS Security Command Reference	<i>Cisco IOS Security Command Reference</i> , Release 12.4T <a href="http://www.cisco.com/en/US/partner/products/ps6441/products_command_reference_book09186a0080497056.html">http://www.cisco.com/en/US/partner/products/ps6441/products_command_reference_book09186a0080497056.html</a>
TIDP-Based Mitigation Services	<i>TIDP-Based Mitigation Services</i> <a href="http://www.cisco.com/en/US/customer/products/ps6441/products_feature_guide09186a00805ec975.html">http://www.cisco.com/en/US/customer/products/ps6441/products_feature_guide09186a00805ec975.html</a>

## Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

## MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB gateways, go to the Cisco MIB website on Cisco.com at the following URL: <a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a>

## RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature.	—

## Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Command Reference

The following commands are introduced or modified in the feature or features

- **active**
- **authentication-key receive**
- **authentication-key send**
- **clear tidp counters**
- **debug tidp**
- **encryption-key receive**
- **encryption-key send**
- **key-set**
- **peer**
- **registration retry-interval (TIDP)**
- **show tidp**
- **show tidp group**
- **show tidp key-set**
- **show tidp peer**
- **test tidp**
- **tidp enable**
- **tidp group**
- **tidp key-set**
- **tidp source**

For information about these commands, see the Cisco IOS Security Command Reference at [http://www.cisco.com/en/US/docs/ios/security/command/reference/sec\\_book.html](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html).

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

# Feature Information for TIDP

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1**      **Feature Information for TIDP**

<b>TIDP-Based Mitigation Services</b>	12.4(6)T	TIDP provides a rapid and secure mechanism to distribute security threat information. TIDP is designed to support large groups of devices throughout the network. TIDP supports peer authentication and message encryption. TIDP is the distribution layer protocol for TIDP Based Mitigation Services (TMS). TMS provides the framework to rapidly and efficiently distribute threat information to devices across the network.
---------------------------------------	----------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



# TIDP Based Mitigation Services

---

**First Published: February 27, 2006**

**Last Updated: March 20, 2006**

Threat Information Distribution Protocol (TIDP) is the distribution layer protocol for TIDP Based Mitigation Services (TMS). TMS provides the framework to rapidly and efficiently distribute threat information to devices across the network. The TMS framework transports messages that contain specific threat information about suspect traffic and associated mitigation enforcement actions to all devices in the network. Threat Information Messages (TIMs) are distributed throughout the network in near real time. TIMs are distributed from a central device, the TMS controller. TMS consumers are devices configured to receive TIMs. Each consumer can be configured with a unique rule set to locally enforce mitigation actions based on local requirements. Local rule sets can be customized on demand.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for TMS](#)” section on [page 66](#)*

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for TMS, page 2](#)
- [Restrictions for TMS, page 2](#)
- [Information About TMS, page 2](#)
- [How to Configure TMS, page 10](#)
- [Configuration Examples for TMS, page 59](#)
- [Additional References, page 61](#)



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2007 Cisco Systems, Inc. All rights reserved.

- [Command Reference, page 64](#)

## Prerequisites for TMS

- You should have a clear understanding of the physical topology and traffic patterns in your network before deploying TIDP and TMS.
- This document assumes that all devices, on which TMS services are to be deployed, have been preconfigured to run TIDP. If TIDP has not been configured, use the following document to configure TIDP before continuing with TMS configuration: [Threat Information Distribution Protocol](#).

## Restrictions for TMS

The following restrictions apply to TMS in Cisco IOS Release 12.4(6)T:

- High availability (HA) features are not supported.
- Only one controller can be configured for each TMS group. However, up to 250 consumers can be configured in one or more groups. Up to 64 groups can be configured in a network.

## Information About TMS

You should understand the following concepts, before configuring TMS:

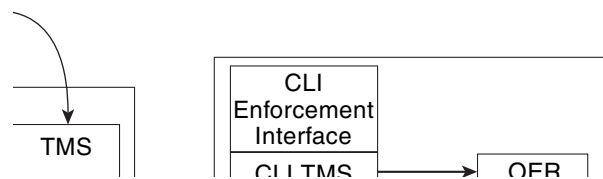
- [Threat Information Distribution Protocol, page 2](#)
- [TIDP Based Mitigation Services, page 3](#)
- [Threat Information Messages, page 4](#)
- [TMS Protocol Configuration, page 5](#)
- [Mitigation Enforcement Actions, page 6](#)
- [TMS Rules Engine Configuration, page 7](#)
- [Local Device Exceptions, page 8](#)
- [TMS System Logging, page 8](#)

## Threat Information Distribution Protocol

TIDP Based Mitigation Services (TMS) run over Threat Information Distribution Protocol (TIDP). TIDP is the distribution layer protocol that runs over of TCP (transport layer protocol). TIDP distributes Threat Information Messages (TIMs), for TMS, across the network in near real time.

[Figure 1](#) shows TIDP distribution and transport.

**Figure 1** *TMS Service Run over TIDP*



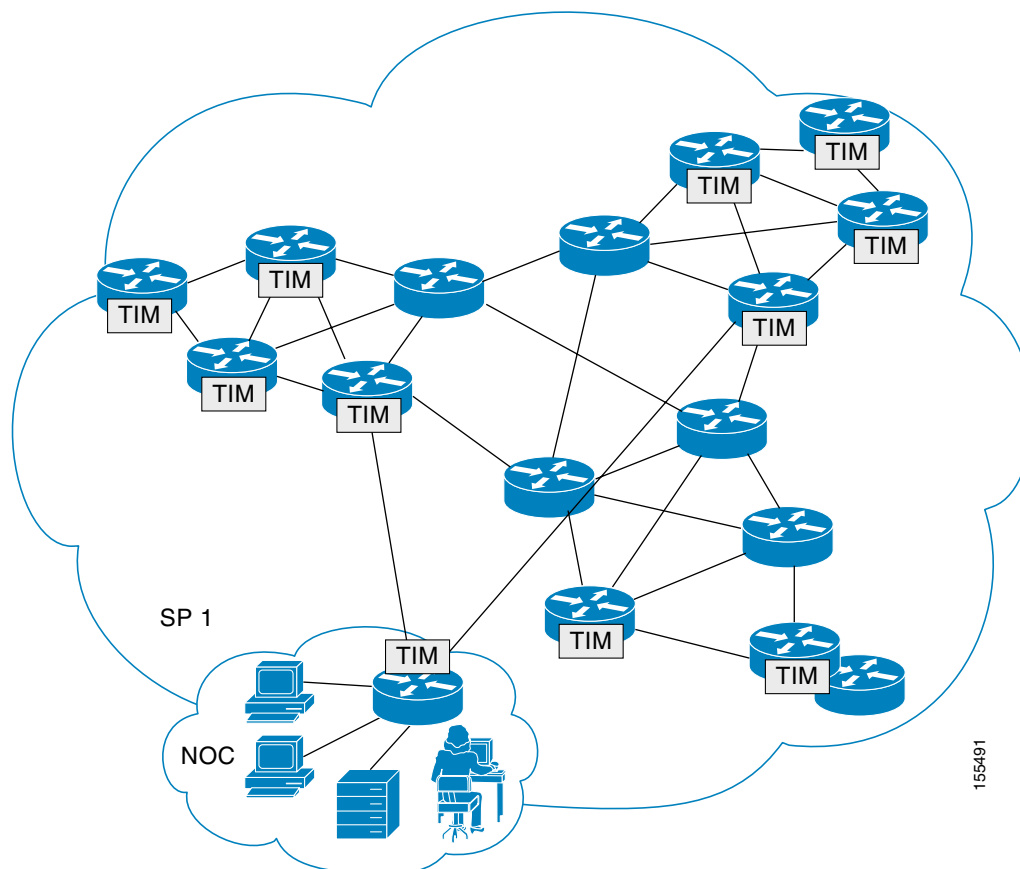
TIDP is designed to be a scalable and secure. TIDP supports point-to-point and point-to-multipoint communication. TIDP provides secure communication and message distribution. Message authentication is configured for all TIDP peering sessions. The message payload can be optionally encrypted to protect the contents. Authentication and encryption are configured using AES-128, HMAC-SHA1-160, or RSA key generation. TIDP is designed with replay protection (an attack that reuses old TCP sequence numbers to flood packets).

## TIDP Based Mitigation Services

TMS provides the framework to rapidly and efficiently distribute Threat Information Messages (TIMs) to devices across the network. The network administrator distributes one or more TIMs from a central location, such as the network operations center (NOC). The TMS framework transports TIMs that contain specific threat information about suspect traffic and an associated mitigation enforcement actions to all devices in the network. [Figure 2](#) shows TMS message distribution.



**Figure 2** *Threat Information Messages are Distributed over the TMS Framework*



TMS provides a scalable point-to-point or point-to-multipoint framework. A TIM can be sent from the TMS controller to a single device (TMS consumer) or all devices in the network. Each TIM message is structured to identify suspect traffic and to enforce a mitigation action.

TMS is configured on a per group basis. A single device is configured as the TMS controller. The controller is the central point in the network for TMS message distribution. The controller packages and distributes TIMs to TMS consumers. All other devices in the group are configured as consumers. A controller can support 250 TMS consumers in one or more TMS groups. Up to 64 TMS groups can be configured in a network.

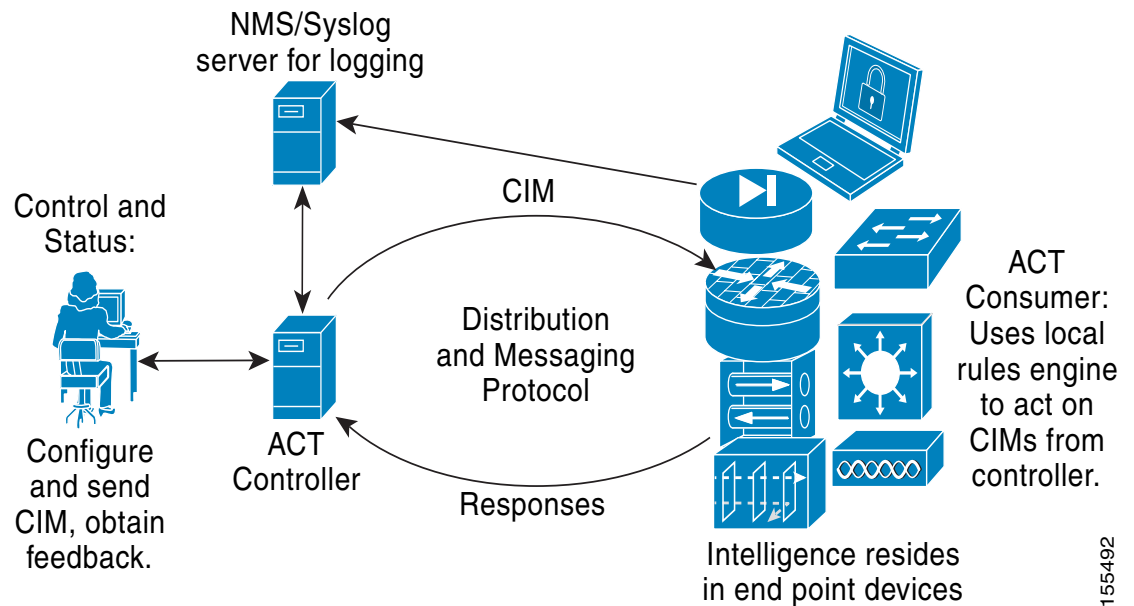
The consumer is any device that is configured to receive and process TIMs and send status to the controller. The mitigation enforcement action is applied based on rules in the TIM. Each consumer can be optionally configured with a individual rule set (TMS Rules Engine) customized to fit local requirements.

## Threat Information Messages

Each Threat Information Message (TIM) is identified by a threat ID, owner ID, and version number. The TIM is configured to identify suspect traffic. This traffic can be a single host IP address or entire major network range. The TIM is configured with a mitigation enforcement action that is associated with suspect traffic.

Each TIM is created in a threat definition file. The threat definition file is authored in a text or XML editor. The threat definition file must comply with Extensible Markup Language (XML) version 1.0 syntax. Each threat definition file can be up to 64 kb in size. A typical TIM is between 800 and a 1000 bytes. Each TMS group can support up to 256 active TIMs.

**Figure 3** *TIMs are Distributed from the TMS Controller*



The threat definition file is loaded to the TMS controller from a local storage device, such as ATA or linear flash memory. The file can also be loaded from a reachable host (using FTP, HTTPS, RCP, or TFTP protocols). This action places the TIMs contained within the threat definition file into the “loaded” database. The TIMs are then distributed (sent) from the controller to TMS consumers by the network administrator. Sending a TIM activates and places the TIM in the active database.

## TMS Protocol Configuration

TMS protocol operation, on the controller or consumer, is configured in a TMS type service policy using the Modular QoS CLI (MQC). The TMS type service policy is configured with TMS type class, parameter, and policy maps.

- The *TMS type class map* identifies TMS group consumers a traffic class.
- The *TMS type parameter map* is a container for TMS protocol-specific configuration parameters.
  - On the controller, TMS protocol operation timers, such as the heartbeat (keepalive) and message timers are configured.
  - On the consumer, the controller is identified and the controller registration timer is configured.
  - TMS event logging is enabled on both the controller and consumer.

- The *TMS type policy map* binds (or attaches) the class and parameter maps. The policy map is attached to the global consumer or controller process, which activates the TMS type service policy.

**Tip**

Default values for unconfigured parameter map commands are displayed in the router configuration file when a parameter map is created.

## Mitigation Enforcement Actions

The mitigation enforcement action is defined globally in the TIM. It is associated with suspect traffic and conditionally enforced depending on the configuration of the TIM or the configuration rule on the TMS consumer (Custom rules are configured on TMS consumers in a mitigation type parameter map).

In a TIM, the enforcement action is configured as a block or redirect. The redirect rule can be configured to route null0 (blackhole) or route to a specific host IP address for collection and analysis or to host IP address configured as a sinkhole. The TIM can be also configured to use a mitigation enforcement action defined in a mitigation type parameter map on a TMS consumer.

### Block Rule

The block mitigation enforcement action drops suspect traffic when suspect traffic meets all conditions of the rule. The behavior of this action is similar to a deny access list.

### Redirect Rule

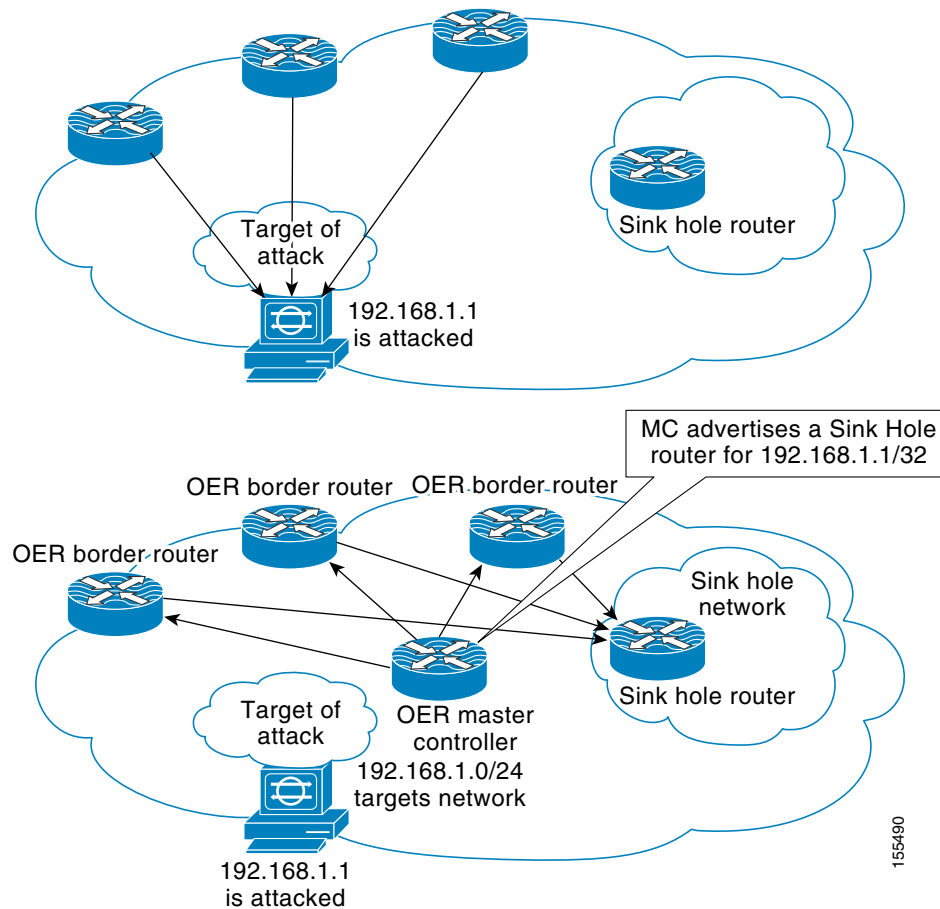
The redirect enforcement action is configured to route to null0 or to route to a specific host. Cisco IOS Optimized Edge Routing (OER) dynamically controls and implements redirect mitigation enforcement rules. Support for OER is automatically provided in Cisco IOS software images that support TMS. No explicit OER configuration is required. OER will function as if an OER master controller and border router processes has been configured on the TMS consumer.

Cisco IOS OER can also be explicitly configured on TMS consumers. However, the following caveats have been observed:

- Active threats on the TMS consumer must be resynchronized if you change the role that the consumer performs in the OER managed network. For example, if you reconfigure a border router to also perform OER master controller functions or vice versa.
- If multiple TIMs are configured with the same match criteria but different next-hop addresses. The next hop from the first threat will be selected.

Figure 4 shows a typical example where sinkhole routing is used.

**Figure 4** Typical OER Route to Sinkhole Example



The OER master controller process advertises the sinkhole router as the next hop for the 192.168.1.1 host, which is under attack.

## TMS Rules Engine Configuration

The TMS Rules Engine is a flexible mechanism that allows you to apply custom rules on individual consumers. A TIM can be configured to take the next-hop variable from a rules engine configuration, or a custom rule can be configured to override a mitigation enforcement action sent in a TIM from the TMS controller.

Using the TMS Rules Engine, you can configure a local rule to route traffic to a null0, route traffic to a specific interface for collection and analysis, configure a nonstandard primitive, or configure the local device to ignore an enforcement action sent by the controller.



### Note

Nonstandard primitives are predefined in the threat definition file that is loaded on the TMS controller.

The TMS Rules Engine is configured with a mitigation type service policy. The mitigation type service policy is created by configuring and linking mitigation type parameter and class maps to a mitigation type policy map.

- The *mitigation type class map* is used to define threat primitive and priority traffic matching conditions.
- The *mitigation type parameter map* contains the next-hop variable in the mitigation type service policy.
- The mitigation type policy map is used to attach the class and parameter maps.
- The *mitigation type policy map* is configured to bind mitigation type class and parameter maps together, creating a mitigation type service policy.

The mitigation type service policy is activated by attaching the mitigation type policy-map to the TMS type policy map in policy-map class configuration mode. The TMS type policy map is then attached to the global consumer configuration by configuring the **service-policy** command in TMS Consumer configuration mode.

## Local Device Exceptions

Local device exceptions are configured only on TMS consumers. A local device exception is an override configured for a specific host IP address or network. The TMS consumer negates a mitigation enforcement action sent from the controller or from a mitigation type service policy configured on the consumer.

For example, traffic from the 192.168.1.0/24 network is considered to be suspect. So, an ACL drop enforcement action is configured for all traffic sourced from this network. However, a device with a host address in this range (192.168.1.55) has to transit over a specific consumer. A local device exception is configured on the consumer to override ACL drop enforcement action.

## TMS System Logging

TMS system logging is enabled in the TMS type parameter map configuration. It is disabled by default.

### Controller System Logging Messages

This feature introduces the following system logging messages on the controller.

- TMS controller configuration status notification:  
12:58:02: %TMS-6-GROUP: CONTROLLER| Group=1| Host=10.3.3.1| Status=CONFIGURED
- Consumer registration notification:  
11:56:44: %TMS-6-DEVICE: CONTROLLER| Group=1| Host=10.3.3.2| Status=REGISTERED
- Consumer deregistration notification:  
12:52:55: %TMS-6-DEVICE: CONTROLLER| Group=1| Host=10.3.3.2| Status=DEREGISTERED
- Consumer threat send/reset/status notification:  
12:30:47: %TMS-6-RESET: CONTROLLER| Group=1| Device=10.3.3.2| Action=Delete| Start TID=1| End TID=1  
12:30:47: %TMS-6-THREATSTATUS: CONTROLLER| Group=1| Device=10.3.3.2| Threat=1| Status=Threat deleted

### Consumer System Logging Messages

This feature introduces the following system logging messages on the consumer.

- TMS consumer configuration status notification:

```
Feb 27 02:53:02.620: %TMS-6-GROUP: CONSUMER| Group=2| Host=10.3.3.2| Status=CONFIGURED
```

- Consumer registration notification:

```
*Feb 27 02:00:42.213: %TMS-6-DEVICE: CONSUMER| Group=1| Host=10.3.3.1| Status=REG
Requested
```

```
*Feb 27 02:00:42.241: %TMS-6-DEVICE: CONSUMER| Group=1| Host=10.3.3.1|
Status=REGISTERED
```

- Consumer response to send/reset/status message sent from the controller:

```
*Feb 27 02:34:40.417: %TMS-6-RESET: CONSUMER| Group=1| Device=10.3.3.1| Action=Delete|
Start TID=1| End TID=1
```

```
*Feb 27 02:34:40.425: %TMS-6-THREATSTATUS: CONSUMER| Group=1| Device=10.3.3.1|
Threat=1| Status=Threat deleted
```

- Consumer response to a resynchronization request sent from the controller:

```
*Feb 27 02:48:06.224: %TMS-6-THREAT: CONSUMER| Group=1| Device=10.3.3.1| TID=1
```

```
*Feb 27 02:48:06.232: %TMS-6-THREATSTATUS: CONSUMER| Group=1| Device=10.3.3.1|
Threat=1| Status=Redirect 192.168.2.1
```

TMS syslog messages are processed by Cisco IOS software based on global logging configuration. To modify system, terminal, destination, and other system global logging parameters, use the logging commands in global configuration mode. For more information about global system logging configuration, see the “Troubleshooting, Logging, and Fault Management” section of the *Cisco IOS Network Management Configuration Guide*, Release 12.4.

# How to Configure TMS

This section contains the following tasks:

## Configuring a TMS Type Service Policy

- [Configuring the TMS Type Parameter Map on a Controller, page 10](#) (required)
- [Configuring a TMS Type Parameter Map on a Consumer, page 13](#) (required)
- [Configuring the TMS Type Class Map on a Controller or Consumer, page 16](#) (required)
- [Configuring the TMS Type Policy Map on a Controller or Consumer, page 17](#) (required)

## Attaching the TMS Type Service Policy to a Global TMS Process

- [Attaching the Service Policy to a Global TMS Controller Process, page 19](#) (required)
- [Attaching the Service Policy to a Global TMS Consumer Process, page 21](#) (required)

## Registering and Deregistering a TMS Consumer

- [Registering and Deregistering a TMS Consumer, page 24](#) (optional)

## Managing Threat Information Messages on a TMS Controller

- [Configuring an XML Threat Definition File, page 26](#) (required)
- [Loading a Threat Definition File on a TMS Controller, page 31](#) (required)
- [Sending Threat Information Messages from the Controller to a TMS Consumer, page 33](#) (required)
- [Synchronizing the Threat Status of a Consumer with the TMS Group, page 35](#) (optional)
- [Managing Threat Information Messages on a Consumer from the Controller, page 36](#) (optional)
- [Sending a Status Request Message to Consumers from the TMS Controller, page 38](#) (optional)
- [Unloading a Threat Information Messages from the Loaded Database, page 40](#) (optional)

## Managing Threat Information Messages on a TMS Consumer

- [Configuring the TMS Rules Engine on a Consumer, page 41](#) (optional)
- [Configuring Local Device Exceptions on a Consumer, page 48](#) (optional)
- [Clearing Threat Information Messages on a Consumer, page 51](#) (optional)

## Verifying and Debugging TMS Configuration

- [Verifying TMS Configuration and Threat Status on a Controller or Consumer, page 52](#) (optional)
- [Enabling TMS Debug Messages on a Controller or Consumer, page 55](#) (optional)

## Configuring the TMS Type Parameter Map on a Controller

The steps in this task show how to configure a TMS type parameter map on a controller. The TMS type parameter map is a container for TMS protocol-specific configuration parameters. A TMS type parameter map is configured on the controller and on each consumer. On the controller, the heartbeat (keepalive) and threat message timers are configured. Entering the **parameter-map type tms** command places the router in parameter-map configuration mode.

## TMS Event Logging

The **logging tms events** command is entered in a TMS type parameter map on the consumer and/or controller. TMS system logging is disabled by default. TMS syslog messages are processed by Cisco IOS software based on global logging configuration. To modify system, terminal, destination, and other system global logging parameters, use the logging commands in global configuration mode. For more information about global system logging configuration, see the “Troubleshooting, Logging, and Fault Management” section of the *Cisco IOS Network Management Configuration Guide*, Release 12.4.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type tms {name}**
4. **heartbeat retry count {number}**
5. **heartbeat retry interval {time}**
6. **message retry count {number}**
7. **message retry interval {time}**
8. **logging tms events**
9. **exit**



## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>parameter-map type tms name</b>  <b>Example:</b> Router(config)# parameter-map type tms TMS_PAR_1	Configures a TMS type parameter map.  <b>Tip</b> Default values for unconfigured parameter map commands are displayed in the router configuration file when a parameter map is created.
Step 4	<b>heartbeat retry count {number}</b>  <b>Example:</b> Router(config-profile)# heartbeat retry count 5	Configures the number of times that heart beat messages are sent from a TMS controller to a consumer. <ul style="list-style-type: none"> <li>The heart beat message timer is configured on the TMS controller to regulate the frequency and interval of the transmission of heart beat (keepalive) messages.</li> <li>A number from 1 to 5 is entered for the <i>number</i> argument. The default number is 2.</li> <li>The controller is configured to send up to 5 heart beat messages to a nonresponsive peer in this example.</li> </ul>
Step 5	<b>heartbeat retry interval {time}</b>  <b>Example:</b> Router(config-profile)# heartbeat retry interval 60	Configures the time interval between the transmission of heart beat messages. <ul style="list-style-type: none"> <li>The <i>time</i> argument is configured in seconds. A number from 60 to 3000 is entered. The default time interval is 120 seconds.</li> <li>The controller is configured to send heart beat messages at 60 second intervals in this example.</li> </ul>
Step 6	<b>message retry count {number}</b>  <b>Example:</b> Router(config-profile)# message retry count 3	Configures the number of times that a threat message is sent from a TMS controller to a consumer. <ul style="list-style-type: none"> <li>The threat message timer is configured on the TMS controller to regulate the frequency and interval that the controller attempts to send threat messages to a nonresponsive peer.</li> <li>A number from 0 to 5 is entered for the <i>number</i> argument. The default number is 5.</li> <li>The controller is configured to send a threat message up to 3 times to a nonresponsive consumer in this example.</li> </ul>

	Command or Action	Purpose
Step 7	<b>message retry interval</b> {time}  <b>Example:</b> Router(config-profile)# message retry interval 15	Configures the time interval between the transmission of threat messages. <ul style="list-style-type: none"> <li>The <i>time</i> argument is configured in seconds. A number from 3 to 300 is entered. The default time interval 10 seconds.</li> <li>The controller is configured to send threat messages at 15 second intervals to a nonresponsive consumer in this example.</li> </ul>
Step 8	<b>logging tms events</b>  <b>Example:</b> Router(config-profile)# logging tms events	Enables TMS event logging on the controller. <ul style="list-style-type: none"> <li>TMS specific events are logged to syslog in this example.</li> </ul>
Step 9	<b>exit</b>  <b>Example:</b> Router(config-profile)# exit	Exits parameter-map configuration mode, and enters global configuration mode.

## Examples

The following example, starting in global configuration mode, configures a TMS type parameter map on a controller:

```
Router(config)# parameter-map type tms TMS_PAR_1
Router(config-profile)# logging tms events
Router(config-profile)# heartbeat retry interval 60
Router(config-profile)# heartbeat retry count 3
Router(config-profile)# message retry interval 15
Router(config-profile)# message retry count 5
Router(config-profile)# exit
```

## What to Do Next

A TMS type parameter map must also be configured on each consumer. Proceed to the next section to see more information.

## Configuring a TMS Type Parameter Map on a Consumer

The steps in this task show how to configure a TMS type parameter map on a consumer. A TMS type parameter map is configured on the controller and on each consumer. On the consumer, it is configured to identify the controller to and to set registration timers. Entering the **parameter-map type tms** command places the router in parameter-map configuration mode.

## TMS Event Logging

The **logging tms events** command is entered in a TMS type parameter map on the consumer and/or controller. TMS system logging is disabled by default. TMS syslog messages are processed by Cisco IOS software based on global logging configuration. To modify system, terminal, destination, and other

system global logging parameters, use the logging commands in global configuration mode. For more information about global system logging configuration, refer to the “Troubleshooting and Fault Management” section of the *Cisco IOS Network Management Configuration Guide*, Release 12.4.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type tms {name}**
4. **controller ipv4 {ip-address}**
5. **registration retry count {number}**
6. **registration retry interval {time}**
7. **logging tms events**
8. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>parameter-map type tms name</b>  <b>Example:</b> Router(config)# parameter-map type tms TMS_PAR_2	Configures a TMS type parameter map. <p><b>Tip</b> Default values for unconfigured parameter map commands are displayed in the router configuration file when a parameter map is created.</p>
Step 4	<b>controller ipv4 {ip-address}</b>  <b>Example:</b> Router(config-profile)# controller ipv4 10.1.1.1	Specifies the TMS controller in the parameter map of a TMS consumer. <ul style="list-style-type: none"> <li>The 10.1.1.1 host IP address is configured as the TMS controller in this example.</li> </ul> <p><b>Tip</b> The IP address that is configured in this step is the IP address that was configured as the source interface in the TIDP configuration on the TMS controller.</p>
Step 5	<b>registration retry count {number}</b>  <b>Example:</b> Router(config-profile)# registration retry count 5	Configures the number of times that an implicit TMS registration message is sent from a TMS controller to a controller. <ul style="list-style-type: none"> <li>The TMS consumer must register before the controller will send threat messages. Implicit registration messages are sent when a TMS type service policy is activated on the consumer or when the consumer is deregistered (by the administrator) from the controller.</li> <li>A number from 1 to 5 is entered for the <i>number</i> argument. The default number is 3.</li> <li>The consumer is configured to send a registration message to a controller up to 5 times or until successfully registered in this example.</li> </ul>
Step 6	<b>registration retry interval {time}</b>  <b>Example:</b> Router(config-profile)# registration retry interval 60	Configures the time interval between the transmission of registration messages. <ul style="list-style-type: none"> <li>The <i>time</i> argument is configured in seconds. A number from 30 to 3000 is entered. The default time interval is 180 seconds.</li> <li>The consumer is configured to registration messages at 60 second intervals in this example.</li> </ul>

	Command or Action	Purpose
Step 7	<b>logging tms events</b>  <b>Example:</b> Router(config-profile)# logging tms events	Enables logging for TMS events on a TMS controller or consumer.  <ul style="list-style-type: none"> <li>TMS specific events are logged to syslog in this example.</li> </ul>
Step 8	<b>exit</b>  <b>Example:</b> Router(config-profile)# exit	Exits parameter-map configuration mode, and enters global configuration mode.

## Examples

The following example, starting in global configuration mode, configures a TMS type parameter map on a consumer:

```
Router(config)# parameter-map type tms TMS_PAR_2
Router(config-profile)# controller ipv4 10.1.1.1
Router(config-profile)# logging tms events
Router(config-profile)# registration retry count 5
Router(config-profile)# registration retry interval 60
Router(config-profile)# exit
```

## What to Do Next

The next step is to identify the TIDP group, over which TMS services are to be configured. Proceed to the next section to see more information.

## Configuring the TMS Type Class Map on a Controller or Consumer

The steps in this task show how to configure a TMS type class map to define a TMS group as a class of traffic. A single TMS group or range of groups are configured with the **match tidp-group** command. This task is performed on the controller and on each consumer.

## Prerequisites

TIDP is operational on the controller and all consumers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type tms {[match-any] name}**
4. **match tidp-group number [- number]**
5. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>class-map type tms {[match-any] name}</b>  <b>Example:</b> Router(config)# class-map type tms TMS_CLASS_1	Configures a TMS type class map to define a TMS group as a class of traffic.
Step 4	<b>match tidp-group number [- number]</b>  <b>Example:</b> Router(config-cmap)# match tidp group 10	Defines a TMS group or a range of groups as match criteria in a class map. <ul style="list-style-type: none"> <li>TMS group 10 is defined in this example.</li> </ul>
Step 5	<b>exit</b>  <b>Example:</b> Router(config-cmap)# exit	Exits class-map configuration mode, and enters global configuration mode.

## Examples

The following example, starting in global configuration mode, configures groups 10 through 20 and group 30 as match criteria in the TMS\_CLASS\_1 class map:

```
Router(config)# class-map type tms TMS_CLASS_1
Router(config-cmap)# match tidp group 10 - 20
Router(config-cmap)# match tidp group 30
Router(config-cmap)# exit
```

## What to Do Next

The next step is to attach the TMS type class and parameter maps to a TMS type policy map. Proceed to the next section to see more information.

## Configuring the TMS Type Policy Map on a Controller or Consumer

The steps in this task show how to configure a TMS type policy map. The TMS policy map is configured to bind (attach) TMS type class and parameter maps. Any number of class maps, with different parameter maps, can be attached to the policy map. This task is performed on the controller and on each consumer.

## Prerequisites

A TMS type class and parameter map is configured.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control tms {name}**
4. **class {class-name | class-default}**
5. **mitigation {parameter-map}**
6. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>policy-map type control tms {name}</b>  <b>Example:</b> Router(config)# policy-map type control tms TMS_POL_1	Configures a TMS type policy map.
Step 4	<b>class {class-name   class-default}</b>  <b>Example:</b> Router(config-pmap)# class TMS_CLASS_1	Defines the TMS traffic class (TMS group) to attach to the policy map. <ul style="list-style-type: none"><li>• The <i>class-name</i> argument must be configured in this step.</li></ul>
Step 5	<b>mitigation {parameter-map}</b>  <b>Example:</b> Router(config-pmap-c)# mitigation TMS_PAR_1	Attaches the TMS parameter map to the class map under the policy map.
Step 6	<b>end</b>  <b>Example:</b> Router(config-pmap-c)# end	Exits policy-map class configuration mode, and enters privileged EXEC mode.

## Examples

The following example, starting in global configuration mode, attaches TMS type class and parameter maps to a TMS type policy map:

```
Router(config)# parameter-map type tms TMS_PAR_1
Router(config-profile)# logging tms events
Router(config-profile)# exit
Router(config)# class-map type tms TMS_CLASS_1
Router(config-cmap)# match tidp-group 10
Router(config-cmap)# exit
Router(config)# policy-map type control tms TMS_POL_1
Router(config-pmap)# class TMS_CLASS_1
Router(config-pmap-c)# mitigation TMS_PAR_1
Router(config-pmap-c)# end
```

## What to Do Next

The next step is to attach the policy map to the global TMS controller or consumer process. Proceed to the next section to see more information.

## Attaching the Service Policy to a Global TMS Controller Process

The TMS type service policy that was configured in the first three configuration tasks is attached to a global TMS controller process in this task.

## Configuring the TMS Controller Identifier

The **identifier** command is configured to assign a unique ID number to a TMS controller. In Cisco IOS Release 12.4(6)T, only a single controller can be configured in each group. Identifier configuration is required only when multiple controllers are configured in a single TMS group.

## Prerequisites

- A TMS type service policy has been configured.
- TIDP is operational on the controller and all consumers.

## Restrictions

- Only a single TMS type policy map can be attached to the global TMS controller or consumer process. However, you can configure multiple TMS type class maps and associate these maps under the same TMS type policy map. Each class map can be configured with the same parameter map or a different parameter map.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **tms controller**
4. **service-policy type tms {policy-map}**
5. **identifier {number}**
6. **end**



## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>tms controller</b>  <b>Example:</b> Router(config)# tms controller	Configures a networking device as a TMS controller.
Step 4	<b>service-policy type tms {policy-map}</b>  <b>Example:</b> Router(cfg-tms-ctrl)# service-policy type tms TMS_POL_1	Attaches a TMS type service policy to a TMS consumer process.
Step 5	<b>identifier {number}</b>  <b>Example:</b> Router(cfg-tms-ctrl)# identifier 1000	(Optional) Configures a unique identifier for a TMS controller. <ul style="list-style-type: none"><li>A number from 1 to 4294967295 can be entered for the <i>number</i> argument.</li></ul> <b>Note</b> This configuration step is not required in Cisco IOS Release 12.4(6)T.
Step 6	<b>end</b>  <b>Example:</b> Router(cfg-tms-cons)# end	Exits TMS consumer configuration mode, and enters privileged EXEC mode.

## Examples

The following example, starting in global configuration mode, configures a global TMS controller process, attaches a TMS type policy map:

```
Router(config)# tms controller
Router(cfg-tms-ctrl)# service-policy type tms TMS_POL_1
Router(cfg-tms-ctrl)# end
```

## Troubleshooting Tips

If the controller is unable to send threat messages to the consumer, perform the following steps:

1. Verify the registration status of the consumers by entering the **show tms controller** command. A registered consumer will be listed as “Registered Successfully” in the “Status” column. If the Status column displays “Configured Available”, then the controller is activated and waiting for a consumer to send a registration message.

2. If a consumer does not register successfully, use the **ping** command to send extended pings to the consumer to verify reachability.
3. If the consumer is reachable from the controller, enter the **tms consumer register** command on the consumer.
4. If the controller and consumers are properly configured and reachable via TCP/IP but the consumer is still unable to register with the controller, enable the **debug tms controller error** command to display related error messages.

## What to Do Next

A TMS type policy map must also be attached to a global TMS consumer process. Proceed to the next section to see more information.

## Attaching the Service Policy to a Global TMS Consumer Process

The TMS type service policy that was configured in the first three configuration tasks is attached to a global TMS consumer process in this task. Attaching the service policy activates a TMS consumer.

## Consumer Registration

The TMS consumer must register with the TMS controller before the controller can send Threat Information Messages (TIMs). Implicit registration requests are automatically sent to the controller when a TMS type service policy is activated on the consumer.

By default, a TMS consumer sends a registration request message to the TMS controller once every 3 minutes for up to 3 times or until successfully registered. If the consumer is a member of multiple groups, it will send a separate registration request messages to the controller of each group.



**Tip**

Explicit registration is configured by entering the **tms consumer registration** command on a TMS consumer in privileged EXEC mode. This command is unaffected by registration timer configuration and can be used to register the consumer with the controller at any time.

## Configuring Device Exceptions

The **exception access-group** command is configured to attach a local device exception to a TMS consumer process. A local device exception is an override configured on the TMS consumer that negates a enforcement action sent from the TMS controller or from a TMS Rules Engine configuration (mitigation type service policy) configured on the TMS consumer.

For example, traffic from the 192.168.1.0/24 network is considered to be suspect. So, an ACL drop mitigation enforcement action is configured for all traffic sourced from this network. However, a device with a host address in this range (192.168.1.55) needs to transit over a specific consumer. A local device exception is configured on the consumer to override ACL drop enforcement action.

The device exception is configured locally. A host IP address (or any other subset of the network) is defined in an extended access list and then referenced by the **exception access-group** command. The **tms-class** command is configured to associate an interface with the device exception. The enforcement action configured on the controller is not applied to traffic that is permitted by the access list.

## Prerequisites

- A TMS type service policy has been configured.
- TIDP is operational on the controller and all consumers.

## Restrictions

- Only a single TMS type policy map can be attached to the global TMS controller or consumer process. However, you can configure multiple TMS type class maps and associate these maps under the same TMS type policy map. Each class map can be configured with the same parameter map or a different parameter map.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **tms consumer**
4. **service-policy type tms** {*policy-map*}
5. **exception access-group** {*extended-acl*}
6. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>tms consumer</b>  <b>Example:</b> Router(config)# tms consumer	Enters TMS consumer configuration mode to configure a consumer.
Step 4	<b>service-policy type tms {policy-map}</b>  <b>Example:</b> Router(cfg-tms-cons)# service-policy type tms TMS_POL_1	Binds a TMS type service policy to a TMS consumer process.
Step 5	<b>exception access-group {named-acl}</b>  <b>Example:</b> Router(cfg-tms-cons)# exception access-group NAMED_ACL	Configures a device exception in a global TMS consumer configuration.
Step 6	<b>end</b>  <b>Example:</b> Router(cfg-tms-cons)# end	Exits TMS consumer configuration mode, and enters privileged EXEC mode.

## Examples

The following example, starting in global configuration mode, configures a global TMS consumer process, attaches a TMS type policy map, and configures a device exception:

```
Router(config)# ip access-list extended NAMED_ACL
Router(config-ext-nacl)# permit tcp host 192.168.1.55 any
Router(config-ext-nacl)# exit
Router(config)# interface Ethernet 0/0
Router(config-if)# ip access-group NAMED_ACL in
Router(config-if)# tms-class
Router(config-if)# exit
Router(config)# tms consumer
Router(cfg-tms-cons)# exception access-group NAMED_ACL
Router(cfg-tms-cons)# service-policy type tms TMS_POL_1
Router(cfg-tms-cons)# end
```

## Troubleshooting Tips

If the consumer does not receive threat messages from the controller, perform the following steps:

1. Verify the registration status of the consumer by entering the **show tms consumer** command. A registered consumer will be listed as “Registered Successfully” in the “Status” column. If logging is enabled, the syslog output will show registered consumers as REGISTERED.
2. If a consumer does not register successfully, use the **ping** command to send extended pings to the controller (defined in the TMS type parameter map) to verify reachability.
3. If the controller is reachable from the consumer, use the **tms consumer register** command to explicitly register the consumer with the controller.
4. If the controller and consumers are properly configured and reachable via TCP/IP but the consumer is still unable to register with the controller, enable the **debug tms consumer error** command to display related error messages.

## What to Do Next

A consumer must be registered with the controller to receive TIMs. Implicit registration occurs automatically when this task is completed. A consumer can be explicitly registered or deregistered at any time. Proceed to the next section to see more information.

## Registering and Deregistering a TMS Consumer

This task is optional. The steps in this task shows how to register or deregister a consumer with a controller. All commands described in this section are entered in privileged EXEC mode.

### Implicit Synchronization

Implicit synchronization (resync) messages are sent between the controller and consumer when the **tms consumer register** command is entered. Implicit synchronization ensures that the consumer has received all threats that have been configured its TMS group. Threats remain active until they are removed by the controller or until the consumer is deregistered.

### Prerequisites

- TIDP and TMS is operational on the controller and all consumers.

### SUMMARY STEPS

1. **enable**
2. **tms consumer register {group group-id controller ipv4 ip-address}**
3. **tms consumer deregister {group group-id controller ipv4 ip-address}**
4. **tms controller deregister {group group-id consumer ipv4 ip-address}**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>tms consumer register {group group-id controller ipv4 ip-address}</b>  <b>Example:</b> Router# tms consumer register group 10 controller ipv4 10.1.1.1	(Required) Registers the consumer with a controller. This command is entered on a consumer. <ul style="list-style-type: none"> <li>The <i>group-id</i> is entered as a number from 1 to 4294967295.</li> </ul>
Step 3	<b>tms consumer deregister {group group-id controller ipv4 ip-address}</b>  <b>Example:</b> Router# tms consumer deregister group 10 controller ipv4 10.1.1.1	(Optional) Deregisters the consumer from a controller. This command is entered on a consumer. <ul style="list-style-type: none"> <li>Threats sent to a deregistered consumer are deleted.</li> </ul>
Step 4	<b>tms controller deregister {group group-id consumer ipv4 ip-address}</b>  <b>Example:</b> Router# tms controller deregister group 10 consumer ipv4 10.1.1.2	Deregisters the consumer from a controller. This command is entered on a controller. <ul style="list-style-type: none"> <li>Threats sent to a deregistered consumer are deleted.</li> </ul>

## Examples

The following example registers a TMS consumer with a TMS controller:

```
Router# tms consumer register group 10 controller ipv4 10.1.1.1
```

The following example deregisters the 10.1.1.2 consumer from the controller:

```
Router# tms controller deregister group 10 consumer ipv4 10.1.1.2
```

## Troubleshooting Tips

If the consumer is unable to register with the controller, perform the following steps:

1. Verify registration status by entering the **show tms controller** command on the controller or the **show tms consumer** command on the consumer.
2. Use the **ping** command to send extended pings to the controller to verify reachability.
3. If the controller and consumers are properly configured and reachable via TCP/IP but the consumer is still unable to register with the controller, enable the **debug tms consumer error** command to display related error messages.

## What to Do Next

At completion of this task, the framework and services for distributing threat messages is complete and operational. Proceed to the next section to see information on configuring a threat definition file.

## Configuring an XML Threat Definition File

The steps in this task show how to configure an XML threat definition file. The threat definition file is a container for Threat Information Messages (TIMs). The threat definition file first is configured in a text or XML editor. The threat definition file loaded to the TMS controller. TIMs are then distributed to TMS consumers.

### XML Version 1.0 Syntax

The syntax of the threat definition file must comply with Extensible Markup Language (XML) version 1.0 syntax. For information about version 1.0 XML syntax, refer to the following document:

- <http://www.w3.org/TR/REC-xml/>

### Threat Definition File Syntax Guidelines

The following list describes required and optional syntax for the threat definition file:

- The threat file must contain descriptions for one or more threats
- Threat details are encoded in XML notation
- The threat file itself should begin with the following version encoding:  
`<?xml version="1.0" encoding="utf-8"?>`
- XML tags are represented by **bold** text
- Attribute syntax is represented by *italic* text
- Each threat is uniquely identified by the owner ID, threat ID, and version number
- Each threat should start with a threat tag, which contains the owner/threat ID/version values
- The following XML tags are mandatory for every threat:  
**threat**, **threat\_info**, **primitive** and **tcdf**
- The following XML tags are optional for every threat:  
**condition** and **parameter**

### Threat File Tag Descriptions

This section describes required and optional XML tags.

#### **threat (required)**

The **threat** tag must follow the XML version tag. This tag has the following three required attributes:

**threat\_info (required)**

The **threat\_info** tag contains the Event Risk Rating (ERR) attribute. The ASR field in this tag is used to set the priority of the threat. The priority is configured with a number from 1 to 5. The priority implies no preference or hierarchy. It simply provides 5 levels of independent classification for threat messages.

**Tip**

The ASR field maps directly to the **match priority** command. It is configured on the consumer to match the ASR field to a traffic class in a mitigation type service policy (TMS Rule Engine configuration).

**Note**

In Cisco IOS Release 12.4(6)T, the threat priority cannot be configured in the TMS Rules Engine (mitigation type service policy). However, priority values can be with the **match priority** command.

**primitive (required)**

The **primitive** tag contains the *primitive* attribute. The *primitive* attribute defines the mitigation enforcement action: *block*, *redirect*, or a nonstandard (user-defined) primitive. The nonstandard primitive is configured with any string value. *Block* and *redirect* are standard primitives. Any other value is interpreted as a nonstandard.

**Tip**

The *primitive* attribute maps directly to the **match primitive** command. It is configured on a consumer to match the mitigation enforcement action to a traffic class in a mitigation type service policy.

**parameter (optional)**

The **parameter** tag is a container for the next-hop variable of the mitigation enforcement action. The next-hop variable is defined in a nested **redirect** tag. The next hop is configured to route to a specific IPv4 host address or to the null0 interface (black hole).

The *profile* attribute is defined to configure the threat to take the next hop from a mitigation type parameter map configured on the consumer.

**Tip**

The *profile* attribute maps directly to the name of the mitigation type parameter map configured on the TMS consumer. The **variable** command is configured in the parameter-map to define the next hop. The **parameter** tag can be configured with either the *profile* attribute or a nested **redirect** tag but not both.

**condition (optional)**

The **condition** tag is used to define a conditional enforcement rule on an interface for a mitigation action. The mitigation action is enforced on the interface when any condition (first match) or all conditions (strict match) are met.

- The **condition** tag should have at least one **match** tag.
- A **match** tag must be configured with the attribute of type “all” or “any.”
- A **match** tag can contain nested **match** tags, or it can contain the **device\_class**, **sub\_device\_class**, or **host\_locate** optional tags.

The **device\_class** tag is configured with an attribute name that identifies the router or networking device.

**Note**

In Cisco IOS Release 12.4(6)T, “Router” is the only supported attribute name for the **device\_class** tag.



The **sub\_device\_class** tag is configured with an attribute name that identifies an interface. This tag is used to associate one or more threats with one or more interfaces.

**Tip**

The **sub\_device\_class** tag maps directly to the *name* argument of the **tms-class** command. The **tms-class** command is configured in interface configuration mode to associate an interface with an ACL drop enforcement action.

The **host\_locate** tag is configured with the *ipv4\_address* attribute. This attribute is entered with a valid IP version 4 (IPv4) address to identify a specific host. This tag is used to associate a specific host with a threat.

**Tip**

The **host\_locate** tag maps directly to the **edge** keyword of the **tms-class** command. This configuration is used to associate a host with a threat. The mitigation action is enforced only if the host is reachable from the interface when the **edge** keyword is configured.

**tcdf (required)**

The **tcdf** tag defines the traffic class for which the mitigation action that is enforced. This includes the classification match rule (strict or first) and the network (IP) and the transport (TCP or UDP) layer protocols that carry the traffic.

- Only one classification is allowed for each tag.
- Information attributes of the class, such as the name, are ignored.
- Attribute *match= "all"* or *match= "any"* are supported by TCDF.
- Only one match tag can be entered. The attribute for match, is *type*, which can take values *"all"* or *"any"*.

**Note**

In Cisco IOS Release 12.4(6)T, only strict traffic class matching (*match= "all"*) is supported.

- *Eq* and *range* filters are supported.
- The attribute field can accept the following string values:  
*ip.src\_addr*  
*ip.dst\_addr*  
*ip.proocol*  
*tcp.src\_port*  
*tcp.dst\_port*  
*udp.src\_port*  
*udp.dst\_port*
- The *range* filter can be configured for only TCP and UDP port numbers.
- The *ip.protocol* attribute can be configured with only TCP and UDP values (6 and 17). When TCP is configured, *tcp.src\_port* and *tcp.dst\_port* range can be defined. When UDP is configured as the protocol, *udp.src\_port* and *udp.dst\_port* range can be defined.

**Tip**

If the *ip.protocol* attribute is not specified, the traffic class is processed without regard to the transport layer protocol. Only the source and destination IP addresses are entered for this type of traffic class definition. Port numbers are not.

## XML Threat Definition File Configuration Steps

Steps 5, 6, and 7 contain branching tasks. Each branching task shows an alternate configuration that can be applied for the given step.

- 
- Step 1** (Required) The threat file is configured with the version and encoding declaration.
- ```
<?xml version="1.0" encoding="utf-8"?>
```
- Step 2** (Required) The threat ID, owner ID, and version numbers are configured. The version must be incremented each time the threat is updated (replaced with a newer version).
- ```
<threat tid="1" owner="1000" version="10">
</threat>
```
- Step 3** (Required) Threat information is configured. In this sample step, the ASR field is set to 3 (threat priority level).
- ```
<threat_info threat_name="NAME"
             threat_text="THREATTEXT"
             mitigation_text="mitigaationtext" >
    <err ASR="3" SFR="20" ARR="30" TFR="40" PD="50"></err>
    <threat_class name="tc1"> </threat_class>
    <threat_class name="tc2"> </threat_class>
</threat_info>
```
- Step 4** (Required) The threat primitive is configured as a *block*, *redirect*, or nonstandard (user-defined) mitigation action.
- ```
<primitive name="redirect"> </primitive>
```
- Step 5** (Optional) The next-hop variable is set to a host IP address (172.16.1.1).
- ```
<parameter>
    <redirect nexthop="172.16.1.1"> </redirect>
</parameter>
```
- Or**
- (Optional) The next-hop variable is set to the null0 interface (0.0.0.0).
- ```
<parameter>
 <redirect nexthop="0.0.0.0"> </redirect>
</parameter>
```
- Or**
- (Optional) The next-hop variable is determined by the configuration of the mitigation type parameter map configured on the TMS consumer (MIT\_PAR\_2).
- ```
<parameter profile="MIT_PAR_2"> </parameter>
```

- Step 6** (Optional) A first match conditional enforcement rule is configured. In this sample step, the mitigation action is enforced when suspect traffic travels over an interface tagged with the sub_device_class name (Ingress_Ethernet) or when suspect traffic travels over an interface that is reachable from the 10.2.2.2 host.

```
<condition>
  <match type="any">
    <match type="any">
      <host_locate ipv4_addr="10.2.2.2" > </host_locate>
      <device_class name="Router" > </device_class>
    </match>
    <match type="any">
      <device_class name="Router" > </device_class>
      <sub_dev_class name="Ingress_Ethernet" > </sub_dev_class>
    </match>
  </match>
</condition>
```

Or

- (Optional) A strict match conditional enforcement rule is configured. In this sample step, the mitigation action is enforced only when suspect traffic travels over an interface that is reachable from the 10.2.2.2 host and is tagged with the sub_device_class name (Ingress_Ethernet).

```
<condition>
  <match type="all">
    <host_locate ipv4_addr="10.2.2.2" > </host_locate>
    <device_class name="Router" > </device_class>
    <sub_dev_class name="Ingress_Ethernet" > </sub_dev_class>
  </match>
</condition>
```

- Step 7** (Required) The traffic class is defined to specify suspect traffic. In this sample step, TCP is identified as the transport layer protocol. Specific source and destination IP addresses and port numbers are configured.

```
<tcdcf>
  <class name="match-criteria" type="access-control" match="all">
    <match>
      <eq field="ip.src_addr" value="192.168.7.66" mask="255.255.255.255"> </eq>
      <eq field="ip.dst_addr" value="10.3.3.3" mask="255.255.255.255"> </eq>
      <eq field="ip.protocol" value="6"> </eq>
      <range field="tcp.src_port" from="10" to="200"> </range>
      <range field="tcp.dst_port" from="50"> </range>
    </match>
  </class>
</tcdcf>
```

Or

- (Required) In this sample step, UDP is identified as the transport layer protocol.

```
<tcdcf>
  <class name="match-criteria" type="access-control" match="all">
    <match>
      <eq field="ip.src_addr" value="192.168.7.66" mask="255.255.255.255"> </eq>
      <eq field="ip.dst_addr" value="10.3.3.3" mask="255.255.255.255"> </eq>
      <eq field="ip.protocol" value="17"> </eq>
      <range field="udp.src_port" from="1000" to="2000"> </range>
      <range field="udp.dst_port" from="5000"> </range>
    </match>
  </class>
</tcdcf>
```

Or

(Required) In this sample step, no transport layer protocol is defined. Only source and destination IP addresses are configured to identify suspect traffic.

```
<tcdf>
  <class name="match-criteria" type="access-control" match="all">
    <match>
      <eq field="ip.src_addr" value="192.168.7.66" mask="255.255.255.255"> </eq>
      <eq field="ip.dst_addr" value="10.3.3.3" mask="255.255.255.255"> </eq>
    </match>
  </class>
</tcdf>
```



Tip

Source and destination port number are not configured when a transport layer protocol is not specified.

What to Do Next

The threat definition file must be loaded to the controller before threats contained in the threat definition file can be sent to consumers. Proceed to the next section to see information on loading and unloading threats.

Loading a Threat Definition File on a TMS Controller

This task shows how to load a threat definition file on a TMS controller. The **tms controller load threat** command is entered in privileged EXEC mode to load an XML threat definition file to the TMS controller from a local storage device, such as ATA or linear flash memory. The file can also be loaded from a reachable host (using FTP, HTTPS, RCP, or TFTP protocols).

Loaded and Active Databases

Two databases are maintained on the controller: the “loaded” database and the “active” database. The **tms controller load threat** command is used to upload a threat definition file on the controller. Once the threat definition file has been loaded, individual threats contained within the threat definition file are placed in the “loaded” database for distribution to consumers. Threats are removed from the loaded database by entering the **tms controller unload** command. Entering this command does not remove the threat from the active database if the threat is active on at least one consumer.

A threat is placed in the “active” database when the **tms controller send** command is used to send one or more threats to one or more consumers. A threat remains in the active database as long as it is active on at least one consumer. An active threat can be removed from consumers by entering the **tms controller reset** command on the controller. Active threats can be removed on the consumer by entering **clear tms consumer** or by reloading the consumer.

Updating or Replacing a Loaded Threat

Each threat that is contained within a threat definition file is uniquely identified by the threat ID, owner ID, and version number. The controller uses the version field to ensure that the most recent threat is sent to consumers. A higher version number indicates a more current or newer threat.

To replace or update an existing threat in the loaded database, a modified threat definition file must be loaded to the controller. The threat contained within this file must have a higher number in the version field. If the version field is the same or contains a lower number, the updated threat will not be loaded.

To distribute the updated threat to TMS consumers, the older version of the threat must be removed from the active database. The **tms controller reset** command can be entered with the **delete** keyword to remove the threat from all consumers.

Prerequisites

- TIDP and TMS is operational on the controller and all consumers.
- A threat definition file that contains one or more TIMs has been created.
- The threat definition file has been copied to flash memory on the controller or is accessible on a reachable host.

Restrictions

- There is no limit on the number of threats that can be loaded on to the controller. However, the amount of memory required is dependent on the number consumers, the number of threats, and the number of other processes that run on the router or network device.

SUMMARY STEPS

1. **enable**
2. **tms controller load threat** *{file-source}*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	tms controller load threat <i>{file-source}</i> Example: Router#_tms controller load threat disk0: THREAT_DEFINITION_FILE	(Required) Loads a threat definition file on to a TMS controller. <ul style="list-style-type: none"> • The threat definition file can be loaded from a local file system, such as flash memory, or it can be loaded from a reachable host over the network.

Examples

The following example loads a threat definition file from local flash memory:

```
Router# tms controller load threat disk0: THREAT_FILE
```

The following example loads a threat definition file from a TFTP server:

```
Router# tms controller load threat tftp://172.16.1.1/THREAT_DEFINITION_FILE
```

Troubleshooting Tips

If there is a problem loading or unloading an XML threat definition file, the **debug tms controller xml error** command can be enabled to configure the router to print related error messages.

What to Do Next

The threat message is not activated until it is sent to TMS consumers. Proceed to the next section to see more information.

Sending Threat Information Messages from the Controller to a TMS Consumer

This task shows how to send a TIM to TMS consumers. A single threat, a range of threats, or all threats can be sent. The threat can be sent to a single group or all groups. The start time when the threat is activated and the duration of the threat are configurable. The **tms controller send** command is entered in privileged EXEC mode.

Prerequisites

- TIDP and TMS is operational on the controller and all consumers.
- A threat definition file that contains one or more TIMs has been put in the loaded database on the controller.

SUMMARY STEPS

1. **enable**
2. **tms controller send {group {group-id | all} owner owner-id tid {threat-id [- number] | all} consumer {all | ipv4 ip-address} [start_time seconds] [duration seconds]}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	tms controller send {group {group-id all} owner owner-id tid {threat-id [- number] all} consumer {all ipv4 ip-address} [start_time seconds] [duration seconds]} Example: Router# tms controller send group 10 owner 1000 tid 100 consumer all duration 3600	Configures a TMS controller to send a threat definition file to TMS consumers.

Examples

The following example sends threat ID 100 to all consumers in TIDP group 10. The threat will remain active for 1 hour.

```
Router# tms controller send group 10 owner 1000 tid 100 consumer all duration 3600
```

Troubleshooting Tips

If the controller is unable to send threat messages to the consumer, perform the following steps:

1. Verify the registration status of the consumers by entering the **show tms controller** command. A registered consumer will be listed as “Registered Successfully” in the “Status” column. If the Status column displays “Configured Available”, then the controller is activated and waiting for a consumer to send a registration message.
2. If a consumer does not register successfully, use the **ping** command to send extended pings to the consumer to verify reachability.
3. If the consumer is reachable from the controller, enter the **tms consumer register** command on the consumer.
4. If the controller and consumers are properly configured and reachable via TCP/IP but the consumer is still unable to register with the controller, enable the **debug tms controller error** command to display related error messages.

What to Do Next

Proceed to the next section to see information about synchronizing the threat status on a consumer with other consumers in a TMS group.

Synchronizing the Threat Status of a Consumer with the TMS Group

This task is optional. This task shows how to synchronize the threat status on a consumer with the threat status on other consumers. This command is entered to ensure that the consumer has received all messages that have been sent to the TMS group. The **tms consumer resync** command is entered in privileged EXEC mode.

Implicit Synchronization

Implicit synchronization (resync) messages are sent between the controller and consumer when the **tms consumer register** command is entered. Implicit synchronization ensures that the consumer has received all threats that have been configured its TMS group. Threats remain active until they are removed by the controller or until the consumer is deregistered.

Prerequisites

- TIDP and TMS is operational on the controller and all consumers.
- A threat definition file that contains one or more TIMs has been put in the loaded database on the controller.

SUMMARY STEPS

1. **enable**
2. **tms consumer resync {group group-id owner {owner-id | any} tid {threat-id [- number] | all} controller ipv4 ip-address}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	tms consumer resync {group group-id owner {owner-id any} tid {threat-id [- number] all} controller ipv4 ip-address} Example: Router# tms consumer resync group 10 owner any tid all controller ipv4 10.1.1.1	(Optional) Synchronizes a TMS consumer with a TMS controller. <ul style="list-style-type: none">• The example synchronizes all threats from any owner that were sent to TIDP group 10.

Examples

The following example synchronizes all threats from any owner that were sent to TIDP group 10.

```
Router# tms consumer resync group 10 owner any tid all controller ipv4 10.1.1.1
```


Troubleshooting Tips

If you are unable to synchronize the consumer with the TMS group, perform the following steps:

1. Verify the threat status on the controller and consumers by entering the **show tms controller** and **show tms consumer** commands. Filter the output to display information about the group and threat ID numbers.
2. If the consumer is reachable from the controller, enter the **tms consumer register** command on the consumer.
3. If the controller and consumers are properly configured and reachable but the consumer is still unable to synchronize, enable the following debug commands to display related error messages:
 - **debug tms controller error** or **debug tms consumer error**
 - **debug tms controller events** or **debug tms consumer events**
 - **debug tms consumer feature-interface**



Tip

You can also process these messages through syslog by enabling the **logging tms events** command in a TMS type parameter map type.

What to Do Next

Proceed to the next section to see information about updating and removing threats on a consumer.

Managing Threat Information Messages on a Consumer from the Controller

This task is optional. This task shows how to activate, deactivate and delete threat messages on one or all consumers. The **tms controller reset** command is entered in privileged EXEC mode.

Updating or Replacing a Loaded Threat

Each threat that is contained within a threat definition file is uniquely identified by the threat ID, owner ID, and version number. The controller uses the version field to ensure that the most recent threat is sent to consumers. A higher version number indicates a more current or newer threat.

To replace or update an existing threat in the loaded database, a modified threat definition file must be loaded to the controller. The threat contained within this file must have a higher number in the version field. If the version field is the same or contains a lower number, the updated threat will not be loaded.

To distribute the updated threat to TMS consumers, the older version of the threat must be removed from the active database. The **tms controller reset** command can be entered with the **delete** keyword to remove the threat from all consumers.

Prerequisites

- TIDP and TMS is operational on the controller and all consumers.
- A threat definition file that contains one or more TIMs has been put in the loaded database on the controller.

SUMMARY STEPS

1. **enable**
2. **tms controller reset {activate | delete | inactivate} group {group-id | all} owner owner-id tid {threat-id [- number] | all} consumer {all | ipv4 ip-address}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	tms controller reset {activate delete inactivate} group {group-id all} owner owner-id tid {threat-id [- number] all} consumer {all ipv4 ip-address} Example: Router# tms consumer reset activate group 10 owner 1000 tid 1000 consumer ipv4 10.1.1.2	Manages threat definition messages on a TMS consumer from the TMS controller. <ul style="list-style-type: none"> • A single peer or range of TIDP groups can be managed. • Threat definition files can be activated, deactivated, or deleted based on the group ID, owner ID, threat ID, or host address.

Examples

Threat Activation Example

The following example activates all threats on all consumers in all groups that belong to owner number 1000:

```
Router# tms controller reset activate group all owner 1000 tid all consumer all
```

Threat Removal Example

The following example removes threats, 1 through 10, from the active database for all consumers in group 10:

```
Router# tms controller reset delete group 10 owner 1000 tid 1 - 10 consumer all
```

Threat Deactivation Example

The following example deactivates threats, 1 through 10, from the active database for all consumers in group 10:

```
Router# tms controller reset inactivate group 10 owner 1000 tid 1 - 10 consumer all
```

Troubleshooting Tips

If you are unable to manage threats on a consumer, perform the following steps:

1. Verify the threat status on the controller and consumers by entering the **show tms controller** and **show tms consumer** commands. Filter the output to display information about the group and threat ID numbers.

2. If the consumer is reachable from the controller, enter the **tms consumer register** command on the consumer.
3. If the controller and consumers are properly configured and reachable but the consumer is still unable to synchronize, enable the following debug commands to display related error messages:
 - **debug tms controller error** or **debug tms consumer error**
 - **debug tms controller events** or **debug tms consumer events**
 - **debug tms consumer feature-interface**

**Tip**

You can also process these messages through syslog by enabling the **logging tms events** command in a TMS type parameter map type.

What to Do Next

Proceed to the next section to see information about sending a status request message to a consumer.

Sending a Status Request Message to Consumers from the TMS Controller

This task is optional. This task shows how to send a status request message from a controller to a consumer or group of consumers. The consumer must be registered to receive this message. In response, the consumer sends information about one or all threats to the controller. The **tms controller status** command is entered in privileged EXEC mode.

Prerequisites

- TIDP and TMS is operational on the controller and all consumers.
- A threat definition file that contains one or more threat information messages has been loaded on the controller.

SUMMARY STEPS

1. **enable**
2. **tms controller status {group {group-id | all} owner owner-id tid {threat-id [- number] | all} consumer {all | ipv4 ip-address}}**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	tms controller status {group {group-id all} owner owner-id tid {threat-id [- number] all} consumer {all ipv4 ip-address}} Example: Router# tms controller status group 10 owner 1000 tid 1 consumer ipv4 10.1.1.2	Sends a status request message to a TMS consumer from the TMS controller.

Examples

The following example sends a status request message for information about all threats from owner 1000:

```
Router# tms controller status group all owner 1000 tid all consumer all
```

The following example sends a status request message to the 10.1.1.2 consumer in group 10 for information threats, 1 through 10:

```
Router# tms controller status group 10 owner 1000 tid 1 - 10 consumer ipv4 10.1.1.2
```

Troubleshooting Tips

If you are unable to send a status request message to a consumer, perform the following steps:

1. Verify the threat status on the controller and consumers by entering the **show tms controller** and **show tms consumer** commands. Filter the output to display information about the group and threat ID numbers.
2. If the consumer is reachable from the controller, enter the **tms consumer register** command on the consumer.
3. If the controller and consumers are properly configured and reachable but the consumer is still unable to synchronize, enable the following debug commands to display related error messages:
 - **debug tms controller error** or **debug tms consumer error**
 - **debug tms controller events** or **debug tms consumer events**
 - **debug tms consumer feature-interface**



Tip

You can also process these messages through syslog by enabling the **logging tms events** command in a TMS type parameter map type.

What to Do Next

Proceed to the next section to see information about unloading threat messages from the loaded database.

Unloading a Threat Information Messages from the Loaded Database

This task is optional. This task shows how to unload a TIM from the “loaded” database. The **tms controller unload** command is entered on a TMS controller in privileged EXEC mode.

Loaded and Active Databases

Two databases are maintained on the controller: the “loaded” database and the “active” database. The **tms controller load threat** command is used to upload a threat definition file on the controller. Once the threat definition file has been loaded, individual threats contained within the threat definition file are placed in the “loaded” database for distribution to consumers. Threats are removed from the loaded database by entering the **tms controller unload** command. Entering this command does not remove the threat from the active database if the threat is active on at least one consumer.

A threat is placed in the “active” database when the **tms controller send** command is used to send one or more threats to one or more consumers. A threat remains in the active database as long as it is active on at least one consumer. An active threat can be removed from consumers by entering the **tms controller reset** command on the controller. Active threats can be removed on the consumer by entering **clear tms consumer** or by reloading the consumer.

Prerequisites

- TIDP and TMS is operational on the controller and all consumers.
- A threat definition file that contains one or more TIMs has been put in the loaded database on the controller.

SUMMARY STEPS

1. **enable**
2. **tms controller unload** {**owner** *owner-id* **tid** {*threat-id* [- *number*] | **all**}}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	tms controller unload { owner <i>owner-id</i> tid { <i>threat-id</i> [- <i>number</i>] all }} Example: Router# tms controller unload owner 10 tid 1-10	(Optional) Unloads a threat definition file from a TMS controller. <ul style="list-style-type: none"> The <i>owner-id</i> argument is entered as a number from 1 to 65535 The <i>threat-id</i> argument is entered as a number from 1 to 65535. A range of threat ID numbers can be configured by entering a hyphen and an ascending number.

Examples

The following example unloads threats, 1 through 10, from the loaded database on a TMS controller:

```
Router#_tms controller unload owner 1000 tid 1 - 10 threat
```

Troubleshooting Tips

If there is a problem loading or unloading an XML threat definition file, enabling the **debug tms controller xml error** command will configure the router to print related error messages.

What to Do Next

At completion of this procedure, all configuration tasks that are performed on a controller are complete. The remaining configuration tasks are performed on a consumer. Proceed to the next section for information about configuring the TMS Rules Engine on a consumer.

Configuring the TMS Rules Engine on a Consumer

This task is optional. The steps in this task show how to configure the TMS Rules Engine. The TMS Rules Engine is configured using a mitigation type service policy.

The TMS Rules Engine is used to configure a mitigation enforcement action directly on a consumer to override an enforcement action sent from the controller. The following tasks are performed in this section:

- The mitigation traffic class is defined in a class map
- The next hop variable is defined in parameter map
- A mitigation type policy map is configured to bind the class and parameter maps
- The mitigation type service policy is associated with the TMS type policy map

Mitigation Type Service Policy

The mitigation type service policy is configured only on the consumer. It is used to customize or override mitigation enforcement actions sent by the controller. The TMS Rules Engine is used to configure an ACL drop, an ignore, or a redirect enforcement action. Only one action can be configured for each mitigation type traffic class.

This type of service policy is created by configuring and linking mitigation type parameter and class maps to a mitigation type policy map. The class map is configured to define threat primitive and priority traffic matching conditions (as a class of traffic). The parameter map is configured to apply a next-hop variable to the class of traffic. The class and parameter maps are attached to a mitigation type policy map. The mitigation type service policy is activated by attaching the mitigation type policy map to a TMS type policy map, which is attached to the global TMS consumer process.

ACL Drop Rule

The ACL drop rule is configured to drop packets that are permitted by a predefined extended access-list. The **ip access-group** command is configured to attach the access list to the interface. The **tms-class** command is configured to associate the interface with the ACL drop enforcement action.

Ignore Rule

The ignore rule configures the TMS Rules Engine to ignore (not carry out any action for) a mitigation enforcement action defined for the matching traffic class. The traffic class is defined by the primitive and/or priority configured in a mitigation type class map.

Redirect Rule

The redirect rule is configured to redirect traffic to an explicitly defined IPv4 host, to a null interface or to an IPv4 host defined in a variable. The variable is initialized under the mitigation parameter-map using the **variable** command. If no destination is configured, the TMS Rules Engine will first check the threat information message (associated with the mitigation class map). If a destination cannot be derived from the threat information message, then the mitigation type parameter map is checked (if one is configured and attached to the mitigation type service policy).

If a next-hop IP address, null interface, or user-defined variable is not configured, the next hop variable must be defined in a mitigation type parameter map and then associated under the policy map with the **source parameter** command, or the parameter-map name must be specified in the *profile* attribute entered under the **parameter** tag in the threat definition file.

Prerequisites

- TIDP and TMS is operational on the controller and all consumers.
- A TMS type service policy has been configured and attached to the global TMS consumer process.

Restrictions

- Only one mitigation enforcement action can be configured for each mitigation type traffic class.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type mitigation** {[**match-all** | **match-any**] *name*}
4. **match priority** {*number*}
5. **match primitive** {**any** | **block** | **redirect** | *any-string*}
6. **exit**
7. **parameter-map type mitigation** {*name*}
8. **variable** *name* {**ipv4** *ip-address* | **null0**}
9. **exit**
10. **policy-map type control mitigation** {*name*}
11. **class** {*class-name* | **class-default**}
12. **acl drop**
13. **ignore**
14. **redirect route** {*next-hop-ip-address* | **null** | *\$-variable*}
15. **source parameter**{*parameter-map*}
16. **exit**
17. **exit**
18. **policy-map type control mitigation** {*name*}
19. **service-policy** {*policy-map*}
20. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	class-map type mitigation {[match-all match-any] name} Example: Router(config)# class-map type mitigation MIT_CLASS_1	Configures a mitigation class map. Note Match all is default behavior if no optional keywords are configured.
Step 4	match priority {number} Example: Router(config-cmap)# match priority 4	Configures the traffic class to match the priority level of a mitigation enforcement action.
Step 5	match primitive {any block redirect any-string} Example: Router(config-cmap)# match primitive block	Configures the traffic class to match the primitive (mitigation enforcement action.)
Step 6	exit Example: Router(config-cmap)# exit	Exits class map configuration mode, and enters global configuration mode.
Step 7	parameter-map type {mitigation name tms name} Example: Router(config)# parameter-map type mitigation MIT_PAR_1	Configures a mitigation type parameter map.
Step 8	variable name {ipv4 ip-address null0} Example: Router(config-profile)# variable nexthop ipv4 192.168.1.1	Defines the next-hop variable in the mitigation type parameter map.
Step 9	exit Example: Router(config-profile)# exit	Exits parameter-map configuration mode, and enters global configuration mode.

	Command or Action	Purpose
Step 10	policy-map type control mitigation {name} Example: Router(config)# policy-map type control mitigation MIT_POL_1	Configures a mitigation type policy map.
Step 11	class {class-name class-default} Example: Router(config-pmap)# class MIT_CLASS_1	Attaches the mitigation traffic class to the policy map. <ul style="list-style-type: none"> The <i>class-name</i> argument must be configured in this step.
Step 12	redirect route {next-hop-ip-address null \$-variable} Example: Router(config-pmap-c)# redirect route	(Optional) Configures a redirect enforcement action in a mitigation type policy map. <ul style="list-style-type: none"> The next hop is configured as specific IP address, the null 0 interface, or a user-defined variable. If a user-defined variable is entered, the variable string must start with the \$ character.
Step 13	acl drop Example: Router(config-pmap-c)# acl drop	(Optional) Configures an access list drop enforcement action. <ul style="list-style-type: none"> The drop action is based on a predefined named access list.
Step 14	ignore Example: Router(config-pmap-c)# ignore	(Optional) Configures TMS to ignore the enforcement action.
Step 15	source parameter {parameter-map} Example: Router(config-pmap-c)# source parameter MIT_PAR_1	Attaches a mitigation type parameter map in a policy-map class configuration.
Step 16	exit Example: Router(config-pmap-c)# exit	Exits policy-map class configuration mode, and enters policy-map configuration mode.
Step 17	exit Example: Router(config-pmap)# exit	Exits policy-map configuration mode, and enters global configuration mode.
Step 18	policy-map type control {mitigation name tms name} Example: Router(config)# policy-map type control tms TMS_POL_1	Configures the TMS type policy map.

	Command or Action	Purpose
Step 19	class { <i>name</i> } Example: Router(config-pmap)# class MIT_CLASS_1	Configures the TMS type class under the policy map. Note The TMS type class-map configuration is not shown in this task table.
Step 20	service-policy { <i>policy-map</i> } Example: Router(config-pmap-c)# service policy MIT_POL_1	Attaches the mitigation type policy map to the TMS type policy map. Note A TMS type policy map that has a mitigation type policy map attached cannot be attached to a global TMS controller process.
Step 21	end Example: Router	Exits policy-map class configuration mode, and enters privileged EXEC mode.

Examples

ACL Drop Rule Example

The following example, starting in global configuration mode, configures an ACL drop enforcement action. Traffic that matches the extended access list (172.16.1/24) is dropped.

```
Router(config)# ip access-list extended 100
Router(config-ipacl)# permit ip 172.16.1.0 0.0.0.255 any
Router(config-ipacl)# exit
Router(config)# interface Ethernet 0/0
Router(config-if)# ip access-group 100 in
Router(config-if)# tms-class
Router(config-if)# exit
Router(config)# class-map type mitigation match-all MIT_CLASS_1
Router(config-cmap)# match priority 3
Router(config-cmap)# match primitive block
Router(config-cmap)# exit
Router(config)# policy-map type control mitigation MIT_POL_1
Router(config-pmap)# class MIT_CLASS_1
Router(config-pmap-c)# acl drop
Router(config-pmap-c)# end
```

Blackhole (Redirect) Rule Example

The following example, starting in global configuration mode, configures the TMS Rules Engine to send priority 5 redirect threat mitigation traffic to a null interface (black hole):

```
Router(config)# parameter-map type mitigation MIT_PAR_2
Router(config-profile)# variable RTBH NULL0
Router(config-profile)# exit
Router(config)# class-map type mitigation match-all MIT_CLASS_2
Router(config-cmap)# match priority 5
Router(config-cmap)# match primitive redirect
Router(config-cmap)# exit
Router(config)# policy-map type control mitigation MIT_POL_2
Router(config-pmap)# class MIT_CLASS_2
Router(config-pmap-c)# source parameter MIT_PAR_2
Router(config-pmap-c)# redirect route $RTBH
Router(config-pmap-c)# end
```

Collection (Redirect) Rule Example

The following example, starting in global configuration mode, configures the TMS Rules Engine to set the next hop variable to 192.168.1.1 for traffic that matches the mitigation class (priority 1 traffic and any primitive):

```
Router(config)# class-map type mitigation MIT_CLASS_3
Router(config-cmap)# match primitive any
Router(config-cmap)# match priority 1
Router(config-cmap)# exit
Router(config)# parameter-map type mitigation MIT_PAR_3
Router(config-profile)# variable COLLECTION ipv4 192.168.1.1
Router(config-profile)# exit
Router(config)# policy-map type control mitigation MIT_POL_3
Router(config-pmap)# class MIT_CLASS_3
Router(config-pmap-c)# source parameter MIT_PAR_3
Router(config-pmap-c)# end
```

Ignore Example

The following example, starting in global configuration mode, configures a TMS consumer to ignore a priority 5 redirect primitive:

```
Router(config)# parameter-map type mitigation MIT_PAR_4
Router(config-profile)# variable RTBH NULL0
Router(config-profile)# exit
Router(config)# class-map type mitigation match-all MIT_CLASS_4
Router(config-cmap)# match priority 5
Router(config-cmap)# match primitive redirect
Router(config-cmap)# exit
Router(config)# policy-map type control mitigation MIT_POL_4
Router(config-pmap)# class MIT_CLASS_4
Router(config-pmap-c)# source parameter MIT_PAR_4
Router(config-pmap-c)# ignore
Router(config-pmap-c)# end
```

Activating the TMS Rules Engine Example (Complete Configuration)

The following example, starting in global configuration mode, creates a Rules Engine configuration and activates it under the global TMS consumer process:

```
Router(config)# class-map type mitigation MIT_CLASS_3
Router(config-cmap)# match primitive block
Router(config-cmap)# match priority 1
Router(config-cmap)# exit
Router(config)# parameter-map type mitigation MIT_PAR_3
Router(config-profile)# variable COLLECTION ipv4 192.168.1.1
Router(config-profile)# exit
Router(config)# policy-map type control mitigation MIT_POL_3
Router(config-pmap)# class MIT_CLASS_3
Router(config-pmap-c)# redirect route
Router(config-pmap-c)# source parameter MIT_PAR_3
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# policy-map type control tms TMS_POL_1
Router(config-pmap)# class TMS_CLASS_1
Router(config-pmap-c)# mitigation TMS_PAR_1
Router(config-pmap-c)# service-policy MIT_POL_3
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# tms consumer
Router(config-cons)# service-policy type tms TMS_POL_1
Router(config-cons)# end
```

Troubleshooting Tips

Troubleshooting Strict Match Mitigation Policies

The TMS Rules Engine provides a flexible mechanism to match TIMs on the TMS consumer. A match policy can be configured to match any (first) threat priority or primitive or to match all (strict).

Match all is the default when a mitigation type class map is configured without entering either optional keyword. This, as the name implies, is a strict match that requires all elements to match in order for the rule to be processed. Therefore, it is possible to configure a strict match that cannot function because it is impossible to match all elements. The following example illustrates this point:

```
class-map type mitigation MIT_CLASS
  match primitive block
  match primitive redirect
  match priority 2
  match priority 3
```

The above configuration uses a default match-all rule because no keyword is entered. The match-all rule invalidates the above configuration because no threat can satisfy all match criteria (block and redirect).

This configuration can be corrected by configuring the class map with the **match-any** keyword, as shown in the following configuration:

```
class-map type mitigation match-any MIT_CLASS
  match primitive block
  match primitive redirect
  match priority 2
  match priority 3
```

The above configuration could be configured with a match-all rule if either the block or redirect primitive is removed.

General TMS Rules Engine Troubleshooting

The Rules Engine configuration can be verified by entering the **show tms consumer** and **show tms controller** commands. If the enforcement action is not applied, you can enable the **debug tms consumer feature-interface** command to print error messages to help determine if the correct feature interface is called (ACL or OER).

What to Do Next

In this task, the TMS Rules Engine was configured to override a threat enforcement action on the consumer. Proceed to the next section to see information on excluding a device from TMS control.

Configuring Local Device Exceptions on a Consumer

This task is optional. The steps in this task show how to configure local device exceptions. Local device exceptions are configured on TMS consumers only. A local device exception is an override configured for a specific host IP address or network. The TMS consumer negates a mitigation enforcement action sent from the controller or from a mitigation type service policy configured on the consumer.

For example, traffic from the 192.168.1.0/24 network is considered to be suspect. So, an ACL drop enforcement action is configured for all traffic sourced from this network. However, a device with a host address in this range (192.168.1.55) needs to transit over a specific consumer. A local device exception is configured on the consumer to override ACL drop enforcement action.

A host IP address (or any other subset of the network) is defined in an extended access list and then referenced by the **exception access-group** command. The **tms-class** command is configured to associate an interface with the device exception. The enforcement action configured on the controller is not applied to traffic that is permitted by the access list.

Prerequisites

- TIDP and TMS is operational on the controller and all consumers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list** {**standard** | **extended**} [*access-list-name* | *access-list-number*]
4. [*sequence-number*] **permit** | **deny protocol** *source source-wildcard destination destination-wildcard* [**option** *option-value*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]
5. **exit**
6. **interface** {*type* | *number*}
7. **ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**}
8. **tms-class**
9. **exit**
10. **tms consumer**
11. **exception access-group** {*extended-acl*}
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip access-list { standard extended } [<i>access-list-name</i> <i>access-list-number</i>] Example: Router(config)# ip access-list extended NAMEDACL	Specifies the IP access list type, and enters the corresponding access list configuration mode. <ul style="list-style-type: none"> A named or numbered extended access list must be configured in this step.
Step 4	[<i>sequence-number</i>] permit deny protocol source <i>source-wildcard destination</i> <i>destination-wildcard</i> [option <i>option-value</i>] [precedence <i>precedence</i>] [tos <i>tos</i>] [log] [time-range <i>time-range-name</i>] [fragments] Example: Router(config-ext-nacl)# permit tcp host 192.168.1.55 any	Defines the criteria for which the access list will permit or deny packets. <ul style="list-style-type: none"> A host IP address or any subset of the network can be configured.
Step 5	exit Example: Router(config-ext-nacl)# exit	Exits named access list configuration mode, and enters global configuration mode.
Step 6	interface { <i>type</i> <i>number</i> } Example: Router(config)# interface Ethernet 0/0	Enters interface configuration mode to configure an interface.
Step 7	ip access-group { <i>access-list-number</i> <i>access-list-name</i> } { in out } Example: Router(config-if)# ip access-group NAMED_ACL in	Applies an access list to the interface.
Step 8	tms-class Example: Router(config-if)# tms-class	Associates the interface with the device exception.
Step 9	exit Example: Router(config-if)# exit	Exits interface configuration mode, and enters global configuration mode.

	Command or Action	Purpose
Step 10	tms consumer Example: Router(config)# tms consumer	Enters TMS consumer configuration mode to configure a consumer.
Step 11	exception access-group {named-acl} Example: Router(cfg-tms-cons)# exception access-group NAMED_ACL	Defines the extended access list as the source criteria for the device exception under the global TMS consumer process.
Step 12	end Example: Router(cfg-tms-cons)# end	Exits TMS consumer configuration mode, and enters privileged EXEC mode.

Examples

The following example, starting in global configuration mode, configures an device exception for the 192.168.1.55 host address:

```
Router(config)# ip access-list extended NAMED_ACL
Router(config-ext-nacl)# permit tcp host 192.168.1.55 any
Router(config-ext-nacl)# exit
Router(config)# interface Ethernet 0/0
Router(config-if)# ip access-group NAMED_ACL in
Router(config-if)# tms-class
Router(config-if)# exit
Router(config)# tms consumer
Router(cfg-tms-cons)# exception access-group NAMED_ACL
Router(cfg-tms-cons)# service-policy type tms TMS_POL_1
Router(cfg-tms-cons)# end
```

Troubleshooting Tips

If the interface is operational and the device exception is properly configured, you can enable the **debug tms consumer feature-interface** command to print error messages to help determine if the correct feature interface is called (ACL or OER).

What to Do Next

At completion of this task, all procedures related to TMS configuration and management have been completed. Proceed to the following sections to see information about using TMS **clear**, **show**, and **debug** commands.

Clearing Threat Information Messages on a Consumer

This task is optional. This task shows how to clear threat information messages on a TMS consumer. The **clear tms consumer group** command is entered in privileged EXEC mode. Entering this command on a consumer has an effect similar to entering the **tms controller reset** command from the TMS controller.

SUMMARY STEPS

1. **enable**
2. **clear tms consumer group** {*group-id* | **all**} **owner** {*owner-id* | **any**} **tid** {*threat-id* [- *number*] | **all**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	clear tms consumer group { <i>group-id</i> all } owner { <i>owner-id</i> any } tid { <i>threat-id</i> [- <i>number</i>] all } Example: Router# clear tms consumer group all owner any tid all	Clears threat information messages on a TMS consumer.

Examples

The following example clears all threat information messages:

```
Router# clear tms consumer group all owner any tid all
```

Troubleshooting Tips

The **show tms controller** and **show tms consumer** commands can be entered to verify that the clear command was successful.

What to Do Next

Proceed to the next section to see information on verifying TMS configuration.

Verifying TMS Configuration and Threat Status on a Controller or Consumer

This task is optional. This task shows how to verify TMS configuration on a controller or consumer using TMS show commands. All commands described in this section are entered in privileged EXEC mode.

SUMMARY STEPS

1. **enable**
2. **show tms consumer**
3. **show tms consumer group** {*group-id* [**owner** {*owner-id* | **any**}] **tid** {*threat-id* | **all**} [**controller** *ipv4 ip-address*] [**verbose**] | **threats**] | **all** **owner** {*owner-id* | **any**} **tid** {*threat-id* | **all**} [**controller** *ipv4 ip-address*] [**verbose**]}

4. **show tms controller**
5. **show tms controller group** {group-id [owner {owner-id | any}] tid {threat-id | all} [controller ipv4 ip-address] [verbose] | threats] | all owner {owner-id | any} tid {threat-id | all} [controller ipv4 ip-address] [verbose]}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show tms consumer Example: Router# show tms consumer	Displays information about TMS consumer registration, TIDP membership, and TMS controllers.
Step 3	show tms consumer group {group-id [owner {owner-id any}] tid {threat-id all} [consumer ipv4 ip-address] [verbose] threats] all owner {owner-id any} tid {threat-id all} [controller ipv4 ip-address] [verbose]} Example: Router# show tms consumer group all owner any tid all verbose	Displays information about threats sent to the specified consumer groups.
Step 4	show tms controller Example: Router# show tms controller	Displays information about TMS consumer registration and TIDP membership.
Step 5	show tms controller group {group-id [owner {owner-id any}] tid {threat-id all} [controller ipv4 ip-address] [verbose] threats] all owner {owner-id any} tid {threat-id all} [controller ipv4 ip-address] [verbose]} Example: Router# show tms controller group 10	Displays information about TMS controller groups.

Examples

show tms consumer example

The following example is sample output from the **show tms consumer** command:

```
Router# show tms consumer

TMS Interface details
Interface      Edge      SubDeviceClass
-----      -

```

```

Fa0/0
Fa0/1    Edge

TIDP-Group    TMS-Controller-IP    Status
-----
10            10.11.11.55                Registered Successfully
20            10.11.11.55                Registered Successfully

```

show tms consumer group examples

The following is sample output from the **show tms consumer group** command.

```
Router# show tms consumer group all owner any tid all verbose
```

OwnerID	TID	Ver	Group	Controller	Status	ActionTaken
1	1	1	10	10.1.1.1	Active	Redirect 172.16.1.1
1	2	1	10	10.1.1.1	Active	Redirect NULL
1	3	1	10	10.1.1.1	Inactive	Threat Inactive
2	10	1	10	10.1.1.1	Active	ACL-Drop
2	20	1	10	10.1.1.1	Active	ACL-Drop

The following example is sample output from the **show tms consumer group** command entered with the **threats** keyword:

```
Router# show tms consumer group 10 threats
```

```
TIDP Group 10
Number of Threats : 13
```

```

#sh tms controller group 10 threats
TIDP Group 10 ptr 656C4848
Number of Threats : 1
OwnerID    TID    Ver    State
-----
1          10     1      Active

```

show tms controller example

The following is sample output from the **show tms controller** command:

```
Router# show tms controller
```

TIDP-Group	TMS-Consumer-IP	Status
10	10.3.3.2	Registered Successfully
10	10.1.1.2	Registered Successfully
20	10.3.3.2	Registered Successfully
20	10.1.1.2	Registered Successfully

show tms controller group example

The following is sample output from the **show tms controller group** command:

```
Router# show tms controller group 10
```

```

TMS-Controller# show tms controller group all owner any tid all verbose
OwnerID    TID    Ver    Group    Consumer    Status    ActionTaken
-----

```

1	1	1			Load	Active	
1	1	1	10	10.1.1.2		Active	Redirect 172.16.1.1
1	2	1			Load	Active	
1	2	1	10	10.1.1.2		Active	Redirect NULL
1	3	1			Load	Active	
1	3	1	10	10.1.1.2		Inactive	Threat Inactive
2	10	1			Load	Active	
2	10	1	10	10.1.1.2		Active	ACL-Drop
2	20	1			Load	Active	
2	20	1	10	10.1.1.2		Active	ACL-Drop

What to Do Next

Proceed to the next section to see information on enabling TMS debug messages.

Enabling TMS Debug Messages on a Controller or Consumer

This task shows how to enable TMS debugging on a controller or consumer. All commands described in this section are entered in privileged EXEC mode.

Restrictions

These commands should be used with caution on a production router or networking device. We recommend that debugging is enabled for only individual components as necessary. This restriction is intended to prevent the console session from be overwhelmed by large numbers of messages.

SUMMARY STEPS

1. **enable**
2. **debug tms consumer { all | errors [details] | events [details] | feature-interface | packet | protocol | xml [detail | error] }**
3. **debug tms controller { all | errors [details] | events [details] | feature-interface | packet | protocol | xml [detail | error] }**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	debug tms consumer {all errors [details] events [details] feature-interface packet protocol xml [detail error]} Example: Router# debug tms consumer all	Enables the generation of debugging messages on a TMS consumer.
Step 3	debug tms controller {all errors [details] events [details] feature-interface packet protocol xml [detail error]} Example: Router# debug tms controller xml detail	Enables the generation of debugging messages on a TMS controller.

Examples

Consumer Event Debugging Example

The following is sample output from the **debug tms consumer** command entered with the **events** keyword:

```
Router# debug tms consumer events
```

```
TMS consumer event debugging is on
*Feb 27 21:27:18: TMS_EVE_CO:start timer Controller=10.1.1.1 period=180
*Feb 27 21:27:18: TMS_EVE:Posting a message for the service layer
*Feb 27 21:27:18: TMS_EVE_CO:Processing Reg message from ctrl=10.1.1.1 group=10
*Feb 27 21:27:18: TMS_EVE_CO:Processing Reg response from ctrl=10.1.1.1 group=10
*Feb 27 21:27:18: TMS_EVE_CO:start timer Controller=10.1.1.1 period=120
```

Consumer Feature-Interface Debugging Example

The following is sample output from the **debug tms consumer** command entered with the **feature-interface** keyword:

```
Router# debug tms consumer feature-interface
```

```
TMS consumer feature-interface debugging is on
*Feb 27 21:28:12: TMS_FI_CO:OER:Policy Add client 2 pol id 12 tag 5000 nxthop 172.16.1.1
*Feb 27 21:28:12: TMS_FI_CO:OERCB:ctx C type 2 values 0
*Feb 27 21:28:12: TMS_FI_CO:OERCB:return code rcvd rc 1
*Feb 27 21:28:12: TMS_FI_CO:OERCB:Threat (1, 1, 1) grpId 10 ctrlIp 10.1.1.1 statflags 0
pol state 1
*Feb 27 21:28:12: TMS_FI_CO:OERCB:Prefix create client 2 id 12 src 0.0.0.0 0.0.0.0 dst
192.168.8.0 255.255.255.0 proto 6 0 - 0, 10 - 2000 grant TRUE exact TRUE
*Feb 27 21:28:12: TMS_FI_CO:OERCB:ctx C type 2 values 0
*Feb 27 21:28:12: TMS_FI_CO:OERCB:return code rcvd rc 1
```

```
*Feb 27 21:28:12: TMS_FI_CO:OERCB:Threat (1, 1, 1) grpId 10 ctrlIp 10.1.1.1 statFlags 0
pol state 3
*Feb 27 21:28:12: TMS_FI_CO:OERCB:Prefix create success with rc = 1
*Feb 27 21:28:13: TMS_FI_CO:ACL:CB3: acl 66886028 item 669C9F98 type 3 ADD
*Feb 27 21:28:13: TMS_FI_CO:ACL:CB1: acl 66886028 modified.
*Feb 27 21:28:13: TMS_FI_CO:ACL:CB3: acl 66886098 item 669CA0E0 type 3 ADD
*Feb 27 21:28:13: TMS_FI_CO:ACL:CB1: acl 66886098 modified.
```

Consumer Packet Debugging Example

The following is sample output from the **debug tms consumer** command entered with the **packet** keyword:

```
Router# debug tms consumer packet
```

```
TMS consumer packets debugging is on
*Feb 27 00:00:38: TMSCONS:out:Type(6)HeartBeat Req trans-id 15698 len 16
*Feb 27 00:00:38:   tms_flags 8 msg_flags 0 reason 0
*Feb 27 00:00:38:   TLVs:
*Feb 27 00:00:38: TMSCONS:in:Type(6)HeartBeat Req trans-id 158 len 16
*Feb 27 00:00:38:   tms_flags 0 msg_flags 0 reason 0
*Feb 27 00:00:38:   TLVs:
```

Consumer Protocol Debugging Example

The following is sample output from the **debug tms consumer** command entered with the **protocol** keyword:

```
Router# debug tms consumer protocol
```

```
TMS consumer protocol debugging is on
*Feb 27 21:27:18: TMS_PRO_CO:Sending RegReq ctrl=10.1.1.1 group=10
*Feb 27 21:27:18: TMS_PRO_CO:RegResp recvd controller 10.1.1.1 group 10
*Feb 27 21:27:18: TMS_PRO_CO:Sending Resync request for ctrl=10.1.1.1 group=10
*Feb 27 21:27:18: TMS_PRO_CO:Resync response recvd controller 10.1.1.1, group 10
*Feb 27 21:27:18: TMS_PRO_CO:Processing Resync response from Controller=10.1.1.1on
Group=10
*Feb 27 21:28:12: TMS_PRO_CO:Threat msg recvd controller 10.1.1.1, Group 10
*Feb 27 21:28:12: TMS_PRO_CO:Processing Threat request from Controller=10.1.1.1on Group=10
*Feb 27 21:28:12: TMS_PRO_CO:msg:NewThreat (1,1,1) in grp 10 ctrl 10.1.1.1
*Feb 27 21:28:58: TMS_PRO_CO:Heartbeat msg recvd controller 10.1.1.1, Group 10
```

Controller Event Debugging Example

The following is sample output from the **debug tms controller** command entered with the **events** keyword:

```
Router# debug tms controller events
```

```
TMS controller events debugging is on
*Feb 27 10:12:42: TMS_EVE_CN:Timer expired group=10
*Feb 27 10:12:42: TMS_EVE_CN:Start timer: Group=10, period=120
*Feb 27 10:12:42: TMS_EVE_CN:Posting a message for the service layer
*Feb 27 10:12:42: TMS_EVE_CN:Data packet recvd from DL layer
*Feb 27 10:13:34: TMS_EVE_CN:Posting a message for the service layer
*Feb 27 10:13:34: TMS_EVE_CN:Data packet recvd from DL layer
*Feb 27 10:13:34: TMS_EVE_CN:Start timer: Group=10, period=120
*Feb 27 10:13:34: TMS_EVE_CN:Posting a message for the service layer
*Feb 27 10:13:34: TMS_EVE_CN:Data packet recvd from DL layer
```

Controller Packet Debugging Example

The following is sample output from the **debug tms controller** command entered with the **packet** keyword:

```
Router# debug tms controller packet

TMS controller packets debugging is on
TMS controller packets debugging is on
*Feb 27 10:13:34: TMSCTRL:in:Type(1)Registration Req trans-id 15685 len 16
*Feb 27 10:13:34:   tms_flags 8 msg_flags 1 reason 0
*Feb 27 10:13:34:   TLVs:
*Feb 27 10:13:34: TMSCTRL:out:Type(1)Registration Resp trans-id 15685 len 16
*Feb 27 10:13:34:   tms_flags 1 msg_flags 1 reason 1
*Feb 27 10:13:34:   TLVs:
*Feb 27 10:13:34: TMSCTRL:in:Type(4)Resync/Audit Req trans-id 15686 len 16
*Feb 27 10:13:34:   tms_flags 8 msg_flags 1 reason 0
*Feb 27 10:13:34:   TLVs:
*Feb 27 10:13:34: TMSCTRL:out:Type(4)Resync/Audit Resp trans-id 15686 len 24
*Feb 27 10:13:34:   tms_flags 1 msg_flags 0 reason 0
*Feb 27 10:13:34:   TLVs: Summary(514,8)
```

Controller Protocol Debugging Example

The following is sample output from the **debug tms controller** command entered with the **protocol** keyword:

```
Router# debug tms controller protocol

TMS controller protocol debugging is on
*Feb 27 10:13:34: TMS_PRO_CN:Registration request recvd consumer 10.1.1.2, group 10
*Feb 27 10:13:34: TMS_PRO_CN:Sending Reg resp to cons=10.1.1.2 group=10
*Feb 27 10:13:34: TMS_PRO_CN:Resync request recvd consumer 10.1.1.2, group 10
*Feb 27 10:13:34: TMS_PRO_CN:Received Resync Req Group=10
*Feb 27 10:13:34: TMS_PRO_CN:Sending Resync resp for cons=10.1.1.2 group=10 ntids=0
```

XML Debugging Example

The following is sample output from the **debug tms controller** command entered with the **xml** keyword:

```
Router# debug tms controller xml

TMS controller xml debugs debugging is on
*Feb 27 10:13:45: TMS_XML_CN:Found tag threat in threat file
*Feb 27 10:13:45: TMS_XML_CN:Found tag threat_info in threat file
*Feb 27 10:13:45: TMS_XML_CN:Found tag primitive in threat file
*Feb 27 10:13:45: TMS_XML_CN:Found tag parameter in threat file
*Feb 27 10:13:45: TMS_XML_CN:Found tag tcdf in threat file
*Feb 27 10:13:45: TMS_XML_CN:Found tag threat in threat file
*Feb 27 10:13:45: TMS_XML_CN:Found tag threat_info in threat file
*Feb 27 10:13:45: TMS_XML_CN:Found tag parameter in threat file
*Feb 27 10:13:45: TMS_XML_CN:Found tag primitive in threat file
*Feb 27 10:13:45: TMS_XML_CN:Found tag tcdf in threat file
*Feb 27 10:13:45: TMS_XML_CN:Found tag threat in threat file
*Feb 27 10:13:45: TMS_XML_CN:Found tag threat_info in threat file
*Feb 27 10:13:45: TMS_XML_CN:Found tag parameter in threat file
*Feb 27 10:13:45: TMS_XML_CN:Found tag primitive in threat file
*Feb 27 10:13:45: TMS_XML_CN:Found tag tcdf in threat file
*Feb 27 10:13:45: TMS_XML_EVE:Decoding threat tag
*Feb 27 10:13:45: TMS_XML_EVE:Found threat
*Feb 27 10:13:45: TMS_XML_EVE:Decoded threat TLV - threat id : 1, owner id : 1,
version : 1
*Feb 27 10:13:45: TMS_XML_EVE:Decoding threat info
```

```

*Feb 27 10:13:45: TMS_XML_EVE:Found threat info
*Feb 27 10:13:45: TMS_XML_EVE:Found ERR
*Feb 27 10:13:45: TMS_XML_EVE:name is name, value is tc2
*Feb 27 10:13:45: Decoded Threat desc TLV:
*Feb 27 10:13:45: Threat name = NAME:
*Feb 27 10:13:45: Threat text = THREATTEXT:
*Feb 27 10:13:45: Mitigation text = mitigationtext:
*Feb 27 10:13:45: Threat classes : [ tc2 ]
*Feb 27 10:13:45: ERR:
*Feb 27 10:13:45: ASR = 5, SFR = 20, TFR = 40, ARR = 30 PD = 50
*Feb 27 10:13:45: TMS_XML_EVE:Decoding primitive
*Feb 27 10:13:45: TMS_XML_EVE:Found primitive
*Feb 27 10:13:45: TMS-XML: Decoded primitive TLV
*Feb 27 10:13:45: Prim type = 2
*Feb 27 10:13:45: Primitive = redirect
*Feb 27 10:13:45: TMS_XML_EVE:Decoding parameter
*Feb 27 10:13:45: TMS_XML_EVE:CNS PARSER : Node is 129 tag = parameter
*Feb 27 10:13:45: TMS_XML_EVE:Found parameter
*Feb 27 10:13:45: TMS_XML_EVE:CNS PARSER : Node is 130 tag = redirect
*Feb 27 10:13:45: TMS_XML_EVE:parameter : Found redirect
*Feb 27 10:13:45: TMS_XML_EVE:Found nexthop in redirect
*Feb 27 10:13:45: TMS_XML:Decoded Parameter TLV
*Feb 27 10:13:45: Parameter type = 1
*Feb 27 10:13:45: Redirect addr = 172.16.1.1
*Feb 27 10:13:45: TMS_XML_EVE:Decoding match criteria
*Feb 27 10:13:45: TMS-XML: Decoded match crt TLV :
*Feb 27 10:13:45: Src addr : 0.0.0.0 , Src mask : 0.0.0.0
*Feb 27 10:13:45: Dest addr : 192.168.8.0 , Dest mask : 255.255.255.0
*Feb 27 10:13:45: Protocol : 6
*Feb 27 10:13:45: Src port - Start : 0, End : 0
*Feb 27 10:13:45: Dest port - Start : 10, End : 2000
*Feb 27 10:13:45: TMS_EVE_CN:Threat (1,1,1) allocated.
*Feb 27 10:13:45: TMS_EVE_CN:Threat (1,1,1) added to LoadDB.
*Feb 27 10:13:45: TMS_XML_CN:Threat (1,1,1) Loaded into LoadDB
*Feb 27 10:13:45: TMS_XML_EVE:Decoding threat tag
*Feb 27 10:13:45: TMS_XML_EVE:Found threat
*Feb 27 10:13:45: TMS_XML_EVE:Decoded threat TLV - threat id : 2, owner id : 1,
version : 1

```

What to Do Next

Proceed to the next section to see complete TMS configuration examples.

Configuration Examples for TMS

This section provides the following configuration examples:

- [Controller: TMS Configuration Example, page 59](#)
- [Consumer: TMS Configuration Example, page 60](#)
- [Consumer: TMS Rules Engine Configuration Example, page 61](#)

Controller: TMS Configuration Example

The following example, starting in global configuration mode, configures a TMS type parameter map:


```
Router(config)# parameter-map type tms TMS_PAR_1
Router(config-profile)# logging tms events
Router(config-profile)# heartbeat retry interval 60
Router(config-profile)# heartbeat retry count 3
Router(config-profile)# message retry interval 15
Router(config-profile)# message retry count 5
Router(config-profile)# exit
```

TMS groups 10 through 20 and group 30 are configured as a TMS traffic class:

```
Router(config)# class-map type tms TMS_CLASS_1
Router(config-cmap)# match tidp group 10 - 20
Router(config-cmap)# match tidp group 30
Router(config-cmap)# exit
```

TMS type class and parameter maps are attached to a TMS type policy map:

```
Router(config)# policy-map type control tms TMS_POL_1
Router(config-pmap)# class TMS_CLASS_1
Router(config-pmap-c)# mitigation TMS_PAR_1
Router(config-pmap-c)# end
```

A global TMS controller process is created and a policy map (TMS type service policy) is attached:

```
Router(config)# tms controller
Router(cfg-tms-ctrl)# service-policy type tms TMS_POL_1
Router(cfg-tms-ctrl)# end
```

Consumer: TMS Configuration Example

The following example, starting in global configuration mode, configures a TMS type parameter map:

```
Router(config)# parameter-map type tms TMS_PAR_2
Router(config-profile)# controller ipv4 10.1.1.1
Router(config-profile)# logging tms events
Router(config-profile)# registration retry count 5
Router(config-profile)# registration retry interval 60
Router(config-profile)# exit
```

TMS groups 10 through 20 and group 30 are configured as a TMS traffic class:

```
Router(config)# class-map type tms TMS_CLASS_2
Router(config-cmap)# match tidp group 10 - 20
Router(config-cmap)# match tidp group 30
Router(config-cmap)# exit
```

TMS type class and parameter maps are attached to a TMS type policy map:

```
Router(config)# policy-map type control tms TMS_POL_2
Router(config-pmap)# class TMS_CLASS_2
Router(config-pmap-c)# mitigation TMS_PAR_2
Router(config-pmap-c)# end
```

A global TMS consumer process is created and a policy map (TMS type service policy) is attached. A local device exception is configured for the 192.168.1.55 host.

```
Router(config)# ip access-list extended NAMED_ACL
Router(config-ext-nacl)# permit tcp host 192.168.1.55 any
Router(config-ext-nacl)# exit
Router(config)# interface Ethernet 0/0
Router(config-if)# ip access-group NAMED_ACL in
Router(config-if)# tms-class
```

```
Router(config-if)# exit
Router(config)# tms consumer
Router(cfg-tms-cons)# exception access-group NAMED_ACL
Router(cfg-tms-cons)# service-policy type tms TMS_POL_2
Router(cfg-tms-cons)# end
```

Consumer: TMS Rules Engine Configuration Example

The following example, starting in global configuration mode, creates a TMS Rules Engine configuration and activates it under the global TMS consumer process.

The priority 1 block traffic is defined as a traffic class:

```
Router(config)# class-map type mitigation MIT_CLASS_3
Router(config-cmap)# match primitive block
Router(config-cmap)# match priority 1
Router(config-cmap)# exit
```

The next-hop variable is defined in a mitigation type parameter map:

```
Router(config)# parameter-map type mitigation MIT_PAR_3
Router(config-profile)# variable COLLECTION ipv4 192.168.1.1
Router(config-profile)# exit
```

The mitigation type policy map is configured to bind the class and parameter maps. A redirect mitigation action is also configured in this policy map:

```
Router(config)# policy-map type control mitigation MIT_POL_3
Router(config-pmap)# class MIT_CLASS_3
Router(config-pmap-c)# redirect route
Router(config-pmap-c)# source parameter MIT_PAR_3
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

The mitigation service policy (TMS Rules Engine configuration) is attached to a TMS type policy map:

```
Router(config)# policy-map type control tms TMS_POL_2
Router(config-pmap)# class TMS_CLASS_1
Router(config-pmap-c)# mitigation TMS_PAR_2
Router(config-pmap-c)# service-policy MIT_POL_3
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

The TMS type policy map is attached to a global consumer process, activating the mitigation type service policy:

```
Router(config)# tms consumer
Router(config-cons)# service-policy type tms TMS_POL_2
Router(config-cons)# end
```

Additional References

The following sections provide references related to TMS.

Related Documents

Related Topic	Document Title
Cisco IOS Configuration Fundamentals Configuration Guide	<i>Cisco IOS Configuration Fundamentals Configuration Guide</i> , Release 12.4 http://www.cisco.com/en/US/customer/products/ps6350/products_configuration_guide_book09186a0080430ee6.html
Cisco IOS Configuration Fundamentals Command Reference	<i>Cisco IOS Configuration Fundamentals Command Reference</i> , Release 12.4T http://www.cisco.com/en/US/customer/products/ps6441/products_command_reference_book09186a0080497a1e.html
Cisco IOS Optimized Edge Routing Configuration Guide	<i>Cisco IOS Optimized Edge Routing Configuration Guide</i> , Release 12.4T http://www.cisco.com/en/US/customer/products/ps6441/products_configuration_guide_book09186a008049e22f.html
Cisco IOS Optimized Edge Routing Command Reference	<i>Cisco IOS Optimized Edge Routing Command Reference</i> , Release 12.4T http://www.cisco.com/en/US/customer/products/ps6441/products_command_reference_book09186a008049704
Cisco IOS Security Configuration Guide	<i>Cisco IOS Security Configuration Guide</i> , Release 12.4 http://www.cisco.com/en/US/customer/products/ps6350/products_configuration_guide_book09186a008043360a.html
Cisco IOS Security Command Reference	<i>Cisco IOS Security Command Reference</i> , Release 12.4T http://www.cisco.com/en/US/partner/products/ps6441/products_command_reference_book09186a0080497056.html
Extensible Markup Language (XML)	<i>Extensible Markup Language (XML) 1.0 (Third Edition)</i> http://www.w3.org/TR/REC-xml/
Threat Information Distribution Protocol	<i>Threat Information Distribution Protocol</i> http://www.cisco.com/en/US/customer/products/ps6441/products_feature_guide09186a00805e2380.html

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB gateways, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features

- **acl drop**
- **class-map type mitigation**
- **class-map type tms**
- **clear tms consumer group**
- **controller (TMS)**
- **debug tms consumer**
- **debug tms controller**
- **exception access-group**
- **heartbeat retry count**
- **heartbeat retry interval**
- **identifier**
- **ignore (TMS)**
- **logging tms events**
- **match primitive**
- **match priority**
- **match tidp-group**
- **message retry count**
- **message retry interval**
- **mitigation**
- **parameter-map type mitigation**
- **parameter-map type tms**
- **policy-map type control mitigation**
- **policy-map type control tms**
- **redirect route**
- **registration retry count**
- **registration retry interval**
- **show tms consumer**
- **show tms consumer group**
- **show tms controller**
- **show tms controller group**
- **service-policy type tms**
- **source parameter**
- **tms consumer**
- **tms consumer deregister**
- **tms consumer register**

- **tms consumer resync**
- **tms controller**
- **tms controller deregister**
- **tms controller load threat**
- **tms controller reset**
- **tms controller send**
- **tms controller status**
- **tms controller unload**
- **tms-class**
- **variable**

For information about these commands, see the Cisco IOS Security Command Reference at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

Feature Information for TMS

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for TMS

TIDP Based Mitigation Services	12.4(6)T	TMS was introduced. TMS provides the framework to rapidly and efficiently distribute threat information to devices across the network. The TMS framework transports messages that contain specific threat information about suspect traffic and associated mitigation enforcement actions to all devices in the network.
--------------------------------	----------	--

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Tag and Template

First Published: February 27, 2006

Last Updated: February 27, 2006

The Tag and Template feature allows network administrators to define enforcement policies on a local device and have a RADIUS server specify the policy selector to be enforced. This feature can be applied to a Network Admission Control (NAC) architecture.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Tag and Template](#)” section on page 11.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Tag and Template, page 2](#)
- [Requirements for Tag and Template, page 2](#)
- [Information About Tag and Template, page 2](#)
- [How to Configure Tag and Template, page 2](#)
- [Configuration Examples for Tag and Template, page 8](#)
- [Where to Go Next, page 9](#)
- [Additional References, page 9](#)
- [Command Reference, page 10](#)
- [Feature Information for Tag and Template, page 11](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for Tag and Template

- You must have a Cisco IOS image that supports the Modular Quality of Service (QoS) command-line interface (CLI).

Requirements for Tag and Template

- To apply the enforcement policies, the identity policy and access groups that are associated with the identity policy have to be configured for Tag and Template.

Information About Tag and Template

Before configuring Tag and Template, you should understand the following concepts:

- [Tag and Template Overview, page 2](#)

Tag and Template Overview

In a typical Network Admission Control deployment, an access control server (ACS) or a RADIUS server is used for validating the user posture information and for applying the policies on the network access device (NAD). A centralized ACS can be used to support multiple NADs. This solution has inherent problems associated with it, namely:

- Version control of policies. Typically, a specific NAD that is running a Cisco IOS image may support some ACLs, and another NAD may support a different version. Managing different versions can be a problem.
- Users connect on different interfaces to the NAD, and on the basis of the interface type, the policies that can be applied to the user can change, and the NAD can determine the policies to be applied. In the current architecture, the ACS sends the same set of policies to all the NADs when a profile is matched, which does not give enough control to the administrator to configure the policies on the basis of the NAD configuration.

To overcome the above problems, the Tag and Template concept has been introduced. The concept is that the ACS maps users to specific groups and associates a tag with them. For example, the Usergroup1 user group may have a tag with the name “usergroup1.” When the NAD queries the ACS for the policies, the ACS can return the tag that is associated with the user group. When this tag is received at the NAD, the NAD can map the tag to a specific template that can have a set of policies that are associated with the user group. This mapping provides administrators with the flexibility to configure the template on a NAD basis, and the policies can change from NAD to NAD even though the tag is the same.

In summary, a template must be configured on the NAD, and the template must be associated with a tag. When the ACS sends the policies back to the NAD, the template that matches the tag that was received from the ACS is used.

How to Configure Tag and Template

This section includes the following procedures:

- [Defining a Class Map for a Specific Type and Associating Match Conditions with It, page 3](#)

- [Associating the Class Map with the Policy Map and Applying Actions for Classes That Match, page 4](#)
- [Associating the Service Policy with a Specific IP Admission Rule, page 5](#)
- [Monitoring the Template Configuration, page 6](#)
- [Verifying the Template Configuration, page 7](#)

Defining a Class Map for a Specific Type and Associating Match Conditions with It

To define a class map and associate match conditions with it, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type tag [match-all | match-any] *class-map-name***
4. **match port-type {routed | switched}**
5. **match tag *tag-name***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	class-map type tag [match-all match-any] <i>class-map-name</i> Example: Router (config)# class-map tag match-all group1_class	Creates a class map to be used for matching packets to a specified class and enters class-map configuration mode.
Step 4	match port-type {routed switched} Example: Router (config-cmap)# match port-type routed	Matches the access policy on the basis of the port for a class map.
Step 5	match tag tag-name Example: Router (config-cmap)# match tag group1_class	Specifies the tag to be matched for a tag type of class map.

What to Do Next

Associate the class map with the policy map and apply actions for classes that match.

Associating the Class Map with the Policy Map and Applying Actions for Classes That Match

To associate the class map with the policy map and apply actions for classes that match, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control tag policy-map-name**
4. **class type tag {class-name} [insert-before {class-name}]**
5. **identity policy policy-name**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy-map type control tag <i>policy-map-name</i> Example: Router (config)# policy-map type control tag usergroup1_pmap	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy and enters policy-map configuration mode.
Step 4	class type tag { <i>class-name</i> } [insert-before { <i>class-name</i> }] Example: Router (config-pmap)# class type tag usergroup1_class	Associates a class map with a policy map.
Step 5	identity policy <i>policy-name</i> Example: Router (config-pmap)# identity policy usergroup1_iden_policy	Associates an identity policy with the class map.

What to Do Next

Associate the service policy with a specific IP admission table.

Associating the Service Policy with a Specific IP Admission Rule

The policy map defined above can be associated with an IP authentication proxy or IP admission rule. To associate the map with the IP authentication proxy or IP admission rule, perform the following steps.



Note

There can be multiple policy maps, and each one can be associated with a different IP admission rule even though an IP admission rule can have only one instance of the policy map.

SUMMARY STEPS

- enable**
- configure terminal**
- ip admission name** *admission-name* [**eapoudp** | **proxy** {**ftp** | **http** | **telnet**} | **service-policy type tag** {*service-policy-name*}] [**list** {*acl* | *acl-name*}]

or

```
ip auth-proxy name auth-proxy-name {ftp | http | telnet} [inactivity-timer min] [absolute-timer min] [list {acl | acl-name}] [service-policy type tag {service-policy-name} ]
```

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	<pre>ip admission name <i>admission-name</i> [eapoudp proxy {ftp http telnet} service-policy type tag {<i>service-policy-name</i>}] [list {<i>acl</i> <i>acl-name</i>}]</pre> <p>or</p> <pre>ip auth-proxy name <i>auth-proxy-name</i> {ftp http telnet} [inactivity-timer <i>min</i>] [absolute-timer <i>min</i>] [list {<i>acl</i> <i>acl-name</i>}] [service-policy type tag {<i>service-policy-name</i>}]</pre> Example: Router (config)# ip admission name nac eapoudp service-policy type tag usergroup1_iden_policy or Router (config)# ip auth-proxy name nac eapoudp service-policy type tag usergroup1_iden_policy	Associates the policy map with an IP network admission control rule. <ul style="list-style-type: none"> The service policy name must be the same as the policy map name. <p>or</p> Associates the policy map with an authentication proxy rule.

Monitoring the Template Configuration

To monitor the template configuration, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **debug tag-template event**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
	Example: Router> enable	
Step 2	debug tag-template event	Displays the tag application on a session (an Authentication Proxy or Extensible Authentication Protocol over UDP [EAPoUDP] session).
	Example: Router# debug tag-template event	

Verifying the Template Configuration

To verify the template configuration, perform the following steps. The **show** commands can be used individually or together.

SUMMARY STEPS

1. **enable**
2. **show class-map type tag** *class-map-name*
3. **show epm session ip** { *ip-address* | **summary** }
4. **show policy-map type control tag** *type-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show class-map type tag class-map-name Example: Router# show class-map type tag map1	Displays all class maps and their matching criteria.
Step 3	show epm session ip {ip-address summary} Example: Router# show epm session ip 10.1.1.1	Displays whether tag policies or authentication, authorization, and accounting (AAA) policies are actually applied to a service policy application.
Step 4	show policy-map type control tag type-name Example: Router# show policy-map type control tag type1	Displays a template configuration when applying access policies on Layer 2 and Layer 3 interfaces.

Configuration Examples for Tag and Template

This section provides the following configuration example.

- [Typical Tag and Template Configuration: Example, page 8](#)

Typical Tag and Template Configuration: Example

In the following service policy (Tag and Template) example, tags named “healthy” and “non_healthy” can be received from an AAA server, the policy map is defined on the NAD, and the tag policy type is associated with the IP admission name “greentree.”

Class Map Definition for the “healthy class” Type Tag

```
Router (config)# class-map type tag healthy_class
Router(config-cmap)# match tag healthy
Router(config-cmap)# end
```

Class Map Definition for the “non_healthy_class” Type Tag

```
Router (config)# class-map type tag non_healthy_class
Router (config-cmap)# match tag non_healthy
Router (config-cmap)# end
```

Policy Map Is Defined

```
! The following line will be associated with the IP admission name.
Router (config)# policy-map type control tag global_class
! The following line refers to the class map that was defined above.
Router (config-pmap)# class healthy_class
Router (config-pmap-c)# identity policy healthy_policy
Router(config-pmap-c)# exit
```

The following line refers to the `non_healthy` class that was defined above.

```
Router (config-pmap)# class non_healthy_class
Router (config-pmap-c)# identity policy non_healthy_policy
Router (config-pmap-c)# end
```

Identity Policy Can Be Defined As Follows

```
Router (config)# identity policy healthy_policy
! The following line is the IP access list for healthy users.
Router (config-identity-policy)# access-group healthy
Router (config-identity-policy)# end
Router (config)# identity policy non_healthy_policy
Router (config-identity-policy)# access-group non_healthy
Router (config-identity-policy)# end
```

Access Lists Can Be Defined As Follows

```
Router (config)# ip access-list extended healthy_class
! The following line can be anything, but as an example, traffic is being allowed.
Router (config-ext-nacl)# permit ip any any
Router (config-ext-nacl)# end
Router (config)# ip access-list extended non_healthy_class
! The following line is only an example. In practical cases, you could prevent a user from
accessing specific networks.
Router (config-ext-nacl)# deny ip any any
Router (config-ext-nacl)# end
```

Policy Map That Was Defined Above Is Associated with the IP Admission Name

```
Router (config)# ip admission name greentree service-policy type tag global_class
! In the next line, the admission name can be associated with the interface.
Router (config)# interface fastethernet 1/0
Router (config-if)# ip admission greentree
```

In the above configuration, if the AAA server sends a tag named "healthy" or "non_healthy" for any host, the policies that are associated with the appropriate identity policy will be applied on the host.

Where to Go Next

The tag attribute must be configured in the RADIUS profile using the following Cisco attribute-value (AV) pair: `tag-name={tag string}`.

For information about configuring RADIUS AV pairs, see the subsection "Configuring Cisco AV Pairs" in the section "[Related Documents](#)."

Additional References

The following sections provide references related to Tag and Template.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List , Release 12.4T
Configuring Cisco RADIUS AV pairs	The section “ Configuring RADIUS ” in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4

Standards

Standard	Title
No new or modified standards are supported by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **class-map**
- **class type tag**
- **debug tag-template event**
- **identity policy (policy-map)**
- **ip admission name**
- **ip auth-proxy name**
- **match port-type**
- **match tag (class-map)**
- **policy-map**
- **show class-map**
- **show epm session ip**
- **show policy-map**

Feature Information for Tag and Template

[Table 1](#) lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Note

[Table 1](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 **Feature Information for Tag and Template**

Feature Name	Releases	Feature Information
Tag and Template	12.4(6)T	<p>The Tag and Template feature allows network administrators to define enforcement policies on a local device and have a RADIUS server specify the policy selector to be enforced. This feature can be applied to a Network Admission Control (NAC) architecture.</p> <p>The following commands were introduced or modified by this feature: class-map, class type, debug tag-template event, identity policy (policy-map), ip admission name, ip auth-proxy name, match port-type, match tag (class-map), show class-map, and show policy-map type.</p>

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Secure Infrastructure



AutoSecure

By using a single command-line interface (CLI), the AutoSecure feature allows a user to perform the following functions:

- Disable common IP services that can be exploited for network attacks
- Enable IP services and features that can aid in the defense of a network when under attack.

This feature also simplifies the security configuration of a router and hardens the router configuration.

Feature History for AutoSecure

Release	Modification
12.3(1)	This feature was introduced.
12.2(18)S	This feature was integrated into Cisco IOS Release 12.2(18)S.
12.3(8)T	Support for the roll-back functionality and system logging messages were added to Cisco IOS Release 12.3(8)T.
12.2(27)SBC	This feature was integrated into Cisco IOS Release 12.(27)SBC.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Information About AutoSecure, page 2](#)
- [How to Configure AutoSecure, page 6](#)
- [Configuration Examples for AutoSecure, page 9](#)
- [Additional References, page 13](#)
- [Command Reference, page 14](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Information About AutoSecure

To configure the AutoSecure feature, you should understand the following concepts:

- [Benefits of AutoSecure, page 2](#)
- [Secure Management Plane, page 3](#)
- [Secure Forwarding Plane, page 5](#)

Benefits of AutoSecure

Simplified Router Security Configuration

AutoSecure is valuable to customers without special Security Operations Applications because it allows them to quickly secure their network without thorough knowledge of all the Cisco IOS features.

This feature eliminates the complexity of securing a router by creating a new CLI that automates the configuration of security features and disables certain features enabled by default that could be exploited for security holes.

Enhanced Password Security

AutoSecure provides the following mechanisms to enhance security access to the router:

- The ability to configure a required minimum password length, which can eliminate common passwords that are prevalent on most networks, such as “lab” and “cisco.”

To configure a minimum password length, use the [security passwords min-length](#) command.

- Syslog messages are generated after the number of unsuccessful attempts exceeds the configured threshold.

To configure the number of allowable unsuccessful login attempts (the threshold rate), use the [security passwords min-length](#) command.

Roll-Back and System Logging Message Support

In Cisco IOS Release 12.3(8)T, support for roll-back of the AutoSecure configuration is introduced. Roll-back enables a router to revert back to its preautosecure configuration state if the AutoSecure configuration fails.



Note

Prior to Cisco IOS Release 12.3(8)T, roll-back of the AutoSecure configuration is unavailable; thus, you should always save the running configuration before configuring AutoSecure.

System Logging Messages capture any changes or tampering of the AutoSecure configuration that were applied on the running configuration. That is, more detailed audit trail information is provided when autosecure is executed.

Secure Management Plane

Securing the management plane is one of two focus areas for the AutoSecure feature. (The other focus area is described in the following section, “[Secure Forwarding Plane](#).”) Securing the management plane is done by turning off certain global and interface services that can be potentially exploited for security attacks and turning on global services that help mitigate the threat of attacks. Secure access and secure logging are also configured for the router.

**Caution**

If your device is managed by a network management (NM) application, securing the management plane could turn off some services like HTTP server and disrupt the NM application support.

The following subsections define how AutoSecure helps to secure the management plane:

- [Disable Global Services](#)
- [Disable Per Interface Services](#)
- [Enable Global Services](#)
- [Secure Access to the Router](#)
- [Log for Security](#)

Disable Global Services

After enabling this feature (via the [auto secure](#) command), the following global services will be disabled on the router without prompting the user:

- Finger—Collects information about the system (reconnaissance) before an attack. If enabled, the information can leave your device vulnerable to attacks.
- PAD—Enables all packet assembler and disassembler (PAD) commands and connections between PAD devices and access servers. If enabled, it can leave your device vulnerable to attacks.
- Small Servers—Causes TCP and User Datagram Protocol (UDP) diagnostic port attacks: a sender transmits a volume of fake requests for UDP diagnostic services on the router, consuming all CPU resources.
- Bootp Server—Bootp is an insecure protocol that can be exploited for an attack.
- HTTP Server—Without secure-http or authentication embedded in the HTTP server with an associated ACL, the HTTP server is insecure and can be exploited for an attack. (If you must enable the HTTP server, you will be prompted for the proper authentication or access list.)

**Note**

If you are using Security Device Manager (SDM), you must manually enable the HTTP server via the **ip http server** command.

- Identification Service—An unsecure protocol, defined in RFC 1413, that allows one to query a TCP port for identification. An attacker can access private information about the user from the ID server.
- CDP—If a large number of Cisco Discovery Protocol (CDP) packets are sent to the router, the available memory of the router can be consumed, causing the router to crash.

**Caution**

NM applications that use CDP to discover network topology will not be able to perform discovery.

- **NTP**—Without authentication or access-control, Network Time Protocol (NTP) is insecure and can be used by an attacker to send NTP packets to crash or overload the router. (If you want to turn on NTP, you must configure NTP authentication using Message Digest 5 (MD5) and the **ntp access-group** command. If NTP is enabled globally, disable it on all interfaces on which it is not needed.)
- **Source Routing**—Provided only for debugging purposes, so source routing should be disabled in all other cases. Otherwise, packets may slip away from some of the access control mechanisms that they should have gone through.

Disable Per Interface Services

After enabling this feature, the following per interface services will be disabled on the router without prompting the user:

- **ICMP redirects**—Disabled on all interfaces. Does not add a useful functionality to a correctly configured to network, but it could be used by attackers to exploit security holes.
- **ICMP unreachable**s—Disabled on all interfaces. Internet Control Management Protocol (ICMP) unreachable are a known cause for some ICMP-based denial of service (DoS) attacks.
- **ICMP mask reply** messages—Disabled on all interfaces. ICMP mask reply messages can give an attacker the subnet mask for a particular subnetwork in the internetwork.
- **Proxy-Arp**—Disabled on all interfaces. Proxy-Arp requests are a known cause for DoS attacks because the available bandwidth and resources of the router can be consumed in an attempt to respond to the repeated requests that are sent by an attacker.
- **Directed Broadcast**—Disabled on all interfaces. Potential cause of SMURF attacks for DoS.
- **Maintenance Operations Protocol (MOP) service**—Disabled on all interfaces.

Enable Global Services

After enabling this feature, the following global services will be enabled on the router without prompting the user:

- The **service password-encryption** command—Prevents passwords from being visible in the configuration.
- The **service tcp-keepalives-in** and **service tcp-keepalives-out** commands—Ensures that abnormally terminated TCP sessions are removed.

Secure Access to the Router



Caution

If your device is managed by an NM application, securing access to the router could turn off vital services and may disrupt the NM application support.

After enabling this feature, the following options in which to secure access to the router are available to the user:

- If a text banner does not exist, users will be prompted to add a banner. This feature provides the following sample banner:

Authorized access only

```
This system is the property of ABC Enterprise
Disconnect IMMEDIATELY if you are not an authorized user!
Contact abc@xyz.com +99 876 543210 for help.
```

- The login and password (preferably a secret password, if supported) are configured on the console, AUX, vty, and tty lines. The **transport input** and **transport output** commands are also configured on all of these lines. (Telnet and secure shell (SSH) are the only valid transport methods.) The **exec-timeout** command is configured on the console and AUX as 10.
- When the image on the device is a crypto image, AutoSecure enables SSH and secure copy (SCP) for access and file transfer to and from the router. The **timeout seconds** and **authentication-retries integer** options for the **ip ssh** command are configured to a minimum number. (Telnet and FTP are not affected by this operation and remain operational.)
- If the AutoSecure user specifies that their device does not use Simple Network Management Protocol (SNMP), one of the following functionalities will occur:
 - In interactive mode, the user is asked whether to disable SNMP regardless of the values of the community strings, which act like passwords to regulate access to the agent on the router.
 - In non-interact mode, SNMP will be disabled if the community string is “public” or “private.”

**Note**

After AutoSecure has been enabled, tools that use SNMP to monitor or configure a device will be unable to communicate with the device via SNMP.

- If authentication, authorization, and accounting (AAA) is not configured, configure local AAA. AutoSecure will prompt users to configure a local username and password on the router.

Log for Security

After this feature is enabled, the following logging options, which allow you to identify and respond to security incidents, are available:

- Sequence numbers and time stamps for all debug and log messages. This option is useful when auditing logging messages.
- Logging messages can be generated for login-related events; for example, the message “Blocking Period when Login Attack Detected” will be displayed when a login attack is detected and the router enters “quiet mode.” (Quiet mode means that the router will not allow any login attempts via Telnet, HTTP, or SSH.)

For more information on login system messages, see the Cisco IOS Release 12.3(4)T feature module *Cisco IOS Login Enhancements*.

- The **logging console critical** command, which sends system logging (syslog) messages to all available TTY lines and limits messages based on severity.
- The **logging buffered** command, which copies logging messages to an internal buffer and limits messages logged to the buffer based on severity.
- The **logging trap debugging** command, which allows all commands with a severity higher than debugging to be sent to the logging server.

Secure Forwarding Plane

To minimize the risk of attacks on the router forward plane, AutoSecure provides the following functions:

- Cisco Express Forwarding (CEF)—AutoSecure enables CEF or distributed CEF (dCEF) on the router whenever possible. Because there is no need to build cache entries when traffic starts arriving for new destinations, CEF behaves more predictably than other modes when presented with large volumes of traffic addressed to many destinations. Thus, routers configured for CEF perform better under SYN attacks than routers using the traditional cache.



Note CEF consumes more memory than a traditional cache.

- If the TCP intercept feature is available, it can be configured on the router for connection timeout.
- If strict Unicast Reverse Path Forwarding (uRPF) is available, it can be configured on the router to help mitigate problems that are caused by the introduction of forged (spoofed) IP source addresses. uRPF discards IP packets that lack a verifiable IP source address.
- If the router is being used as a firewall, it can be configured for context-based access control (CBAC) on public interfaces that are facing the Internet.



Note At the beginning of the AutoSecure dialogue, you will be prompted for a list of public interfaces.

How to Configure AutoSecure

This section contains the following procedures:

- [Configuring AutoSecure, page 6](#) (required)
- [Configuring Additional Security, page 7](#) (required)
- [Verifying AutoSecure, page 8](#) (optional)

Configuring AutoSecure

To configure AutoSecure, you must perform the following tasks.

The auto secure Command

The **auto secure** command takes you through a semi-interactive session (also known as the AutoSecure dialogue) to secure the management and forwarding planes. This command gives you the option to secure just the management or the forwarding plane; if neither option is selected, the dialogue will ask you to configure both planes.

This command also allows you to go through all noninteractive configuration portions of the dialogue before the interactive portions. The noninteractive portions of the dialogue can be enabled by selecting the optional **no-interact** keyword.



Caution

Although the **auto secure** command helps to secure a router, it does not guarantee the complete security of the router.

Restrictions

The AutoSecure configuration can be configured at run time or setup time. If any related configuration is modified after AutoSecure has been enabled, the AutoSecure configuration may not be fully effective.

SUMMARY STEPS

1. **enable**
2. **auto secure** [**management** | **forwarding**] [**no-interact** | **full**] [**ntp** | **login** | **ssh** | **firewall** | **tcp-intercept**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	auto secure [management forwarding] [no-interact full] [ntp login ssh firewall tcp-intercept] Example: Router# auto secure	Secures the management and forwarding planes of the router. <ul style="list-style-type: none"> • management—Only the management plane will be secured. • forwarding—Only the forwarding plane will be secured. • no-interact—The user will not be prompted for any interactive configurations. • full—The user will be prompted for all interactive questions. This is the default.

Configuring Additional Security

To enable enhanced security access to your router, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **security passwords min-length** *length*
4. **enable password** {*password* | [*encryption-type*] *encrypted-password*}
5. **security authentication failure rate** *threshold-rate* **log**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	security passwords min-length length Example: Router(config)# security passwords min-length 6	Ensures that all configured passwords are at least a specified length. <ul style="list-style-type: none"> <i>length</i>—Minimum length of a configured password.
Step 4	enable password {password [encryption-type] encrypted-password} Example: Router(config)# enable password elephant	Sets a local password to control access to various privilege levels.
Step 5	security authentication failure rate threshold-rate log Example: Router(config)# security authentication failure rate 10 log	Configures the number of allowable unsuccessful login attempts. <ul style="list-style-type: none"> <i>threshold-rate</i>—Number of allowable unsuccessful login attempts. log—Syslog authentication failures if the rate exceeds the threshold.

Verifying AutoSecure

To verify that the AutoSecure feature is working successfully, perform the following optional steps:

SUMMARY STEPS

1. **enable**
2. **show auto secure config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables higher privilege levels, such as privileged EXEC mode.
	Example: Router> enable	Enter your password if prompted.
Step 2	show auto secure config	(Optional) Displays all configuration commands that have been added as part of the AutoSecure configuration.
	Example: Router# show auto secure config	

Configuration Examples for AutoSecure

This section provides the following configuration example:

- [AutoSecure Configuration Dialogue: Example, page 9](#)

AutoSecure Configuration Dialogue: Example

The following example is a sample AutoSecure dialogue. After you enable the **auto secure** command, the feature will automatically prompt you with a similar dialogue unless you enable the **no-interact** keyword. (For information on which features are disabled and which features are enabled, see the sections, “[Secure Management Plane](#)” and “[Secure Forwarding Plane](#)” earlier in this document.)

```
Router# auto secure
--- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of the router but it will not make
router absolutely secure from all security attacks ***

All the configuration done as part of AutoSecure will be shown here. For more details of
why and how this configuration is useful, and any possible side effects, please refer to
Cisco documentation of AutoSecure.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]:y
Enter the number of interfaces facing internet [1]:
Interface                IP-Address OK? Method Status
Protocol
FastEthernet0/1          10.1.1.1   YES NVRAM   up down

FastEthernet1/0          10.2.2.2   YES NVRAM   up down

FastEthernet1/1          10.0.0.1   YES NVRAM   up up

Loopback0                unassigned YES NVRAM   up up

FastEthernet0/0          10.0.0.2   YES NVRAM   up down

Enter the interface name that is facing internet:FastEthernet0/0
```

```

Securing Management plane services..

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp
Enable secret is either not configured or is same as enable password
Enter the new enable secret:abc123
Configuring aaa local authentication
Configuring console, Aux and vty lines for
local authentication, exec-timeout, transport

Configure SSH server? [yes]:
Enter the domain-name:cisco.com

Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:

no ip redirects
no ip proxy-arp
no ip unreachable
no ip directed-broadcast
no ip mask-reply
Disabling mop on Ethernet interfaces

Securing Forwarding plane services..

Enabling CEF (it might have more memory requirements on some low end
platforms)

Enabling unicast rpf on all interfaces connected to internet

Configure CBAC Firewall feature? [yes/no]:yes

This is the configuration generated:

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
security passwords min-length 6
security authentication failure rate 10 log
enable secret 5 $1$CZ6G$GkGONHdNJCO3CjNHHyTUA.
aaa new-model

```

```
aaa authentication login local_auth local
line console 0
  login authentication local_auth
  exec-timeout 5 0
  transport output telnet
line aux 0
  login authentication local_auth
  exec-timeout 10 0
  transport output telnet
line vty 0 4
  login authentication local_auth
  transport input telnet
ip domain-name cisco.com
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
  transport input ssh telnet
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
int FastEthernet0/1
  no ip redirects
  no ip proxy-arp
  no ip unreachable
  no ip directed-broadcast
  no ip mask-reply
  no mop enabled
int FastEthernet1/0
  no ip redirects
  no ip proxy-arp
  no ip unreachable
  no ip directed-broadcast
  no ip mask-reply
  no mop enabled
int FastEthernet1/1
  no ip redirects
  no ip proxy-arp
  no ip unreachable
  no ip directed-broadcast
  no ip mask-reply
  no mop enabled
int FastEthernet0/0
  no ip redirects
  no ip proxy-arp
  no ip unreachable
  no ip directed-broadcast
  no ip mask-reply
  no mop enabled
ip cef

interface FastEthernet0/0
  ip verify unicast reverse-path
ip inspect audit-trail
ip inspect dns-timeout 7
ip inspect tcp idle-time 14400
ip inspect udp idle-time 1800
ip inspect name autosec_inspect cuseeme timeout 3600
ip inspect name autosec_inspect ftp timeout 3600
ip inspect name autosec_inspect http timeout 3600
```



```
ip inspect name autosec_inspect rcmd timeout 3600
ip inspect name autosec_inspect realaudio timeout 3600
ip inspect name autosec_inspect smtp timeout 3600
ip inspect name autosec_inspect tftp timeout 30
ip inspect name autosec_inspect udp timeout 15
ip inspect name autosec_inspect tcp timeout 3600
access-list 100 deny ip any any
interface FastEthernet0/0
  ip inspect autosec_inspect out
  ip access-group 100 in
!
end
```

Apply this configuration to running-config? [yes]:yes

Applying the config generated to running-config
The name for the keys will be:ios210.cisco.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys ...[OK]

Router#

Additional References

The following sections provide references related to AutoSecure.

Related Documents

Related Topic	Document Title
Login functionality (such as login delays and login blocking periods)	<i>Cisco IOS Login Enhancements</i> , Cisco IOS Release 12.3(4)T feature module
Additional information regarding router configuration	<i>Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.3T</i>
Additional router configuration commands	<i>Cisco IOS Configuration Fundamentals Command Reference, Release 12.3T</i>

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 1918	Address Allocation for Private Internets
RFC 2267	<i>Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing</i>

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **auto secure**
- **security passwords min-length**
- **show auto secure config**

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Cisco IOS Login Enhancements (Login Block)

Document First Published: August 2005

Last Updated: October 2007

The Cisco IOS Login Enhancements (Login Block) feature allows users to enhance the security of a router by configuring options to automatically block further login attempts when a possible denial-of-service (DoS) attack is detected.

The login block and login delay options introduced by this feature can be configured for Telnet or SSH virtual connections. By enabling this feature, you can slow down “dictionary attacks” by enforcing a “quiet period” if multiple failed connection attempts are detected, thereby protecting the routing device from a type of denial-of-service attack.

Feature History for Cisco IOS Login Enhancements

Release	Modification
12.3(4)T	This feature was introduced.
12.2(25)S	This feature was integrated into Cisco IOS Release 12.2 S.
12.2(33)SRA	This feature was integrated into Cisco IOS Release 12.2 SR.
12.2(33)SRB, 12.2(33)SXH, 12.4(15)T1	Support for HTTP login blocking was added.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Information About Cisco IOS Login Enhancements, page 2](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [How to Configure Cisco IOS Login Enhancements, page 4](#)
- [Configuration Examples for Login Parameters, page 7](#)
- [Additional References, page 8](#)
- [Command Reference, page 9](#)

Information About Cisco IOS Login Enhancements

To use login enhancements, you should understand the following concepts:

- [Protecting Against Denial of Service and Dictionary Login Attacks](#)
- [Login Enhancements Functionality Overview, page 3](#)

Protecting Against Denial of Service and Dictionary Login Attacks

Connecting to a routing device for the purposes of administering (managing) the device, at either the User or Executive level, is most frequently performed using Telnet or SSH (secure shell) from a remote console (such as a PC). SSH provides a more secure connection option because communication traffic between the user's device and the managed device are encrypted. The Login Block capability, when enabled, applies to both Telnet connections and SSH connections. Beginning in Release versions 12.3(33)SRB2, 12.2(33)SXH2, and 12.4(15)T1, the Login Block capability also applies to HTTP connections."

The automated activation and logging of the Login Block and Quiet Period capabilities introduced by this feature are designed to further enhance the security of your devices by specifically addressing two well known methods that individuals use to attempt to disrupt or compromise networked devices.

If the connection address of a device is discovered and is reachable, a malicious user may attempt to interfere with the normal operations of the device by flooding it with connection requests. This type of attack is referred to as an attempted Denial-of-Service, because it is possible that the device may become too busy trying to process the repeated login connection attempts to properly handle normal routing services or will not be able to provide the normal login service to legitimate system administrators.

The primary intention of a dictionary attack, unlike a typical DoS attack, is to actually gain administrative access to the device. A dictionary attack is an automated process to attempt to login by attempting thousands, or even millions, of username/password combinations. (This type of attack is called a "dictionary attack" because it typically uses, as a start, every word found in a typical dictionary as a possible password.) As scripts or programs are used to attempt this access, the profile for such attempts is typically the same as for DoS attempts; multiple login attempts in a short period of time.

By enabling a detection profile, the routing device can be configured to react to repeated failed login attempts by refusing further connection request (login blocking). This block can be configured for a period of time, called a "quiet period". Legitimate connection attempts can still be permitted during a quiet period by configuring an access-list (ACL) with the addresses that you know to be associated with system administrators.

Login Enhancements Functionality Overview

To better configure security for virtual login connections, the following requirements have been added to the login process:

- [Delays Between Successive Login Attempts](#)
- [Login Shutdown If DoS Attacks Are Suspected](#)
- [Generation of System Logging Messages for Login Detection](#)

Delays Between Successive Login Attempts

A Cisco IOS device can accept virtual connections as fast as they can be processed. Introducing a delay between login attempts helps to protect the Cisco IOS software-based device against malicious login connections such as dictionary attacks and DoS attacks. Delays can be enabled in one of the following ways:

- Via the **auto secure** command. If you enable the AutoSecure feature, the default login delay time of one second is automatically enforced.
- Via the **login block-for** command. You must enter this command before issuing the **login delay** command. If you enter only the **login block-for** command, the default login delay time of one second is automatically enforced.
- Via the new global configuration mode command, **login delay**, which allows you to specify a the login delay time to be enforced, in seconds.

Login Shutdown If DoS Attacks Are Suspected

If the configured number of connection attempts fail within a specified time period, the Cisco IOS device will not accept any additional connections for a “quiet period.” (Hosts that are permitted by a predefined access-control list [ACL] are excluded from the quiet period.)

The number of failed connection attempts that trigger the quiet period can be specified via the new global configuration mode command **login block-for**. The predefined ACL that is excluded from the quiet period can be specified via the new global configuration mode command **login quiet-mode access-class**.

This functionality is disabled by default, and it is not enabled if autosecure is enabled.

Generation of System Logging Messages for Login Detection

After the router switches to and from quiet mode, logging messages are generated. Also, if configured, logging messages are generated upon every successful or failed login request.

Logging messages can be generated for successful login requests via the new global configuration command **login on-success**; the **login on-failure** command generates logs for failed login requests.

Logging messages for failed login attempts are automatically enabled when the **auto secure** command is issued; they are not automatically enabled for successful login attempts via autosecure.



Note

Currently, only system logging (syslog) messages can be generated for login-related events. Support for SNMP notifications (traps) will be added in a later release.

System Logging Messages for a Quiet Period

The following logging message is generated after the router switches to quiet-mode:

```
00:04:07:%SEC_LOGIN-1-QUIET_MODE_ON:Still timeleft for watching failures is 158 seconds,
[user:sfd] [Source:10.4.2.11] [localport:23] [Reason:Invalid login], [ACL:22] at 16:17:23
UTC Wed Feb 26 2003
```

The following logging message is generated after the router switches from quiet mode back to normal mode:

```
00:09:07:%SEC_LOGIN-5-QUIET_MODE_OFF:Quiet Mode is OFF, because block period timed out at
16:22:23 UTC Wed Feb 26 2003
```

System Logging Messages for Successful and Failed Login Requests

The following logging message is generated upon a successful login request:

```
00:04:32:%SEC_LOGIN-5-LOGIN_SUCCESS>Login Success [user:test] [Source:10.4.2.11]
[localport:23] at 20:55:40 UTC Fri Feb 28 2003
```

The following logging message is generated upon a failed login request:

```
00:03:34:%SEC_LOGIN-4-LOGIN_FAILED>Login failed [user:sdfs] [Source:10.4.2.11]
[localport:23] [Reason:Invalid login] at 20:54:42 UTC Fri Feb 28 2003
```

How to Configure Cisco IOS Login Enhancements

This section contains the following procedures:

- [Configuring Login Parameters, page 4](#) (Required)
- [Verifying Login Parameters, page 6](#) (Optional)

Configuring Login Parameters

Use this task to configure your Cisco IOS device for login parameters that help detect suspected DoS attacks and slow down dictionary attacks.

Login Parameter Defaults

All login parameters are disabled by default. You must issue the **login block-for** command, which enables default login functionality, before using any other login commands. After the **login block-for** command is enabled, the following defaults are enforced:

- A default login delay of one second
- All login attempts made via Telnet or SSH are denied during the quiet period; that is, no ACLs are exempt from the login period until the **login quiet-mode access-class** command is issued.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **login block-for** *seconds* **attempts** *tries* **within** *seconds*
4. **login quiet-mode access-class** {*acl-name* | *acl-number*}

5. **login delay** *seconds*
6. **login on-failure log** [**every** *login*]
7. **login on-success log** [**every** *login*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	login block-for <i>seconds</i> attempts <i>tries</i> within <i>seconds</i> Example: Router(config)# login block-for 100 attempts 2 within 100	Configures your Cisco IOS device for login parameters that help provide DoS detection. Note This command must be issued before any other login command can be used.
Step 4	login quiet-mode access-class { <i>acl-name</i> <i>acl-number</i> } Example: Router(config)# login quiet-mode access-class myacl	(Optional) Specifies an ACL that is to be applied to the router when it switches to quiet mode. If this command is not enabled, all login requests will be denied during quiet mode.
Step 5	login delay <i>seconds</i> Example: Router(config)# login delay 10	(Optional) Configures a delay between successive login attempts.
Step 6	login on-failure log [every <i>login</i>] Example: Router(config)# login on-failure log	(Optional) Generates logging messages for failed login attempts.
Step 7	login on-success log [every <i>login</i>] Example: Router(config)# login on-success log every 5	(Optional) Generates logging messages for successful login attempts.

What to Do Next

After you have configured login parameters on your router, you may wish to verify the settings. To complete this task, see the following section “[Verifying Login Parameters](#).”

Verifying Login Parameters

Use this task to verify the applied login configuration and present login status on your router.

SUMMARY STEPS

- 1. enable
- 2. show login [failures]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	show login [failures] Example: Router# show login	Displays login parameters. <ul style="list-style-type: none">• failures—Displays information related only to failed login attempts.

Examples

The following sample output from the **show login** command verifies that no login parameters have been specified:

```
Router# show login

No login delay has been applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps

Router NOT enabled to watch for login Attacks
```

The following sample output from the **show login** command verifies that the **login block-for** command is issued. In this example, the command is configured to block login hosts for 100 seconds if 16 or more login requests fail within 100 seconds; five login requests have already failed.

```
Router# show login

A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.

Router enabled to watch for login Attacks.
If more than 15 login failures occur in 100 seconds or less, logins will be disabled for
100 seconds.

Router presently in Watch-Mode, will remain in Watch-Mode for 95 seconds.
Present login failure count 5.
```

The following sample output from the **show login** command verifies that the router is in quiet mode. In this example, the **login block-for** command was configured to block login hosts for 100 seconds if 3 or more login requests fail within 100 seconds.

```
Router# show login
```

```
A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.
```

```
Router enabled to watch for login Attacks.
If more than 2 login failures occur in 100 seconds or less, logins will be disabled for
100 seconds.
```

```
Router presently in Quiet-Mode, will remain in Quiet-Mode for 93 seconds.
Denying logins from all sources.
```

The following sample output from **show login failures** command shows all failed login attempts on the router:

```
Router# show login failures
```

```
Information about login failure's with the device
```

Username	Source IPAddr	lPort	Count	TimeStamp
try1	10.1.1.1	23	1	21:52:49 UTC Sun Mar 9 2003
try2	10.1.1.2	23	1	21:52:52 UTC Sun Mar 9 2003

The following sample output from **show login failures** command verifies that no information is presently logged:

```
Router# show login failures
```

```
*** No logged failed login attempts with the device.***
```

Configuration Examples for Login Parameters

This section includes the following example:

- [Setting Login Parameters: Example, page 7](#)

Setting Login Parameters: Example

The following example shows how to configure your router to enter a 100 second quiet period if 15 failed login attempts is exceeded within 100 seconds; all login requests will be denied during the quiet period except hosts from the ACL "myacl." Also, logging messages will be generated for every 10th failed login and every 15th successful login.

```
Router(config)# login block-for 100 attempts 15 within 100
Router(config)# login quiet-mode access-class myacl
Router(config)# login on-failure log every 10
Router(config)# login on-success log every 15
```

Additional References

The following sections provide references related to Cisco IOS Login Enhancements.

Related Documents

Related Topic	Document Title
AutoSecure	<ul style="list-style-type: none">AutoSecure (Cisco IOS Release 12.3(1) feature module)Cisco IOS Security Configuration Guides, Release 12.4.
Secure Management/Administrative Access	Role-Based CLI Access

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information

about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **login block-for**
 - **login delay**
 - **login on-failure**
 - **login on-success**
 - **login quiet-mode access-class**
 - **show login**
-



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Cisco IOS Resilient Configuration

The Cisco IOS Resilient Configuration feature enables a router to secure and maintain a working copy of the running image and configuration so that those files can withstand malicious attempts to erase the contents of persistent storage (NVRAM and flash).

Feature History for Cisco IOS Resilient Configuration

Release	Modification
12.3(8)T	This feature was introduced.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions for Cisco IOS Resilient Configuration, page 2](#)
- [Information About Cisco IOS Resilient Configuration, page 2](#)
- [How to Use Cisco IOS Resilient Configuration, page 3](#)
- [Additional References, page 6](#)
- [Command Reference, page 7](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Restrictions for Cisco IOS Resilient Configuration

- This feature is available only on platforms that support a Personal Computer Memory Card International Association (PCMCIA) Advanced Technology Attachment (ATA) disk. There must be enough space on the storage device to accommodate at least one Cisco IOS image (two for upgrades) and a copy of the running configuration. IOS File System (IFS) support for secure file systems is also needed by the software.
- It may be possible to force removal of secured files using an older version of Cisco IOS software that does not contain file system support for hidden files.
- This feature can be disabled only by using a console connection to the router. With the exception of the upgrade scenario, feature activation does not require console access.
- You cannot secure a bootset with an image loaded from the network. The running image must be loaded from persistent storage to be secured as primary.
- Secured files will not appear on the output of a **dir** command issued from an executive shell because the IFS prevents secure files in a directory from being listed. ROM monitor (ROMMON) mode does not have any such restriction and can be used to list and boot secured files. The running image and running configuration archives will not be visible in the Cisco IOS **dir** command output. Instead, use the **show secure bootset** command to verify archive existence.

Information About Cisco IOS Resilient Configuration

Before using Cisco IOS Resilient Configuration, you should understand the following concept:

- [Feature Design of Cisco IOS Resilient Configuration, page 2](#)

Feature Design of Cisco IOS Resilient Configuration

A great challenge of network operators is the total downtime experienced after a router has been compromised and its operating software and configuration data erased from its persistent storage. The operator must retrieve an archived copy (if any) of the configuration and a working image to restore the router. Recovery must then be performed for each affected router, adding to the total network downtime.

The Cisco IOS Resilient Configuration feature is intended to speed up the recovery process. The feature maintains a secure working copy of the router image and the startup configuration at all times. These secure files cannot be removed by the user. This set of image and router running configuration is referred to as the primary bootset.

The following factors were considered in the design of Cisco IOS Resilient Configuration:

- The configuration file in the primary bootset is a copy of the running configuration that was in the router when the feature was first enabled.
- The feature secures the smallest working set of files to preserve persistent storage space. No extra space is required to secure the primary Cisco IOS image file.
- The feature automatically detects image or configuration version mismatch.
- Only local storage is used for securing files, eliminating scalability maintenance challenges from storing multiple images and configurations on TFTP servers.
- The feature can be disabled only through a console session.

How to Use Cisco IOS Resilient Configuration

This section contains the following procedures:

- [Archiving a Router Configuration, page 3](#)
- [Restoring an Archived Router Configuration, page 4](#)

Archiving a Router Configuration

This task describes how to save a primary bootset to a secure archive in persistent storage.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **secure boot-image**
4. **secure boot-config**
5. **end**
6. **show secure bootset**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	secure boot-image Example: Router(config)# secure boot-image	Enables Cisco IOS image resilience.
Step 4	secure boot-config Example: Router(config)# secure boot-config	Stores a secure copy of the primary bootset in persistent storage.

	Command or Action	Purpose
Step 5	end Example: Router(config)# end	Exits to privileged EXEC mode.
Step 6	show secure bootset Example: Router# show secure bootset	(Optional) Displays the status of configuration resilience and the primary bootset filename.

Examples

This section provides the following output example:

- [Sample Output for the show secure bootset Command, page 4](#)

Sample Output for the show secure bootset Command

The following example displays sample output from the **show secure bootset** command:

```
Router# show secure bootset
```

```
IOS resilience router id JMX0704L5GH
```

```
IOS image resilience version 12.3 activated at 08:16:51 UTC Sun Jun 16 2002
```

```
Secure archive slot0:c3745-js2-mz type is image (elf) []
  file size is 25469248 bytes, run size is 25634900 bytes
  Runnable image, entry point 0x80008000, run from ram
```

```
IOS configuration resilience version 12.3 activated at 08:17:02 UTC Sun Jun 16 2002
```

```
Secure archive slot0:.runcfg-20020616-081702.ar type is config
configuration archive size 1059 bytes
```

Restoring an Archived Router Configuration

This task describes how to restore a primary bootset from a secure archive after the router has been tampered with (by an NVRAM erase or a disk format).



Note

To restore an archived primary bootset, Cisco IOS image resilience must have been enabled and a primary bootset previously archived in persistent storage.

SUMMARY STEPS

1. **reload**
2. **dir** [*filesystem*:]
3. **boot** [*partition-number*:] [*filename*]
4. **no**
5. **enable**
6. **configure terminal**

7. **secure boot-config** [restore *filename*]
8. **end**
9. **copy** *filename* **running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	reload Example: Router# reload	(Optional) Enters ROM monitor mode, if necessary.
Step 2	dir [<i>filesystem</i> :] Example: rommon 1 > dir slot0:	Lists the contents of the device that contains the secure bootset file. <ul style="list-style-type: none">The device name can be found in the output of the show secure bootset command.
Step 3	boot [<i>partition-number</i> :][<i>filename</i>] Example: rommon 2 > boot slot0:c3745-js2-mz	Boots up the router using the secure bootset image.
Step 4	no Example: --- System Configuration Dialog --- Would you like to enter the initial configuration dialog? [yes/no]: no	(Optional) Declines to enter an interactive configuration session in setup mode. <ul style="list-style-type: none">If the NVRAM was erased, the router enters setup mode and prompts the user to initiate an interactive configuration session.
Step 5	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 6	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 7	secure boot-config [restore <i>filename</i>] Example: Router(config)# secure boot-config restore slot0:rescue-cfg	Restores the secure configuration to the supplied filename.

	Command or Action	Purpose
Step 8	end Example: Router(config)# end	Exits to privileged EXEC mode.
Step 9	copy filename running-config Example: Router# copy slot0:rescue-cfg running-config	Copies the restored configuration to the running configuration.

Additional References

The following sections provide references related to Cisco IOS Resilient Configuration.

Related Documents

Related Topic	Document Title
Additional commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<i>The Cisco IOS Configuration Fundamentals and Network Management Command Reference, Release 12.3 T</i>

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this

module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **secure boot-config**
- **secure boot-image**
- **show secure bootse**



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Image Verification

The Image Verification feature allows users to automatically verify the integrity of Cisco IOS images. Thus, users can be sure that the image is protected from accidental corruption, which can occur at any time during transit, starting from the moment the files are generated by Cisco until they reach the user.

Feature History for Image Verification

Release	Modification
12.2(18)S	This feature was introduced.
12.0(26)S	This feature was integrated into Cisco IOS Release 12.0(26)S.
12.3(4)T	This feature was integrated in Cisco IOS Release 12.3(4)T.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions for Image Verification, page 2](#)
- [Information About Image Verification, page 2](#)
- [How to Use Image Verification, page 2](#)
- [Configuration Examples for Image Verification, page 5](#)
- [Additional References, page 7](#)
- [Command Reference, page 8](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Restrictions for Image Verification

Cisco IOS Release 12.2(18)S and 12.0(26)S Only

Image Verification is applied to and attempted on any file; however, if the file is not an image file, image verification will not occur and you will see the following error, “SIGNATURE-NOT-FOUND.”

Cisco IOS Release 12.3(4)T Only

Image Verification is applied only to image files. If any other file type is copied or verified, you will not receive a warning that image verification did occur, and the command (copy or verify) will silently succeed.

Information About Image Verification

To use image authentication for your Cisco IOS images, you should understand the following concepts:

- [Benefit of Image Verification, page 2](#)
- [How Image Verification Works, page 2](#)

Benefit of Image Verification

The efficiency of Cisco IOS routers is improved because the routers can now automatically detect when the integrity of an image is accidentally corrupted as a result of transmission errors or disk corruption.

How Image Verification Works

Because a production image undergoes a sequence of transfers before it is copied into the memory of a router, the integrity of the image is at risk of accidental corruption every time a transfer occurs. When downloading an image from Cisco.com, a user can run a message-digest5 (MD5) hash on the downloaded image and verify that the MD5 digest posted on Cisco.com is the same as the MD5 digest that is computed on the user's server. However, many users choose not to run an MD5 digest because it is 128-bits long and the verification is manual. Image verification allows the user to automatically validate the integrity of all downloaded images, thereby, significantly reducing user interaction.

How to Use Image Verification

This section contains the following procedures:

- [Globally Verifying the Integrity of an Image, page 3](#)
- [Verifying the Integrity of an Image That Is About to Be Copied, page 4](#)
- [Verifying the Integrity of an Image That Is About to Be Reloaded, page 4](#)

Globally Verifying the Integrity of an Image

The **file verify auto** command enables image verification globally; that is, all images that are to be copied (via the **copy** command) or reloaded (via the **reload** command) are automatically verified. Although both the **copy** and **reload** commands have a **/verify** keyword that enables image verification, you must issue the keyword each time you want to copy or reload an image. The **file verify auto** command enables image verification by default, so you no longer have to specify image verification multiple times.

If you have enabled image verification by default but prefer to disable verification for a specific image copy or reload, the **/noverify** keyword, along with either the **copy** or the **reload** command, will override the **file verify auto** command.

Use this task to enable automatic image verification.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **file verify auto**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	file verify auto Example: Router(config)# file verify auto	Enables automatic image verification.
Step 4	exit Example: Router(config)# exit	Exits global configuration mode. You must exit global configuration mode if you are going to copy or reload an image.

What to Do Next

After issuing the **file verify auto** command, you do not have to issue the **/verify** keyword with the **copy** or the **reload** command because each image that is copied or reloaded will be automatically verified.

Verifying the Integrity of an Image That Is About to Be Copied

When issuing the **copy** command, you can verify the integrity of the copied file by entering the **/verify** keyword. If the integrity check fails, the copied file will be deleted. If the file that is about to be copied does not have an embedded hash (an old image), you will be prompted whether or not to continue with the copying process. If you choose to continue, the file will be successfully copied; if you choose not to continue, the copied file will be deleted.

Without the **/verify** keyword, the **copy** command could copy a file that is not valid. Thus, after the **copy** command has been successfully executed, you can issue the **verify** command at any time to check the integrity of the files that are in the storage of the router.

Use this task to verify the integrity of an image before it is copied onto a router.

SUMMARY STEPS

1. **enable**
2. **copy** [/erase] [/verify | /noverify] *source-url destination-url*
3. **verify** [/md5 [md5-value]] *filesystem:[file-url]*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	copy [/erase] [/verify /noverify] <i>source-url destination-url</i> Example: Router# copy /verify tftp://10.1.1.1/jdoe/c7200-js-mz disk0:	Copies any file from a source to a destination. <ul style="list-style-type: none"> • /verify—Verifies the signature of the destination file. If verification fails, the file will be deleted. • /noverify—Does not verify the signature of the destination file before the image is copied. <p>Note /noverify is often issued if the file verify auto command is enabled, which automatically verifies the signature of all images that are copied.</p>
Step 3	verify [/md5 [md5-value]] <i>filesystem:[file-url]</i> Example: Router# verify bootflash://c7200-kboot-mz.121-8a.E	(Optional) Verifies the integrity of the images in the router's storage.

Verifying the Integrity of an Image That Is About to Be Reloaded

By issuing the **reload** command with the **/verify** keyword, the image that is about to be loaded onto your system will be checked for integrity. If the **/verify** keyword is specified, image verification will occur before the system initiates the reboot. Thus, if verification fails, the image will not be loaded.

**Note**

Because different platforms obtain the file that is to be loaded in various ways, the file specified in BOOTVAR will be verified. If a file is not specified, the first file on each subsystem will be verified.

On certain platforms, because of variables such as the configuration register, the file that is verified may not be the file that is loaded.

Use this task to verify the integrity of an image before it is reloaded onto a router.

SUMMARY STEPS

1. **enable**
2. **reload** [
 - [warm] [/verify | /noverify] *text* |
 - [warm] [/verify | /noverify] in [*hh:*]*mm* [*text*] |
 - [warm] [/verify | /noverify] at *hh:mm* [*month day* | *day month*] [*text*] |
 - [warm] [/verify | /noverify] **cancel**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	reload [[warm] [/verify /noverify] <i>text</i> [warm] [/verify /noverify] in [<i>hh:</i>] <i>mm</i> [<i>text</i>] [warm] [/verify /noverify] at <i>hh:mm</i> [<i>month day</i> <i>day month</i>] [<i>text</i>] [warm] [/verify /noverify] cancel] Example: Router# reload /verify	Reloads the operating system. <ul style="list-style-type: none"> /verify—Verifies the signature of the destination file. If verification fails, the file will be deleted. /noverify—Does not verify the signature of the destination file before the image is reloaded. Note /noverify is often issued if the file verify auto command is enabled, which automatically verifies the signature of all images that are copied.

Configuration Examples for Image Verification

This section contains the following configuration examples:

- [Global Image Verification: Example, page 6](#)
- [Image Verification via the copy Command: Example, page 6](#)
- [Image Verification via the reload Command: Example, page 6](#)
- [verify Command Sample Output: Example, page 7](#)

Global Image Verification: Example

The following example shows how to enable automatic image verification. After enabling this command, image verification will automatically occur for all images that are either copied (via the **copy** command) or reloaded (via the **reload** command).

```
Router(config)# file verify auto
```

Image Verification via the copy Command: Example

The following example shows how to specify image verification before copying an image:

```
Router# copy /verify tftp://10.1.1.1/jdoe/c7200-js-mz disk0:

Destination filename [c7200-js-mz]?
Accessing tftp://10.1.1.1/jdoe/c7200-js-mz...
Loading jdoe/c7200-js-mz from 10.1.1.1 (via FastEthernet0/0):!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 19879944 bytes]

19879944 bytes copied in 108.632 secs (183003 bytes/sec)
Verifying file integrity of disk0:/c7200-js-mz
.....
.....
.....Done!
Embedded Hash MD5 :CFA258948C4ECE52085DCF428A426DCD
Computed Hash MD5 :CFA258948C4ECE52085DCF428A426DCD
CCO Hash MD5 :44A7B9BDDD9638128C35528466318183

Signature Verified
```

Image Verification via the reload Command: Example

The following example shows how to specify image verification before reloading an image onto the router:

```
Router# reload /verify

Verifying file integrity of bootflash:c7200-kboot-mz.121-8a.E
%ERROR:Signature not found in file bootflash:c7200-kboot-mz.121-8a.E.
Signature not present. Proceed with verify? [confirm]
Verifying file disk0:c7200-js-mz
.....
.....Done!
Embedded Hash MD5 :CFA258948C4ECE52085DCF428A426DCD
Computed Hash MD5 :CFA258948C4ECE52085DCF428A426DCD
CCO Hash MD5 :44A7B9BDDD9638128C35528466318183
Signature Verified

Proceed with reload? [confirm]n
```

verify Command Sample Output: Example

The following example shows how to specify image verification via the **verify** command:

```
Router# verify disk0:c7200-js-mz
```

```
%Filesystem does not support verify operations
Verifying file integrity of disk0:c7200-js-mz.....
.....Done!
Embedded Hash   MD5 :CFA258948C4ECE52085DCF428A426DCD
Computed Hash   MD5 :CFA258948C4ECE52085DCF428A426DCD
CCO Hash        MD5 :44A7B9BDDD9638128C35528466318183

Signature Verified
```

Additional References

The following sections provide references related to Image Verification.

Related Documents

Related Topic	Document Title
Configuration tasks and information for loading, maintaining, and rebooting system images	<i>The section “File Management” in the Cisco IOS Configuration Fundamentals and Network Management Configuration Guide</i>
Additional commands for loading, maintaining, and rebooting system images	<i>Cisco IOS Configuration Fundamentals and Network Management Command Reference, Release 12.3 T</i>

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information

about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

New Command

- **file verify auto**

Modified Commands

- **copy**
- **reload**
- **verify**



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



IP Source Tracker

The IP Source Tracker feature allows you to gather information about the traffic that is flowing to a host that is suspected of being under attack. This feature also allows you to easily trace an attack to its entry point into the network.

Feature History for IP Source Tracker

Release	Modification
12.0(21)S	This feature was introduced on the Cisco 12000 series.
12.0(22)S	This feature was implemented on the Cisco 7500 series.
12.0(26)S	This feature was implemented on Cisco 12000 series IP Service Engine (ISE) line cards.
12.3(7)T	This feature was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This feature was integrated into Cisco IOS Release 12.2(25)S.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions for IP Source Tracker, page 2](#)
- [Information About IP Source Tracker, page 2](#)
- [How to Configure IP Source Tracker, page 4](#)
- [Configuration Examples for IP Source Tracker, page 7](#)
- [Additional References, page 8](#)
- [Command Reference, page 10](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Restrictions for IP Source Tracker

Packets Can Be Dropped for Routers

IP source tracking is designed to track attacks against hosts. Packets can be dropped if the line card or port adapter CPU is overwhelmed. Therefore, when used to track an attack against a router, IP source tracking can drop control packets, such as Border Gateway Protocol (BGP) updates.

Engine 0 and 1 Performances Affected on Cisco 12000 Series

There is no performance impact for packets destined to nontracked IP addresses on Engine 2 and Engine 4 line cards because the IP source tracker affects only tracked destinations. Engine 0 and Engine 1 performances are affected because on these engines all packets are switched by the CPU.



Note

On Cisco 7500 series routers, there is no performance impact on destinations that are not tracked.

Information About IP Source Tracker

To configure source tracking, you should understand the following concepts:

- [Identifying and Tracking Denial of Service Attacks, page 2](#)
- [Using IP Source Tracker, page 3](#)
- [Benefits of IP Source Tracker, page 4](#)

Identifying and Tracking Denial of Service Attacks

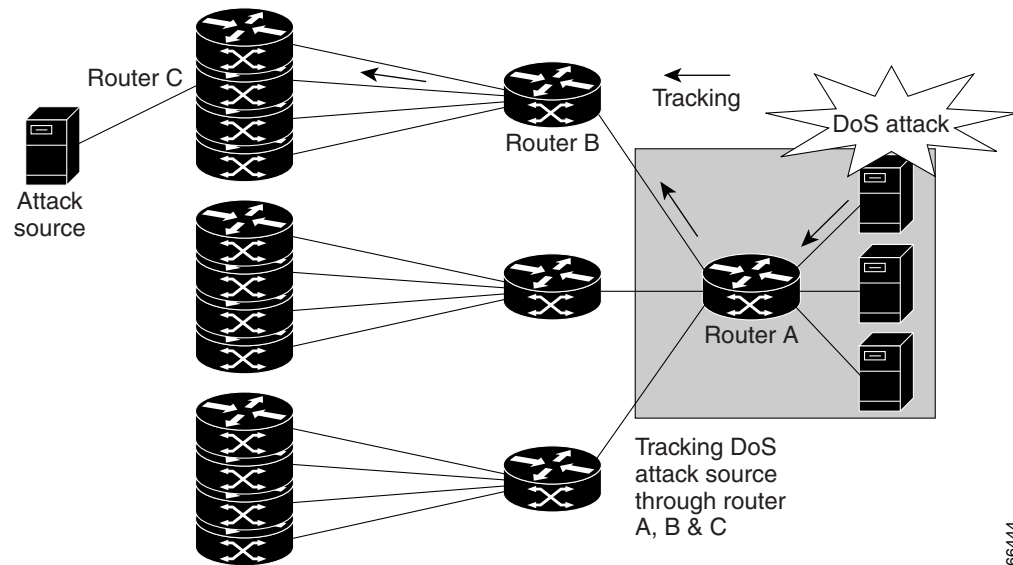
One of the many challenges faced by customers today is the tracking and blocking denial-of-service (DoS) attacks. Counteracting a DoS attack involves intrusion detection, source tracking, and blocking. This functionality addresses the need for source tracking.

To trace attacks, NetFlow and access control lists (ACLs) have been used. To block attacks, committed access rate (CAR) and ACLs have been used. Support for these features on the Cisco 12000 series Internet router has depended on the type of line card used. Support for these features on the Cisco 7500 series routers depends upon the type of port adapter used. There is, therefore, a need to develop a way to receive information that both traces the source of an attack and is supported on all line cards and port adapters.

Normally, when you identify the host that is subject to a DoS attack, you must determine the network ingress point to effectively block the attack. This process starts at the router closest to the host.

For example, in [Figure 124](#), you would start at Router A and try to determine the next upstream router to examine. Traditionally, you would apply an output ACL to the interface connecting to the host to log packets that match the ACL. The logging information is dumped to the router console or system log. You then have to analyze this information, and possibly go through several ACLs in succession to identify the input interface for the attack. In this case the information points back to Router B.

You then repeat this process on Router B, which leads back to Router C, an ingress point into the network. At this point you can use ACLs or CAR to block the attack. This procedure can require applying several ACLs that generate an excessive amount of output to analyze, making this procedure cumbersome and error prone.

Figure 124 Source Tracking in a DoS Attack

66444

Using IP Source Tracker

IP source tracker provides an easier, more scalable alternative to output ACLs for tracking DoS attacks, and it works as follows:

- After you identify the destination being attacked, enable tracking for the destination address on the whole router by entering the **ip source-track** command.
- Each line card creates a special Cisco Express Forwarding (CEF) entry for the destination address being tracked. For line cards or port adapters that use specialized Application-Specific Integrated Circuit (ASICs) for packet switching, the CEF entry is used to punt packets to the line card's or port adapter's CPU.
- Each line card CPU collects information about the traffic flow to the tracked destination.
- The data generated is periodically exported to the router. To display a summary of the flow information, enter the **show ip source-track summary** command. To display more detailed information for each input interface, enter the **show ip source-track** command.
- Statistics provide a breakdown of the traffic to each tracked IP address. This breakdown allows you to determine which upstream router to analyze next. You can shut down the IP source tracker on the current router by entering the **no ip source-track** command, and reopen it on the upstream router.
- Repeat Step 1 to Step 5 until you identify the source of the attack.
- Apply CAR or ACLs to limit or stop the attack.

IP Source Tracker: Hardware Support

IP source tracking is supported on all Engine 0, 1, 2, and 4 line cards in the Cisco 12000 series Internet router. It is also supported on all port adapters and RSPs that have CEF switching enabled on Cisco 7500 series routers.

Benefits of IP Source Tracker

Complete Tracking Information Provided

IP source tracking generates all the necessary information in an easy-to-use format to track the network entry point of a DoS attack.

Tracking an Unlimited Number of IPs Simultaneously

IP source tracking allows you to track multiple IPs at the same time. By default there is no limit. To limit the number of IPs that are simultaneously tracked, use the **ip source-track address-limit** command.

Complete Network Coverage for Cisco 12000 Series and Cisco 7500 Series Routers as of 12.0(26)S

Because IP source tracking is supported on all line cards on the Cisco 12000 series routers and on all port adapters on Cisco 7500 series routers, it allows you to track DoS attacks across your entire network.



Note

For Cisco IOS Release 12.0(21)S and 12.0(22)S, IP source tracking is supported only on Engine 0, 1, 2, and 4 line cards on Cisco 12000 series routers; that is, Engine 3 is not supported.

How to Configure IP Source Tracker

This section contains the following procedures:

- [Configuring IP Source Tracking, page 4](#) (required)
- [Verifying IP Source Tracking, page 5](#) (optional)

Configuring IP Source Tracking

To configure IP source tracking for a host under attack, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip source-track *ip-address***
4. **ip source-track address-limit *number***
5. **ip source-track syslog-interval *number***
6. **ip source-track export-interval *number***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip source-track ip-address Example: Router(config)# ip source-track 100.10.0.1	Enables IP source tracking for a specified host.
Step 4	ip source-track address-limit number Example: Router(config)# ip source-track address-limit 10	(Optional) Limits the number of hosts that can be simultaneously tracked at any given time. Note If this command is not enabled, there is no limit to the number of hosts that be can tracked.
Step 5	ip source-track syslog-interval number Example: Router(config)# ip source-track syslog-interval 2	(Optional) Sets the time interval, in minutes, used to generate syslog messages that indicate IP source tracking is enabled. Note If this command is not enabled, system log messages are not generated.
Step 6	ip source-track export-interval number Example: Router(config)# ip source-track export-interval 30	(Optional) Sets the time interval, in seconds, used to export IP tracking statistics that are collected in the line cards to the gigabit route processor (GRP) and the port adapters to the route switch processor (RSP). Note If this command is not enabled, traffic flow information is exported to the GRP and RSP every 30 seconds.

What to Do Next

After you have configured source tracking on your network device, you can verify your configuration and source tracking statistics, such as traffic flow. To complete this task, see the following section [“Verifying IP Source Tracking.”](#)

Verifying IP Source Tracking

To verify the status of source tracking, such as packet processing and traffic flow information, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show ip source-track** [*ip-address*] [**summary** | **cache**]
3. **show ip source-track export flows**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show ip source-track [<i>ip-address</i>] [summary cache] Example: Router# show ip source-track summary	Displays traffic flow statistics for tracked IP host addresses
Step 3	show ip source-track export flows Example: Router# show ip source-track export flows	Displays the last 10 packet flows that were exported from the line card to the route processor. Note This command can be issued only on distributed platforms, such as the GRP and the RSP.

Examples

The following example, which is sample output from the **show ip source-track summary** command, shows how to verify that IP source tracking is enabled for one or more hosts:

```
Router# show ip source-track summary
```

Address	Bytes	Pkts	Bytes/s	Pkts/s
10.0.0.1	119G	1194M	443535	4432
192.168.1.1	119G	1194M	443535	4432
192.168.42.42	119G	1194M	443535	4432

The following example, which is sample output from the **show ip source-track summary** command, shows how to verify that no traffic has yet to be received for the destination hosts that are being tracked:

```
Router# show ip source-track summary
```

Address	Bytes	Pkts	Bytes/s	Pkts/s
10.0.0.1	0	0	0	0
192.168.1.1	0	0	0	0
192.168.42.42	0	0	0	0

The following example, which is sample output from the **show ip source-track** command, shows how to verify that IP source tracking is processing packets to the hosts and exporting statistics from the line card or port adapter to the GRP and RSP:

```
Router# show ip source-track
```

Address	SrcIF	Bytes	Pkts	Bytes/s	Pkts/s
10.0.0.1	PO0/0	119G	1194M	513009	5127

```

192.168.1.1      PO0/0      119G      1194M      513009      5127
192.168.42.42   PO0/0      119G      1194M      513009      5127

```

Configuration Examples for IP Source Tracker

This section includes the following examples:

- [Configuring IP Source Tracking: Example, page 7](#)
- [Verifying Source Interface Statistics for All Tracked IP Addresses: Example, page 7](#)
- [Verifying a Flow Statistic Summary for All Tracked IP Addresses: Example, page 7](#)
- [Verifying Detailed Flow Statistics Collected by a Line Card: Example, page 8](#)
- [Verifying Flow Statistics Exported from Line Cards and Port Adapters: Example, page 8](#)

Configuring IP Source Tracking: Example

The following example shows how to configure IP source tracking on all line cards and port adapters in the router. In this example, each line card or port adapter collects traffic flow data to host address 100.10.0.1 for 2 minutes before creating an internal system log entry; packet and flow information recorded in the system log is exported for viewing to the route processor or switch processor every 60 seconds.

```

Router# configure interface
Router(config)# ip source-track 100.10.0.1
Router(config)# ip source-track syslog-interval 2
Router(config)# ip source-track export-interval 60

```

Verifying Source Interface Statistics for All Tracked IP Addresses: Example

The following example displays a summary of the traffic flow statistics that are collected on each source interface for tracked host addresses.

```
Router# show ip source-track
```

Address	SrcIF	Bytes	Pkts	Bytes/s	Pkts/s
10.0.0.1	PO2/0	0	0	0	0
192.168.9.9	PO1/2	131M	511M	1538	6
192.168.9.9	PO2/0	144G	3134M	6619923	143909

Verifying a Flow Statistic Summary for All Tracked IP Addresses: Example

The following example displays a summary of traffic flow statistics for all hosts that are being tracked; it shows that no traffic has yet been received.

```
Router# show ip source-track summary
```

Address	Bytes	Pkts	Bytes/s	Pkts/s
10.0.0.1	0	0	0	0
100.10.1.1	131M	511M	1538	6
192.168.9.9	146G	3178M	6711866	145908

Verifying Detailed Flow Statistics Collected by a Line Card: Example

The following example displays traffic flow information that is collected on line card 0 for all tracked hosts.

```
Router# exec slot 0 show ip source-track cache
```

```
===== Line Card (Slot 0) =====
```

```
IP packet size distribution (7169M total packets):
```

```
1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 480
.000 .000 .000 0.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
```

```
512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
.000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
```

```
IP Flow Switching Cache, 278544 bytes
```

```
1 active, 4095 inactive, 13291 added
```

```
198735 aged polls, 0 flow alloc failures
```

```
Active flows timeout in 0 minutes
```

```
Inactive flows timeout in 15 seconds
```

```
last clearing of statistics never
```

Protocol	Total	Flows	Packets	Bytes	Packets	Active(Sec)	Idle(Sec)
-----	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow	/Flow
SrcIf	SrcIPAddress		DstIf		DstIPAddress	Pr	TOS Flgs Pkts
Port Msk AS			Port Msk AS		NextHop		B/Pk Active
PO0/0	101.1.1.0		Null		100.1.1.1	06 00 00	55K
0000 /0 0			0000 /0 0		0.0.0.0	100	10.1

Verifying Flow Statistics Exported from Line Cards and Port Adapters: Example

The following example displays packet flow information that is exported from line cards and port adapters to the GRP and the RSP:

```
Router# show ip source-track export flows
```

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
PO0/0	101.1.1.0	Null	100.1.1.1	06	0000	0000	88K
PO0/0	101.1.1.0	Null	100.1.1.3	06	0000	0000	88K
PO0/0	101.1.1.0	Null	100.1.1.2	06	0000	0000	88K

Additional References

The following sections provide references related to IP Source Tracker.

Related Documents

Related Topic	Document Title
ACLs	The section “Filtering IP Packets Using Access Lists” in the chapter “Configuring IP Services” of the <i>Cisco IOS IP Configuration Guide</i>
Dynamic ACLs	The chapter “Configuring Lock-and-Key Security (Dynamic Access Lists)” in the <i>Cisco IOS Security Configuration Guide</i>
DoS prevention	The chapter “Configuring TCP Intercept (Preventing Denial-of-Service Attacks)” in the <i>Cisco IOS Security Configuration Guide</i>

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	—

Techn

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following new commands are pertinent to this feature.

- **ip source-track**
- **ip source-track address-limit**
- **ip source-track export-interval**
- **ip source-track syslog-interval**
- **show ip source-track**
- **show ip source-track export flows**

For information about these commands, see the Cisco IOS Security Command Reference at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

© 2007 Cisco Systems, Inc. All rights reserved.



IP Traffic Export

The IP Traffic Export feature allows users to configure their router to export IP packets that are received on multiple, simultaneous WAN or LAN interfaces. The unaltered IP packets are exported on a single LAN or VLAN interface, thereby, easing deployment of protocol analyzers and monitoring devices.

Feature History for IP Traffic Export

Release	Modification
12.3(4)T	This feature was introduced.
12.2(25)S	This feature was integrated into Cisco IOS Release 12.2(25)S.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Restrictions for IP Traffic Export, page 2](#)
- [Information About IP Traffic Export, page 2](#)
- [How to Use IP Traffic Export, page 3](#)
- [Configuration Examples for IP Traffic Export, page 6](#)
- [Additional References, page 8](#)
- [Command Reference, page 10](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Restrictions for IP Traffic Export

Platform Restriction

IP traffic export is intended only for software switching platforms; distributed architectures are not supported.

IP Packet Forwarding Performance Impact

When IP traffic export is enabled, a delay is incurred on the outbound interface when packets are captured and transmitted across the interface. Performance delays increase with the increased number of interfaces that are monitored and the increased number of destination hosts.

Exported Traffic Limitation

- The MAC address of the device that is receiving the exported traffic must be on the same VLAN or directly connected to one of the router interfaces. (Use the **show arp** command to determine the MAC address of device that is directly connected to an interface.)
- The outgoing interface for exported traffic must be Ethernet (10/100/1000). (Incoming (monitored) traffic can traverse any interface.)

Information About IP Traffic Export

To use the IP traffic export, you should understand the following concept:

- [Benefits of IP Traffic Export, page 2](#)

Benefits of IP Traffic Export

Simplified IDS Deployment

Without the ability to export IP traffic, the Intrusion Detection System (IDS) probe must be inline with the network device to monitor traffic flow. IP traffic export eliminates the probe placement limitation, allowing users to place an IDS probe in any location within their network or direct all exported traffic to a VLAN that is dedicated for network monitoring. Allowing users to choose the optimal location of their IDS probe reduces processing burdens.

Also, because packet processing that was once performed on the network device can now be performed away from the network device, the need to enable IDS with the Cisco IOS software can be eliminated.

IP Traffic Export Functionality Benefits

Users can configure their router to perform the following tasks:

- Filter copied packets via an access control list (ACL)
- Filter copied packets via sampling, which allows you to export one in every few packets in which you are interested. Use this option when it is not necessary to export all incoming traffic. Also, sampling is useful when a monitored ingress interface can send traffic faster than the egress interface can transmit it.
- Configure bidirectional traffic on an interface. (By default, only incoming traffic is exported.)

How to Use IP Traffic Export

This section contains the following procedures:

- [Configuring IP Traffic Export, page 3](#)
- [Displaying IP Traffic Export Configuration Data, page 5](#)

Configuring IP Traffic Export

Use this task to configure IP traffic export profiles, which enable IP traffic to be exported on an ingress interface and allow you to specify profile attributes, such as the outgoing interface for exporting traffic.



Note

Packet exporting is performed before packet switching or filtering.

IP Traffic Export Profiles Overview

All packet export configurations are specified via IP traffic export profiles, which consist of IP-traffic-export-related command-line interfaces (CLIs) that control various attributes for both incoming and outgoing exported IP traffic. You can configure a router with multiple IP traffic export profiles. (Each profile must have a different name.) You can apply different profiles on different interfaces.

The two different IP traffic export profiles are as follows:

- The global configuration profile, which is configured via the **ip traffic-export profile** command.
- The IP traffic export submode configuration profile, which is configured via any of the following router IP Traffic Export (RITE) commands—**bidirectional**, **incoming**, **interface**, **mac-address**, and **outgoing**.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip traffic-export profile** *profile-name*
4. **interface** *interface-name*
5. **bidirectional**
6. **mac-address** *H.H.H*
7. **incoming** {**access-list** {*standard* | *extended* | *named*} | **sample one-in-every** *packet-number*}
8. **outgoing** {**access-list** {*standard* | *extended* | *named*} | **sample one-in-every** *packet-number*}
9. **exit**
10. **interface** *type number*
11. **ip traffic-export apply** *profile-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip traffic-export profile <i>profile-name</i> Example: Router(config)# ip traffic-export profile my_rite	Creates or edits an IP traffic export profile, enables the profile on an ingress interface, and enters RITE configuration mode.
Step 4	interface <i>interface-name</i> Example: Router(config-rite)# interface FastEthernet 0/1	Specifies the outgoing (monitored) interface for exported traffic. Note If you do not issue this command, the profile will not recognize an interface in which to send the captured IP traffic.
Step 5	bidirectional Example: Router(config-rite)# bidirectional	(Optional) Exports incoming and outgoing IP traffic on the monitored interface. Note If this command is not enabled, only incoming traffic is exported.
Step 6	mac-address <i>H.H.H</i> Example: Router(config-rite)# mac-address 00a.8aab.90a0	Specifies the 48-bit address of the destination host that is receiving the exported traffic. Note If you do not issue this command, the profile will not recognize a destination host in which to send the exported packets.
Step 7	incoming { access-list { <i>standard</i> <i>extended</i> <i>named</i> } sample one-in-every <i>packet-number</i> } Example: Router(config-rite)# incoming access-list my_acl	(Optional) Configures filtering for incoming traffic. After you have created a profile via the ip traffic-export profile , this functionality is enabled by default.
Step 8	outgoing { access-list { <i>standard</i> <i>extended</i> <i>named</i> } sample one-in-every <i>packet-number</i> } Example: Router(config-rite)# outgoing sample one-in-every 50	(Optional) Configures filtering for outgoing export traffic. Note If you issue this command, you must also issue the bidirectional command, which enables outgoing traffic to be exported. However, only routed traffic (such as passthrough traffic) is exported; that is, traffic that originates from the network device is not exported.
Step 9	exit	Exits RITE configuration mode.

	Command or Action	Purpose
Step 10	interface <i>type number</i> Example: Router(config)# interface FastEthernet0/0	Configures an interface type and enters interface configuration mode.
Step 11	ip traffic-export apply <i>profile-name</i> Example: Router(config-if)# ip traffic-export apply my_rite	Enables IP traffic export on an ingress interface.

Troubleshooting Tips

Creating an IP Traffic Export Profile

The **interface** and **mac-address** commands are required to successfully create a profile. If these commands are not issued, you will receive the following profile incomplete message if the **show running config** command is issued:

```
ip traffic-export profile newone
! No outgoing interface configured
! No destination mac-address configured
```

Applying an IP Traffic Export Profile to an interface

The following system logging messages should appear immediately after you activate and deactivate a profile from an interface (via the **ip traffic-export apply profile** command):

- Activated profile:

```
%RITE-5-ACTIVATE: Activated IP traffic export on interface FastEthernet 0/0.
```

- Deactivated profile:

```
%RITE-5-DEACTIVATE: Deactivated IP traffic export on interface FastEthernet 0/0.
```

If you attempt to apply an incomplete profile to an interface, you will receive the following message:

```
Router(config-if)# ip traffic-export apply newone
RITE: profile newone has missing outgoing interface
```

What to Do Next

After you have configured a profile and enabled the profile on an ingress interface, you can monitor IP traffic exporting events and verify your profile configurations. To complete these steps, refer to the following task “[Displaying IP Traffic Export Configuration Data](#).”

Displaying IP Traffic Export Configuration Data

This task allows you to verify IP traffic export parameters such as the monitored ingress interface, which is where the IP traffic is exported, and outgoing and incoming IP packet information, such as configured ACLs. You can also use this task to monitor packets that are captured and then transmitted across an interface to a destination host. Use this optional task to help you troubleshoot any problems with your exported IP traffic configurations.

SUMMARY STEPS

1. **enable**
2. **debug ip traffic-export events**
3. **show ip traffic-export [interface *interface-name* | profile *profile-name*]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	debug ip traffic-export events Example: Router# debug ip traffic-export events	Enables debugging messages for exported IP traffic packets events.
Step 3	show ip traffic-export [interface <i>interface-name</i> profile <i>profile-name</i>] Example: Router# show ip traffic-export	Displays information related to exported IP traffic events. <ul style="list-style-type: none"> • interface <i>interface-name</i>—Only data associated with the monitored ingress interface is shown. • profile <i>profile-name</i>—Only flow statistics, such as exported packets and the number of bytes, are shown.

Examples

The following sample output from the **show ip traffic-export** command is for the profile “one.” This example is for a single, configured interface. If multiple interfaces are configured, the information shown below is displayed for each interface.

```
Router# show ip traffic-export

Router IP Traffic Export Parameters
Monitored Interface      FastEthernet0/0
Export Interface         FastEthernet0/1
Destination MAC address  0030.7131.abfc
bi-directional traffic export is off
Input IP Traffic Export Information   Packets/Bytes Exported   0/0
Packets Dropped          0
Sampling Rate             one-in-every 1 packets
No Access List configured
Profile one is Active
```

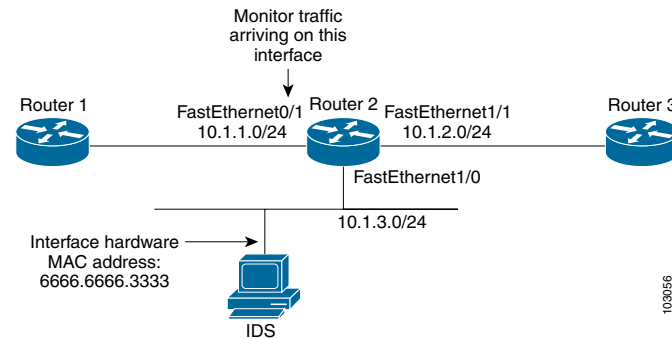
Configuration Examples for IP Traffic Export

This section includes the following configuration example:

- [Exporting IP Traffic Configuration: Example, page 7](#)

Exporting IP Traffic Configuration: Example

Figure 1 and the following sample output from the **show running-config** command illustrate how to configure Router 2 to export the incoming traffic from Router 1 to IDS:



Router2# **show running-config**

Building configuration...

Current configuration :2349 bytes

```

! Last configuration change at 20:35:39 UTC Wed Oct 8 2003
! NVRAM config last updated at 20:35:39 UTC Wed Oct 8 2003
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
!
hostname rite-3745
!
boot system flash:c3745-js-mz.123-1.8.PI2d
no logging console
enable password lab
!
no aaa new-model
ip subnet-zero
!
no ip domain lookup
!
ip cef
!
ip traffic-export profile my_rite
  interface FastEthernet1/0
    mac-address 6666.6666.3333
!
interface FastEthernet0/0
  ip address 10.0.0.94 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet0/1
  ip address 10.1.1.2 255.255.255.0
  duplex auto
  speed auto

```



```
ip traffic-export apply my_rite
!
interface FastEthernet1/0
ip address 10.1.3.2 255.255.255.0
no ip redirects
no cdp enable
!
interface FastEthernet1/1
ip address 10.1.2.2 255.255.255.0
duplex auto
speed auto
!
router ospf 100
log-adjacency-changes
network 10.1.0.0 0.0.255.255 area 0
!
ip http server
ip classless
!
snmp-server engineID local 0000000902000004C1C59140
snmp-server community public RO
snmp-server enable traps tty
!
control-plane
!
dial-peer cor custom
!
gateway
!
line con 0
exec-timeout 0 0
stopbits 1
line aux 0
line vty 0 4
password lab
login
!
ntp clock-period 17175608
ntp server 10.0.0.2
!
end
```

Additional References

The following sections provide references related to IP Traffic Export.

Related Documents

Related Topic	Document Title
Configuring IDS	<i>The chapter “Configuring Cisco IOS Firewall Intrusion Detection System” in the section “Traffic Filtering and Firewalls” of the Cisco IOS Security Configuration Guide.</i>
Configuring IP	<i>The chapter “Configuring IP Services” in the section “IP Addressing and Services” of the Cisco IOS IP Configuration Guide</i>

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features

- **bidirectional**
- **debug ip traffic-export events**
- **incoming**
- **interface (RITE)**
- **ip traffic-export apply**
- **ip traffic-export profile**
- **mac-address (RITE)**
- **outgoing**
- **show ip traffic-export**

For information about these commands, see the Cisco IOS Security Command Reference at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Role-Based CLI Access

The Role-Based CLI Access feature allows the network administrator to define “views,” which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS EXEC and configuration (Config) mode commands. Views restrict user access to Cisco IOS command-line interface (CLI) and configuration information; that is, a view can define what commands are accepted and what configuration information is visible. Thus, network administrators can exercise better control over access to Cisco networking devices.

Feature History for Role-Based CLI Access

Release	Modification
12.3(7)T	This feature was introduced.
12.3(11)T	The CLI view capability was extended to restrict user access on a per-interface level, and additional CLI views were introduced to support the extended view capability. Also, support to group configured CLI views into a superview was introduced.
12.2(33)SRB	This feature was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	All feature functionality was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Role-Based CLI Access, page 2](#)
- [Restrictions for Role-Based CLI Access, page 2](#)
- [Information About Role-Based CLI Access, page 2](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2004, 2007-2008 Cisco Systems, Inc. All rights reserved.

- [How to Use Role-Based CLI Access, page 3](#)
- [Configuration Examples for Role-Based CLI Access, page 9](#)
- [Additional References, page 12](#)
- [Command Reference, page 13](#)

Prerequisites for Role-Based CLI Access

Your image must support CLI views.

Restrictions for Role-Based CLI Access

Lawful Intercept Images Limitation

Because CLI views are a part of the Cisco IOS parser, CLI views are a part of all platforms and Cisco IOS images. However, the lawful intercept view is available only in images that contain the lawful intercept subsystem.

Maximum Number of Allowed Views

The maximum number of CLI views and superviews, including one lawful intercept view, that can be configured is 15. (This does not include the root view.)

Information About Role-Based CLI Access

To create and use views, you should understand the following concepts:

- [Benefits of Using CLI Views, page 2](#)
- [Root View, page 3](#)
- [View Authentication via a New AAA Attribute, page 3](#)

Benefits of Using CLI Views

Views: Detailed Access Control

Although users can control CLI access via both privilege levels and enable mode passwords, these functions do not provide network administrators with the necessary level of detail needed when working with Cisco IOS routers and switches. CLI views provide a more detailed access control capability for network administrators, thereby, improving the overall security and accountability of Cisco IOS software.

As of Cisco IOS Release 12.3(11)T, network administrators can also specify an interface or a group of interfaces to a view; thereby, allowing access on the basis of specified interfaces.

Root View

When a system is in “root view,” it has all of the access privileges as a user who has level 15 privileges. If the administrator wishes to configure any view to the system (such as a CLI view, a superview, or a lawful intercept view), the system must be in root view.

The difference between a user who has level 15 privileges and a root view user is that a root view user can configure a new view and add or remove commands from the view. Also, when you are in a CLI view, you have access only to the commands that have been added to that view by the root view user.

View Authentication via a New AAA Attribute

View authentication is performed by an external authentication, authorization, and accounting (AAA) server via the new attribute “cli-view-name.”

AAA authentication associates only one view name to a particular user; that is, only one view name can be configured for a user in an authentication server.

How to Use Role-Based CLI Access

This section contains the following procedures:

- [Configuring a CLI View, page 3](#) (required)
- [Configuring a Lawful Intercept View, page 5](#) (optional)
- [Configuring a Superview, page 7](#) (optional)
- [Monitoring Views and View Users, page 9](#) (optional)

Configuring a CLI View

Use this task to create a CLI view and add commands or interfaces to the view, as appropriate.

Prerequisites

Before you create a view, you must perform the following tasks:

- Enable AAA via the **aaa new-model** command. (For more information on enabling AAA, see the chapter “Configuring Authentication” in the *Cisco IOS Security Configuration Guide*, Release 12.3.)
- Ensure that your system is in root view—not privilege level 15.

SUMMARY STEPS

1. **enable view**
2. **configure terminal**
3. **parser view** *view-name*
4. **secret 5** *encrypted-password*
5. **commands** *parser-mode* {**include** | **include-exclusive** | **exclude**} [**all**] [**interface** *interface-name* | *command*]

6. **exit**
7. **exit**
8. **enable** [*privilege-level*] [**view** *view-name*]
9. **show parser view** [**all**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable view Example: Router> enable view	Enables root view. <ul style="list-style-type: none"> Enter your privilege level 15 password (for example, root password) if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	parser view <i>view-name</i> Example: Router(config)# parser view first	Creates a view and enters view configuration mode.
Step 4	secret 5 <i>encrypted-password</i> Example: Router(config-view)# secret 5 secret	Associates a command-line interface (CLI) view or superview with a password. Note You must issue this command before you can configure additional attributes for the view.
Step 5	commands <i>parser-mode</i> { include include-exclusive exclude } [all] [interface <i>interface-name</i> <i>command</i>] Example: Router(config-view)# commands exec include show version	Adds commands or interfaces to a view. <ul style="list-style-type: none"> <i>parser-mode</i>—The mode in which the specified command exists. include—Adds a command or an interface to the view and allows the same command or interface to be added to an additional view. include-exclusive—Adds a command or an interface to the view and excludes the same command or interface from being added to all other views. exclude—Excludes a command or an interface from the view; that is, customers cannot access a command or an interface. all—A “wildcard” that allows every command in a specified configuration mode that begins with the same keyword or every subinterface for a specified interface to be part of the view. interface <i>interface-name</i>—Interface that is added to the view. <i>command</i>—Command that is added to the view.

	Command or Action	Purpose
Step 6	exit Example: Router(config-view)# exit	Exits view configuration mode.
Step 7	exit Example: Router(config)# exit	Exits global configuration mode.
Step 8	enable [<i>privilege-level</i>] [view <i>view-name</i>] Example: Router# enable view first	Prompts the user for a password, which allows the user to access a configured CLI view, and is used to switch from one view to another view. After the correct password is given, the user can access the view.
Step 9	show parser view [all] Example: Router# show parser view	(Optional) Displays information about the view that the user is currently in. <ul style="list-style-type: none"> all—Displays information for all views that are configured on the router. Note Although this command is available for both root and lawful intercept users, the all keyword is available only to root users. However, the all keyword can be configured by a user in root view to be available for users in lawful intercept view and CLI view.

Troubleshooting Tips

After you have successfully created a view, a system message such as the following will be displayed:

```
%PARSER-6-VIEW_CREATED: view 'first' successfully created.
```

After you have successfully deleted a view, a system message such as the following will be displayed:

```
%PARSER-6-VIEW_DELETED: view 'first' successfully deleted.
```

You must associate a password with a view. If you do not associate a password, and you attempt to add commands to the view via the **commands** command, a system message such as the following will be displayed:

```
%Password not set for view <viewname>.
```

Configuring a Lawful Intercept View

Use this task to initialize and configure a view for lawful-intercept-specific commands and configuration information. (Only an administrator or a user who has level 15 privileges can initialize a lawful intercept view.)

About Lawful Intercept Views

Like a CLI view, a lawful intercept view restricts access to specified commands and configuration information. Specifically, a lawful intercept view allows a user to secure access to lawful intercept commands that are held within the TAP-MIB, which is a special set of simple network management protocol (SNMP) commands that store information about calls and users.

Commands available in lawful intercept view belong to one of the following categories:

- Lawful intercept commands that should not be made available to any other view or privilege level
- CLI views that are useful for lawful intercept users but do not have to be excluded from other views or privilege levels

Prerequisites

Before you initialize a lawful intercept view, ensure that the privilege level is set to 15 via the **privilege** command.

SUMMARY STEPS

1. **enable view**
2. **configure terminal**
3. **li-view** *li-password* **user** *username* **password** *password*
4. **username** [**lawful-intercept**] *name* [**privilege** *privilege-level* | **view** *view-name*] **password** *password*
5. **parser view** *view-name*
6. **secret** **5** *encrypted-password*
7. **name** *new-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable view Example: Router> enable view	Enables root view. • Enter your privilege level 15 password (for example, root password) if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	li-view <i>li-password</i> user <i>username</i> password <i>password</i> Example: Router(config)# li-view lipass user li_admin password li_adminpass	Initializes a lawful intercept view. After the li-view is initialized, you must specify at least one user via user <i>username</i> password <i>password</i> options.

	Command or Action	Purpose
Step 4	username [lawful-intercept [<i>name</i>] [privilege <i>privilege-level</i> view <i>view-name</i>] password <i>password</i> Example: Router(config)# username lawful-intercept li-user1 password li-user1pass	Configures lawful intercept users on a Cisco device.
Step 5	parser view <i>view-name</i> Example: Router(config)# parser view li view name	(Optional) Enters view configuration mode, which allows you to change the lawful intercept view password or the lawful intercept view name.
Step 6	secret 5 <i>encrypted-password</i> Example: Router(config-view)# secret 5 secret	(Optional) Changes an existing password for a lawful intercept view.
Step 7	name <i>new-name</i> Example: Router(config-view)# name second	(Optional) Changes the name of a lawful intercept view. If this command is not issued, the default name of the lawful intercept view is “li-view.”

Troubleshooting Tips

To display information for all users who have access to a lawful intercept view, issue the **show users lawful-intercept** command. (This command is available only to authorized lawful intercept view users.)

Configuring a Superview

Use this task to create a superview and add at least one CLI view to the superview.

About Superviews

A superview consists of one or more CLI views, which allow users to define what commands are accepted and what configuration information is visible. Superviews allow a network administrator to easily assign all users within configured CLI views to a superview instead of having to assign multiple CLI views to a group of users.

Superviews contain the following characteristics:

- A CLI view can be shared among multiple superviews.
- Commands cannot be configured for a superview; that is, you must add commands to the CLI view and add that CLI view to the superview.
- Users who are logged into a superview can access all of the commands that are configured for any of the CLI views that are part of the superview.
- Each superview has a password that is used to switch between superviews or from a CLI view to a superview.
- If a superview is deleted, all CLI views associated with that superview will not be deleted too.

Adding CLI Views to a Superview

You can add a view to a superview only after a password has been configured for the superview (via the **secret 5** command). Thereafter, issue the **view** command in view configuration mode to add at least one CLI view to the superview.



Note

Before adding a CLI view to a superview, ensure that the CLI views that are added to the superview are valid views in the system; that is, the views have been successfully created via the **parser view** command.

SUMMARY STEPS

1. **enable view**
2. **configure terminal**
3. **parser view** *superview-name* **superview**
4. **secret 5** *encrypted-password*
5. **view** *view-name*
6. **exit**
7. **exit**
8. **show parser view** [**all**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable view Example: Router> enable view	Enables root view. <ul style="list-style-type: none">Enter your privilege level 15 password (for example, root password) if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	parser view <i>superview-name</i> superview Example: Router(config)# parser view su_view1 superview	Creates a superview and enters view configuration mode.
Step 4	secret 5 <i>encrypted-password</i> Example: Router(config-view)# secret 5 secret	Associates a CLI view or superview with a password. Note You must issue this command before you can configure additional attributes for the view.
Step 5	view <i>view-name</i> Example: Router(config-view)# view view_three	Adds a normal CLI view to a superview. Issue this command for each CLI view that is to be added to a given superview.

	Command or Action	Purpose
Step 6	exit Example: Router(config-view)# exit	Exits view configuration mode.
Step 7	exit Example: Router(config)# exit	Exits global configuration mode.
Step 8	show parser view [all] Example: Router# show parser view	<p>(Optional) Displays information about the view that the user is currently in.</p> <ul style="list-style-type: none"> all—Displays information for all views that are configured on the router. <p>Note Although this command is available for both root and lawful intercept users, the all keyword is available only to root users. However, the all keyword can be configured by a user in root view to be available for users in lawful intercept view and CLI view.</p>

Monitoring Views and View Users

To display debug messages for all views—root, CLI, lawful intercept, and super, use the **debug parser view** command in privileged EXEC mode.

Configuration Examples for Role-Based CLI Access

This section contains the following configuration examples:

- [Configuring a CLI View: Example, page 9](#)
- [Verifying a CLI View: Example, page 10](#)
- [Configuring a Lawful Intercept View: Example, page 11](#)
- [Configuring a Superview: Example, page 12](#)

Configuring a CLI View: Example

The following example shows how to configure two CLI views, “first” and “second.” Thereafter, you can verify the CLI view in the running configuration.

```
Router(config)# parser view first
00:11:40:%PARSER-6-VIEW_CREATED:view 'first' successfully created.
Router(config-view)# secret 5 firstpass
Router(config-view)# command exec include show version
Router(config-view)# command exec include configure terminal
Router(config-view)# command exec include all show ip
Router(config-view)# exit
Router(config)# parser view second
```

```

00:13:42:%PARSER-6-VIEW_CREATED:view 'second' successfully created.
Router(config-view)# secret 5 secondpass
Router(config-view)# command exec include-exclusive show ip interface
Router(config-view)# command exec include logout
Router(config-view)# exit
!
!
Router(config-view)# do show run | beg view
parser view first
secret 5 $1$MCmh$QuZaU8PIMPlff9sFCZvgW/
commands exec include configure terminal
commands exec include configure
commands exec include all show ip
commands exec include show version
commands exec include show
!
parser view second
secret 5 $1$iP2M$R16BXKecMEiQesxLyqygW.
commands exec include-exclusive show ip interface
commands exec include show ip
commands exec include show
commands exec include logout
!

```

Verifying a CLI View: Example

After you have configured the CLI views “first” and “second,” you can issue the **enable view** command to verify which commands are available in each view. The following example shows which commands are available inside the CLI view “first” after the user has logged into this view. (Because the **show ip interface** command is configured with the all option, a complete set of suboptions is shown, except the **show ip interface** command, which is using the include-exclusive keyword in the second view.)

```

Router# enable view first
Password:

00:28:23:%PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
Router# ?
Exec commands:
  configure  Enter configuration mode
  enable     Turn on privileged commands
  exit       Exit from the EXEC
  show       Show running system information

Router# show ?

  ip          IP information
  parser      Display parser information
  version     System hardware and software status

Router# show ip ?

  access-lists      List IP access lists
  accounting         The active IP accounting database
  aliases           IP alias table
  arp               IP ARP table
  as-path-access-list List AS path access lists
  bgp               BGP information
  cache             IP fast-switching route cache
  casa              display casa information
  cef               Cisco Express Forwarding
  community-list    List community-list

```

dfp	DFP information
dhcp	Show items in the DHCP database
drp	Director response protocol
dvmrp	DVMRP information
eigrp	IP-EIGRP show commands
extcommunity-list	List extended-community list
flow	NetFlow switching
helper-address	helper-address table
http	HTTP information
igmp	IGMP information
irdp	ICMP Router Discovery Protocol
.	
.	
.	

Configuring a Lawful Intercept View: Example

The following example shows how to configure a lawful intercept view, add users to the view, and verify the users that were added:

```
!Initialize the LI-View.
Router(config-view)# li-view lipass user li_admin password li_adminpass
00:19:25:%PARSER-6-LI_VIEW_INIT:LI-View initialized.
Router(config-view)# end

! Enter the LI-View; that is, check to see what commands are available within the view.
Router# enable view li-view
Password:

Router#
00:22:57:%PARSER-6-VIEW_SWITCH:successfully set to view 'li-view'.
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# parser view li-view
Router(config-view)# ?
View commands:
  commands  Configure commands for a view
  default   Set a command to its defaults
  exit      Exit from view configuration mode
  name      New LI-View name      ===This option only resides in LI View.
  no        Negate a command or set its defaults
  password  Set a password associated with CLI views

Router(config-view)#

! NOTE:LI View configurations are never shown as part of 'running-configuration'.

! Configure LI Users.
Router(config)# username lawful-intercept li-user1 password li-user1pass
Router(config)# username lawful-intercept li-user2 password li-user2pass

! Displaying LI User information.
Router# show users lawful-intercept

li_admin
li-user1
li-user2
Router#
```

Configuring a Superview: Example

The following sample output from the **show running-config** command shows that “view_one” and “view_two” have been added to superview “su_view1,” and “view_three” and “view_four” have been added to superview “su_view2”:

```
!
parser view su_view1 superview
 secret 5 <encoded password>
 view view_one
 view view_two
!
parser view su_view2 superview
 secret 5 <encoded password>
 view view_three
 view view_four
!
```

Additional References

The following sections provide references related to Role-Based CLI Access.

Related Documents

Related Topic	Document Title
SNMP, MIBs, CLI configuration	The chapter “ Configuring SNMP ” in the <i>Cisco IOS Network Management Configuration Guide</i> .
Privilege levels	The chapter “ Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices ” in the <i>Cisco IOS Security Configuration Guide</i> .

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **commands (view)**
- **enable**
- **li-view**
- **name (view)**
- **parser view**
- **parser view superview**
- **secret**
- **show parser view**
- **show users**
- **username**
- **view**

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)

© 2004, 2007-2008 Cisco Systems, Inc. All rights reserved.



Security with Passwords, Privilege Levels, and Login Usernames for CLI Sessions on Networking Devices



Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices

Cisco IOS based networking devices provide several features that can be used to implement basic security for CLI sessions using only the operating system running on the device. These features include the following:

- Different levels of authorization for CLI sessions to control access to commands that can modify the status of the networking device versus commands that are used to monitor the device
- Assigning passwords to CLI sessions
- Requiring users log in to a networking device with a username
- Changing the privilege levels of commands to create new authorization levels for CLI sessions.

This module is a guide to implementing a baseline level of security for your networking devices. It focuses on the least complex options available for implementing a baseline level of security. If you have networking devices installed in your network with no security options configured, or you are about to install a networking device and you need help understanding the how to implement a baseline of security, this document will help you.

Module History

This module was first published on May 2nd, 2005, and last updated on May 2nd, 2005.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all features. To find information about feature support and configuration, use the [“Feature Information for Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices”](#) section on page 42.

Contents

- [Restrictions for Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices, page 2](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Information About Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices, page 2](#)
- [How To Configure Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices, page 15](#)
- [Configuration Examples for Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices, page 36](#)
- [Where to Go Next, page 39](#)
- [Additional References, page 40](#)
- [Feature Information for Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices, page 42](#)

Restrictions for Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices

Your networking device must not be configured to use any local or remote authentication, authorization, and accounting (AAA) security features. This document describes only the non-AAA security features that can be configured locally on the networking device.

For information how to configure AAA security features that can be run locally on a networking device, or for information on how to configure remote AAA security using TACACS+ or RADIUS servers, see the [Cisco IOS Security Configuration Guide](#), Release 12.4.

Information About Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices

To configure router security with passwords, CLI privilege levels and usernames, you should understand the following concepts:

- [Benefits of Creating a Security Scheme for Your Networking Device, page 3](#)
- [Cisco IOS CLI Modes, page 3](#)
- [Cisco IOS CLI Sessions, page 10](#)
- [Protect Access to Cisco IOS EXEC Modes, page 11](#)
- [Cisco IOS Password Encryption Levels, page 11](#)
- [Cisco IOS CLI Session Usernames, page 13](#)
- [Cisco IOS Privilege Levels, page 13](#)
- [Cisco IOS Password Configuration, page 14](#)

Benefits of Creating a Security Scheme for Your Networking Device

The foundation of a good security scheme in the network is the protection of the user interfaces of the networking devices from unauthorized access. Protecting access to the user interfaces on your networking devices prevents unauthorized users from making configuration changes that can disrupt the stability of your network or compromise your network security.

The Cisco IOS features described in this document can be combined in many different ways to create a unique security scheme for each of your networking devices. Here are some possible examples that you can configure:

- You can enable non administrative users to run a subset of the administrative commands available on the networking device by lowering the entitlement level for the commands to the non administrative privilege level. This can be useful for the following scenarios:
 - ISPs that want their first-line technical support staff to perform tasks such as enabling new interfaces for new customers or resetting the connection for a customer whose connection has stopped passing traffic. See the [“Configuring and Verifying a Networking Device to Allow Non Administrative Users to Shutdown and Enable Interfaces: Example”](#) section on page 38 section for an example of how to do this.
 - When you want your first-line technical support staff to have the ability to clear console port sessions that were disconnected improperly from a terminal server. See the [“Configuring and Verifying a Networking Device to Allow Non Administrative Users to Clear Remote CLI Sessions: Example”](#) section on page 37 section for an example of how to do this.
 - When you want your first-line technical support staff to have the ability to view, but not change, the configuration of a networking device to facilitate troubleshooting a networking problem. See the [“Configuring and Verifying a Networking Device to Allow Non Administrative Users to View the Running Configuration Automatically: Example”](#) section on page 38 section for an example of how to do this.

Cisco IOS CLI Modes

To aid in the configuration of Cisco devices, the Cisco IOS command-line interface is divided into different command modes. Each command mode has its own set of commands available for the configuration, maintenance, and monitoring of router and network operations. The commands available to you at any given time depend on the mode you are in. Entering a question mark (?) at the system prompt (router prompt) allows you to obtain a list of commands available for each command mode.

The use of specific commands allows you to navigate from one command mode to another. The standard order in which a user would access the modes is as follows: user EXEC mode; privileged EXEC mode; global configuration mode; specific configuration modes; configuration submodes; and configuration subsubmodes.



Note

The default configuration of a Cisco IOS software based networking device only allows you to configure passwords to protect access to user EXEC mode (for local, and remote CLI sessions) and privileged EXEC mode. This document describes how you can provide additional levels of security by protecting access to other modes, and commands, using a combination of usernames, passwords and the **privilege** command.

Most EXEC mode commands are one-time commands, such as **show** or **more** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. EXEC mode commands are not saved across reboots of the router.

From privileged EXEC mode, you can enter *global configuration mode*. In this mode, you can enter commands that configure general system characteristics. You also can use global configuration mode to enter specific configuration modes. Configuration modes, including global configuration mode, allow you to make changes to the running configuration. If you later save the configuration, these commands are stored across router reboots.

From global configuration mode you can enter a variety of protocol-specific or feature-specific configuration modes. The CLI hierarchy requires that you enter these specific configuration modes only through global configuration mode. For example, *interface configuration mode*, is a commonly used configuration mode.

From configuration modes, you can enter configuration submodes. Configuration submodes are used for the configuration of specific features within the scope of a given configuration mode. As an example, this chapter describes the *subinterface configuration mode*, a submode of the interface configuration mode.

ROM monitor mode is a separate mode used when the router cannot boot properly. If your system (router, switch, or access server) does not find a valid system image to load when it is booting, the system will enter ROM monitor mode. ROM monitor (ROMMON) mode can also be accessed by interrupting the boot sequence during startup. ROMMON is not covered in this document because it does not have any security features available in it.

The following sections contain detailed information on these command modes:

- [User EXEC Mode](#)
- [Privileged EXEC Mode](#)
- [Global Configuration Mode](#)
- [Interface Configuration Mode](#)
- [Subinterface Configuration Mode](#)

User EXEC Mode

When you start a session on a router, you generally begin in *user EXEC mode*, which is one of two access levels of the EXEC mode. For security purposes, only a limited subset of EXEC commands are available in user EXEC mode. This level of access is reserved for tasks that do not change the configuration of the router, such as determining the router status.

If your device is configured to require users to log-in the log-in process will require a username and a password. You may try three times to enter a password before the connection attempt is refused.

User EXEC mode is set by default to privilege level 1. Privileged EXEC mode is set by default to privilege level 15. For more information see the [“Privileged EXEC Mode” section on page 6](#). When you are logged into a networking device in user EXEC mode your session is running at privilege level 1. By default the EXEC commands at privilege level 1 are a subset of those available at privilege level 15. When you are logged into a networking device in privileged EXEC mode your session is running at privilege level 15. You can move commands to any privilege level between 1 and 15 using the **privilege** command. See the [“Cisco IOS Privilege Levels” section on page 13](#) for more information on privilege levels and the **privilege** command.

In general, the user EXEC commands allow you to connect to remote devices, change terminal line settings on a temporary basis, perform basic tests, and list system information.

To list the available user EXEC commands, use the following command:

Command	Purpose
Router(config)# ?	Lists the user EXEC mode commands

The user EXEC mode prompt consists of the host name of the device followed by an angle bracket (>), as shown in the following example:

```
Router>
```

The default host name is generally `Router`, unless it has been changed during initial configuration using the **setup** EXEC command. You also change the host name using the **hostname** global configuration command.



Note

Examples in Cisco IOS documentation assume the use of the default name of “Router.” Different devices (for example, access servers) may use a different default name. If the routing device (router, access server, or switch) has been named with the **hostname** command, that name will appear as the prompt instead of the default name.

To list the commands available in user EXEC mode, enter a question mark (?) as shown in the following example:

```
Router> ?
Exec commands:
<1-99>          Session number to resume
connect         Open a terminal connection
disconnect      Disconnect an existing telnet session
enable         Turn on privileged commands
exit           Exit from Exec mode
help           Description of the interactive help system
lat            Open a lat connection
lock           Lock the terminal
login          Log in as a particular user
logout         Exit from Exec mode and log out
menu          Start a menu-based user interface
mbranch       Trace multicast route for branch of tree
mrbranch      Trace reverse multicast route to branch of tree
mtrace        Trace multicast route to group
name-connection Name an existing telnet connection
pad           Open a X.29 PAD connection
ping          Send echo messages
resume        Resume an active telnet connection
show          Show running system information
sysstat       Display information about terminal lines
telnet        Open a telnet connection
terminal      Set terminal line parameters
tn3270        Open a tn3270 connection
trace         Trace route to destination
where         List active telnet connections
x3            Set X.3 parameters on PAD
```

The list of commands will vary depending on the software feature set and router platform you are using.



Note

You can enter commands in uppercase, lowercase, or mixed case. Only passwords are case sensitive. However, Cisco IOS documentation convention is to always present commands in lowercase.

Privileged EXEC Mode

In order to have access to all commands, you must enter *privileged EXEC mode*, which is the second level of access for the EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. In privileged EXEC mode, you can enter any EXEC command, because privileged EXEC mode is a superset of the user EXEC mode commands.

Because many privileged EXEC mode commands set operating parameters, privileged EXEC level access should be password protected to prevent unauthorized use. The privileged EXEC command set includes those commands contained in user EXEC mode. Privileged EXEC mode also provides access to configuration modes through the **configure** command, and includes advanced testing commands, such as **debug**.

Privileged EXEC mode is set by default to privilege level 15. User EXEC mode is set by default to privilege level 1. For more information see the [“User EXEC Mode” section on page 4](#). When you are logged into a networking device in privileged EXEC mode your session is running at privilege level 15. When you are logged into a networking device in user EXEC mode your session is running at privilege level 1. By default the EXEC commands at privilege level 15 are a superset of those available at privilege level 1. You can move commands to any privilege level between 1 and 15 using the **privilege** command. See the [“Cisco IOS Privilege Levels” section on page 13](#) for more information on privilege levels and the **privilege** command.

The privileged EXEC mode prompt consists of the host name of the device followed by a pound sign(#), as shown in the following example:

```
Router#
```

To access privileged EXEC mode, use the following command:

Command	Purpose
Router> enable Password Router# exit Router>	Enables privileged EXEC mode. <ul style="list-style-type: none"> If a privileged EXEC mode password has been configured the system will prompt you for a password after you issue the enable command. Use the exit command to leave privileged EXEC mode.



Note

Privileged EXEC mode is sometimes referred to as “enable mode,” because the **enable** command is used to enter the mode.

If a password has been configured on the system, you will be prompted to enter it before being allowed access to privileged EXEC mode. The password is not displayed on the screen and is case sensitive. If an enable password has not been set, privileged EXEC mode can be accessed only by a local CLI session (terminal connected to the console port).

If you attempt to access privileged EXEC mode on a router over a remote connection, such as a telnet connection, and you have not configured a password for privileged EXEC mode you will see the **% No password set** error message. For more information on remote connections see the [“Remote CLI Sessions” section on page 10](#). The system administrator uses the **enable secret** or **enable password** global configuration commands to set the password that restricts access to privileged EXEC mode. For information on configuring a password for privileged EXEC mode, see the [“Protecting Access to Privileged Exec Mode” section on page 20](#).

To return to user EXEC mode, use the following command:

Command	Purpose
Router# disable	Exits from privileged EXEC mode to user EXEC mode.

The following example shows the process of accessing privileged EXEC mode:

```
Router> enable
Password:<letmein>
Router#
```

Note that the password will not be displayed as you type, but is shown here for illustrational purposes. To list the commands available in privileged EXEC mode, issue the **?** command at the prompt. From privileged EXEC mode you can access global configuration mode, which is described in the following section.

**Note**

Because the privileged EXEC command set contains all of the commands available in user EXEC mode, some commands can be entered in either mode. In Cisco IOS documentation, commands that can be entered in either user EXEC mode or privileged EXEC mode are referred to as EXEC mode commands. If user or privileged is not specified in the documentation, assume that you can enter the referenced commands in either mode.

Global Configuration Mode

The term “global” is used to indicate characteristics or features that affect the system as a whole. Global configuration mode is used to configure your system globally, or to enter specific configuration modes to configure specific elements such as interfaces or protocols. Use the **configure terminal** privileged EXEC command to enter global configuration mode.

To access global configuration mode, use the following command in privileged EXEC mode:

Command	Purpose
Router# configure terminal	From privileged EXEC mode, enters global configuration mode.

The following example shows the process of entering global configuration mode from privileged EXEC mode:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Note that the system prompt changes to indicate that you are now in global configuration mode. The prompt for global configuration mode consists of the host-name of the device followed by (config) and the pound sign (#). To list the commands available in privileged EXEC mode, issue the **?** command at the prompt.

Commands entered in global configuration mode update the running configuration file as soon as they are entered. In other words, changes to the configuration take effect each time you press the Enter or Return key at the end of a valid command. However, these changes are not saved into the startup configuration file until you issue the **copy running-config startup-config** EXEC mode command. This behavior is explained in more detail later in this document.

As shown in the example above, the system dialogue prompts you to end your configuration session (exit configuration mode) by pressing the Control (Ctrl) and “z” keys simultaneously; when you press these keys, ^Z is printed to the screen. You can actually end your configuration session by entering the Ctrl-Z key combination, using the **end** command, using the Ctrl-C key combination. The **end** command is the recommended way to indicate to the system that you are done with the current configuration session.



Caution

If you use Ctrl-Z at the end of a command line in which a valid command has been typed, that command will be added to the running configuration file. In other words, using Ctrl-Z is equivalent to hitting the Enter (Carriage Return) key before exiting. For this reason, it is safer to end your configuration session using the **end** command. Alternatively, you can use the Ctrl-C key combination to end your configuration session without sending a Carriage Return signal.

You can also use the **exit** command to return from global configuration mode to EXEC mode, but this only works in global configuration mode. Pressing Ctrl-Z or entering the **end** command will always take you back to EXEC mode regardless of which configuration mode or configuration submode you are in.

To exit global configuration command mode and return to privileged EXEC mode, use one of the following commands:

Command	Purpose
Router(config)# end or Router(config)# ^Z	Ends the current configuration session and returns to privileged EXEC mode.
Router(config)# exit	Exits the current command mode and returns to the preceding mode. For example, exits from global configuration mode to privileged EXEC mode.

From global configuration mode, you can enter a number of protocol-specific, platform-specific, and feature-specific configuration modes.

Interface configuration mode, described in the following section, is an example of a configuration mode you can enter from global configuration mode.

Interface Configuration Mode

One example of a specific configuration mode you enter from global configuration mode is interface configuration mode.

Many features are enabled on a per-interface basis. Interface configuration commands modify the operation of an interface such as an Ethernet, FDDI, or serial port. Interface configuration commands always follow an **interface** global configuration command, which defines the interface type.

For details on interface configuration commands that affect general interface parameters, such as bandwidth or clock rate, refer to the Release 12.2 *Cisco IOS Interface Configuration Guide*. For protocol-specific commands, refer to the appropriate Cisco IOS software command reference.

To access and list the interface configuration commands, use the following command:

Command	Purpose
Router(config)# interface <i>type number</i>	Specifies the interface to be configured, and enters interface configuration mode.

In the following example, the user enters interface configuration mode for serial interface 0. The new prompt, `hostname(config-if)#`, indicates interface configuration mode.

```
Router(config)# interface serial 0
Router(config-if)#
```

To exit interface configuration mode and return to global configuration mode, enter the **exit** command. Configuration submodes are configuration modes entered from other configuration modes (besides global configuration mode). Configuration submodes are for the configuration of specific elements within the configuration mode. One example of a configuration submode is subinterface configuration mode, described in the following section.

Subinterface Configuration Mode

From interface configuration mode, you can enter subinterface configuration mode. Subinterface configuration mode is a submode of interface configuration mode. In subinterface configuration mode you can configure multiple virtual interfaces (called subinterfaces) on a single physical interface. Subinterfaces appear to be distinct physical interfaces to the various protocols.

For detailed information on how to configure subinterfaces, refer to the appropriate documentation module for a specific protocol in the Cisco IOS software documentation set.

To access subinterface configuration mode, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# interface <i>type number</i>	Specifies the virtual interface to be configured and enters subinterface configuration mode.

In the following example, a subinterface is configured for serial line 2, which is configured for Frame Relay encapsulation. The subinterface is identified as “2.1” to indicate that it is subinterface 1 of serial interface 2. The new prompt `hostname(config-subif)#` indicates subinterface configuration mode. The subinterface can be configured to support one or more Frame Relay PVCs.

```
Router(config)# interface serial 2
Router(config-if)# encapsulation frame-relay
Router(config-if)# interface serial 2.1
Router(config-subif)#
```

To exit subinterface configuration mode and return to interface configuration mode, use the **exit** command. To end your configuration session and return to privileged EXEC mode, press Ctrl-Z or enter the **end** command.

Cisco IOS CLI Sessions

This section describes the following concepts:

- [Local CLI Sessions, page 10](#)
- [Remote CLI Sessions, page 10](#)
- [Terminal Lines are Used for Local and Remote CLI Sessions, page 10](#)

Local CLI Sessions

Local CLI sessions require direct access to the console port of the networking device. Local CLI sessions start in user EXEC mode. See the “[Cisco IOS CLI Modes](#)” section on page 3 for more information on the different modes that are supported on your networking device. All of the tasks required to configure and manage a networking device can be done using a local CLI session. The most common method for establishing a local CLI session is to connect the serial port on a PC to the console port of the networking device and then to launch a terminal emulation application on the PC. The type of cable and connectors required and the settings for the terminal emulation application on the PC are dependant on the type of networking device that you are configuring. See to the documentation for your networking device for more information on setting it up for a local CLI session.

Remote CLI Sessions

Remote CLI sessions are created between a host such as a PC and a networking device such as a router over a network using a remote terminal access application such as Telnet and Secure Shell (SSH). Local CLI sessions start in user EXEC mode. See the “[Cisco IOS CLI Modes](#)” section on page 3 for more information on the different modes that are supported on your networking device. Most of the tasks required to configure and manage a networking device can be done using a remote CLI session. The exceptions are tasks that interact directly with the console port (such as recovering from a corrupted operating system (OS) by uploading a new OS image over the console port) and interacting with the networking device when it is in ROM Monitor Mode.

This document explains how to configure security for remote Telnet sessions. Telnet is the most common method for accessing a remote CLI session on a networking device.



Note

SSH is a more secure alternative to Telnet. SSH provides encryption for the session traffic between your local management device such as a PC and the networking device that you are managing. Encrypting the session traffic with SSH prevents hackers that might intercept the traffic from being able to decode it. See [Secure Shell Version 2 Support](#) (http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00802045dc.html) for more information on using SSH.

Terminal Lines are Used for Local and Remote CLI Sessions

Cisco networking devices use the word lines to refer to the software components that manage local and remote CLI sessions. You use the **line console 0** global configuration command to enter line configuration mode to configure options, such as a password, for the console port.

```
Router# configure terminal
Router(config)# line console 0
Router(config-line)# password password-string
```

Remote CLI sessions use lines that are referred to virtual teletypewriter (VTY) lines. You use the **line vty line-number [ending-line-number]** global configuration command to enter line configuration mode to configure options, such as a password, for remote CLI sessions.

```
Router# configure terminal
Router(config)# line vty 0 4
Router(config-line)# password password-string
```

Protect Access to Cisco IOS EXEC Modes

Cisco IOS provides the ability to configure passwords that protect access to the following:

- [Protecting Access to User EXEC Mode, page 11](#)
- [Protecting Access to Privileged EXEC mode, page 11](#)

Protecting Access to User EXEC Mode

The first step in creating a secure environment for your networking device is protecting access to user EXEC mode by configuring passwords for local and remote CLI sessions.

You protect access to user EXEC mode for local CLI sessions by configuring a password on the console port. See the [“Configuring and Verifying a Password for Local CLI Sessions” section on page 18](#).

You protect access to user EXEC mode for remote CLI sessions by configuring a password on the virtual terminal lines (VTYs). See the [“Configuring and Verifying a Password for Remote CLI Sessions” section on page 15](#) for instructions on how to configure passwords for remote CLI sessions.

Protecting Access to Privileged EXEC mode

The second step in creating a secure environment for your networking device is protecting access to privileged EXEC mode with a password. The method for protecting access to privileged EXEC mode is the same for local and remote CLI sessions.

You protect access to privileged EXEC mode by configuring a password for it. This is sometimes referred to as the enable password because the command to enter privileged EXEC mode is **enable**.

Command	Purpose
enable	Enables privileged EXEC mode.
Example: Router> enable Password Router#	<ul style="list-style-type: none">• Enter your password if prompted. The password will not be shown in the terminal window.• The “>” at the end of the prompt string is changed to a “#” to indicate that you are in privileged EXEC mode.

Cisco IOS Password Encryption Levels

Some of the passwords that you configure on your networking device are saved in the configuration in plain text. This means that if you store a copy of the configuration file on a disk, anybody with access to the disk can discover the passwords by reading the configuration file. The following password types are stored as plain text in the configuration by default:

- Console passwords for local CLI sessions
- Virtual terminal line passwords for remote CLI sessions
- Username passwords using the default method for configuring the password
- Privileged EXEC mode password when it is configured with the **enable password** *password* command
- Authentication key chain passwords used by RIPv2 and EIGRP
- BGP passwords for authenticating BGP neighbors
- OSPF authentication keys for authenticating OSPF neighbors
- ISIS passwords for authenticating ISIS neighbors

This excerpt from a router configuration file shows examples of passwords and authentication keys that are stored as clear text.

```
!
enable password 09Jb6D
!
username gjones password 0 kv9sIj3
!
key chain trees
  key 1
    key-string willow
!
interface Ethernet1/0.1
 ip address 172.16.6.1 255.255.255.0
 ip router isis
 ip rip authentication key-chain trees
 ip authentication key-chain eigrp 1 trees
 ip ospf authentication-key j7876
 no snmp trap link-status
 isis password u7865k
!
line vty 0 4
 password v9jA5M
!
```

You can encrypt these clear text passwords in the configuration file by using the **service password-encryption** command. This should be considered only a minimal level of security because the encryption algorithm used by the **service password-encryption** command to encrypt passwords creates text strings that be decrypted using tools that are publicly available. You should still protect access to any electronic or paper copies of your configuration files after you use the **service password-encryption** command.

The **service password-encryption** command does not encrypt the passwords when they are sent to the remote device. Anybody with a network traffic analyzer who has access to you network can capture these passwords from the packets as they are transmitted between the devices. See the [“Configuring Password Encryption for Clear Text Passwords”](#) section on page 22 for more information on encrypting clear text passwords in configuration files.

Many of the Cisco IOS features that use clear text passwords can also be configured to use the more secure MD5 algorithm. The MD5 algorithm creates a text string in the configuration file that is much more difficult to decrypt. The MD5 algorithm does not send the password to the remote device. This prevents people using a traffic analyzer to capture traffic on your network from being able to discover your passwords.

You can determine the type of password encryption that has been used by the number that is stored with the password string in the configuration file of the networking device. The number 5 in the configuration excerpt below indicates that the enable secret password has been encrypted using the MD5 algorithm.

```
!  
enable secret 5 $1$fGCS$rkYbR6.Z8xo4qCl3vghWQ0  
!
```

The number 5 in the excerpt below indicates that the enable password has been encrypted using the less secure algorithm used by the **service password-encryption** command.

```
!  
enable password 7 00081204  
!
```

Cisco IOS CLI Session Usernames

After you have protected access to user EXEC mode and privileged EXEC mode by configuring passwords for them you can further increase the level of security on your networking device by configuring usernames to limit access to CLI sessions to your networking device to specific users.

Usernames that are intended to be used for managing a networking device can be modified with additional options such as:

- Automatically starting a CLI session at a specific privilege level. See [“Configuring and Verifying the Networking Device to Require a Username for the First-Line Technical Support Staff” section on page 30](#).
- Running a CLI command automatically. See [“Configuring and Verifying a Networking Device to Allow Non Administrative Users to View the Running Configuration Automatically: Example” section on page 38](#).

See the [Cisco IOS Security Command Reference](#), Release, 12.4

(http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cr/hsec_r/index.htm) for more information on how to configure the **username** command.

Cisco IOS Privilege Levels

The default configuration for Cisco IOS based networking devices uses privilege level 1 for user EXEC mode and privilege level 15 for privileged EXEC. The commands that can be run in user EXEC mode at privilege level 1 are a subset of the commands that can be run in privileged EXEC mode at privilege 15.

The **privilege** command is used to move commands from one privilege level to another. For example, some ISPs allow their first level technical support staff to enable and disable interfaces to activate new customer connections or to restart a connection that has stopped transmitting traffic. See the [“Configuring and Verifying a Networking Device to Allow Non Administrative Users to Shutdown and Enable Interfaces: Example” section on page 38](#) for an example of how to configure this option.

The **privilege** command can also be used to assign a privilege level to a username so that when a user logs in with the username, the session will run at the privilege level specified by the **privilege** command. For example if you want your technical support staff to view the configuration on a networking device to help them troubleshoot network problems without being able to modify the configuration, you can create a username, configure it with privilege level 15, and configure it to run the **show running-config** command automatically. When a user logs in with the username the running configuration will be displayed automatically. The user’s session will be logged out automatically after the user has viewed the last line of the configuration. See the [“Configuring and Verifying a Networking Device to Allow Non Administrative Users to View the Running Configuration Automatically: Example” section on page 38](#) for an example of how to configure this option.

These command privileges can also be implemented when using AAA with TACACS+ and RADIUS. For example, TACACS+ provides two ways to control the authorization of router commands on a per-user or per-group basis. The first way is to assign privilege levels to commands and have the router verify with the TACACS+ server whether or not the user is authorized at the specified privilege level. The second way is to explicitly specify in the TACACS+ server, on a per-user or per-group basis, the commands that are allowed. For more information about implementing AAA with TACACS+ and RADIUS, see the technical note [How to Assign Privilege Levels with TACACS+ and RADIUS](#).

Cisco IOS Password Configuration

Cisco IOS software does not prompt you to repeat any passwords that you configure to verify that you have entered the passwords exactly as you intended. New passwords, and changes to existing passwords, go into effect immediately after you press the Enter key at the end of a password configuration command string. If you make a mistake when you enter a new password and have saved the configuration on the networking device to its startup configuration file and exited privileged EXEC mode before you realize that you made a mistake, you may find that you are no longer able to manage the device.

The following are common situations that can happen:

- You make a mistake configuring a password for local CLI sessions on the console port.
 - If you have properly configured access to your networking device for remote CLI sessions, you can Telnet to it and reconfigure the password on the console port.
- You make a mistake configuring a password for remote Telnet or SSH sessions.
 - If you have properly configured access to your networking device for local CLI sessions, you can connect a terminal to it and reconfigure the password for the remote CLI sessions.
- You make a mistake configuring a password for privileged EXEC mode (enable password or enable secret password).
 - You will have to perform a lost password recovery procedure.
- You make a mistake configuring your username password, and the networking device requires that you log into it with your username.
 - If you do not have access to another account name, you will have to perform a lost password recovery procedure.

To protect yourself from having to perform a lost password recovery procedure open two CLI sessions to the networking device and keep one of them in privilege EXEC mode while you reset the passwords using the other session. You can use the same device (PC or terminal) to run the two CLI sessions or two different devices. You can use a local CLI session and a remote CLI session or two remote CLI sessions for this procedure. The CLI session that you use to configure the password can also be used to verify that the password was changed properly. The other CLI session that you keep in privileged EXEC mode can be used to change the password again if you made a mistake the first time you configured it.

You should not save password changes that you have made in the running configuration to the startup configuration until you have verified that your password was changed successfully. If you discover that you made a mistake configuring a password, and you were not able to correct the problem using the second CLI session technique described above, you can power cycle the networking device so that it returns to the previous passwords that are stored in the startup configuration.

How To Configure Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices

This section contains the following procedures:

- [Protecting Access to User Exec Mode, page 15](#)
- [Protecting Access to Privileged Exec Mode, page 20](#)
- [Configuring Security Options with Passwords, Privilege Levels and usernames to Manage Access to CLI Sessions and CLI Commands, page 25](#)
- [Recovering from a Lost or Misconfigured Password for Local CLI Sessions, page 33](#)
- [Recovering from a Lost or Misconfigured Password for Remote CLI Sessions, page 34](#)
- [Recovering from a Lost or Misconfigured Passwords for Privileged EXEC Mode, page 35](#)

Protecting Access to User Exec Mode

This section contains the following procedures:

- [Configuring and Verifying a Password for Remote CLI Sessions, page 15](#)
- [Configuring and Verifying a Password for Local CLI Sessions, page 18](#)

Configuring and Verifying a Password for Remote CLI Sessions

This task will assign a password for remote CLI sessions. After you have completed this task the networking device will prompt you for a password the next time that you start a remote CLI session with it.

Cisco IOS based networking devices require that you have a password configured for remote CLI sessions. If you attempt to start a remote CLI session with a device that doesn't have a password configured for remote CLI sessions you will see a message that a password is required and has not been set. The remote CLI session will be terminated by the remote host.

Prerequisites

If you have not previously configured a password for remote CLI sessions, you must perform this task over a local CLI session using a terminal or a PC running a terminal emulation application, attached to the console port.

Your terminal, or terminal emulation application, must be configured with the settings that are used by the console port on the networking device. The console ports on most Cisco networking devices require the following settings: 9600 baud, 8 data bits, 1 stop bit, no parity, and flow control is set to "none." See the documentation for your networking device if these settings do not work for your terminal.

To perform the verification step (Step 6) for this task, your networking device must have an interface that is in an operational state. The interface must have a valid IP address.

Restrictions

If you have not previously configured a password for remote CLI sessions, you must perform this task over a local CLI session using a terminal attached to the console port.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line vty** *line-number* [*ending-line-number*]
4. **password** *password*
5. **end**
6. telnet ip-address
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	line vty <i>line-number</i> [<i>ending-line-number</i>] Example: Router(config)# line vty 0 4	Enters line configuration mode.
Step 4	password <i>password</i> Example: Router(config-line)# password H7x3U8	The argument <i>password</i> is a character string that specifies the line password. The following rules apply to the <i>password</i> argument: <ul style="list-style-type: none"> The first character cannot be a number. The string can contain any alphanumeric characters, including spaces, up to 80 characters. You cannot specify the password in the format number-space-anything. Passwords are case sensitive.
Step 5	end Example: Router(config-line)# end	Exits the current configuration mode and returns to privileged EXEC mode.
Step 6	telnet <i>ip-address</i> Example: Router# telnet 172.16.1.1	Start a remote CLI session with the networking device from your current CLI session using the IP address of an interface in the networking device that is in an operational state (interface up, line protocol up). <ul style="list-style-type: none"> Enter the password that you configured in step 4 when prompted. <p>Note This procedure is often referred to as starting a recursive Telnet session because you are initiating a remote Telnet session with the networking device from the networking device itself.</p>
Step 7	exit	Terminates the remote CLI session (recursive Telnet session) with the networking device.

Troubleshooting Tips

Repeat this task if you made a mistake configuring the remote CLI session password.

What to Do Next

Proceed to the [“Configuring and Verifying a Password for Local CLI Sessions”](#) section on page 18 .

Configuring and Verifying a Password for Local CLI Sessions

This task will assign a password for local CLI sessions over the console port. After you have completed this task, the networking device will prompt you for a password the next time that you start a local CLI session on the console port.

This task can be performed over a local CLI session using the console port or a remote CLI session. If you want to perform the optional step of verifying that you configured the password correctly you should perform this task using a local CLI session using the console port.

Prerequisites

If you want to perform the optional step of verifying the local CLI session password, you must perform this task using a local CLI session. You must have a terminal or a PC running a terminal emulation program, connected to the console port of the networking device. Your terminal must be configured with the settings that are used by the console port on the networking device. The console ports on most Cisco networking devices require the following settings: 9600 baud, 8 data bits, 1 stop bit, no parity, and flow control is set to "none." See the documentation for your networking device if these settings do not work for your terminal.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line console 0**
4. **password *password***
5. **end**
6. **exit**
7. Press the Enter key, and enter the password from Step 4 when prompted.

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	line console 0 Example: Router(config)# line console 0	Enters line configuration mode and selects the console port as the line that you are configuring.
Step 4	password password Example: Router(config-line)# password Ji8F5Z	The argument <i>password</i> is a character string that specifies the line password. The following rules apply to the <i>password</i> argument: <ul style="list-style-type: none"> The first character cannot be a number. The string can contain any alphanumeric characters, including spaces, up to 80 characters. You cannot specify the password in the format number-space-anything. Passwords are case sensitive.
Step 5	end Example: Router(config-line)# end	Exits the current configuration mode and returns to privileged EXEC mode.
Step 6	exit Example: Router# exit	Exits privileged EXEC mode.
Step 7	Press the Enter key.	(Optional) Initiates the local CLI session on the console port. <ul style="list-style-type: none"> Enter the password that you configured in step 4 when prompted to verify that it was configured correctly. Note This step can be performed only if you are using a local CLI session to perform this task.

Troubleshooting Tips

If your new password is not accepted proceed to the [“Recovering from a Lost or Misconfigured Password for Local CLI Sessions”](#) section on page 33 for instructions on what to do next.

What to Do Next

Proceed to the [“Protecting Access to Privileged Exec Mode”](#) section on page 20.

Protecting Access to Privileged Exec Mode

This section contains the following procedures:

- [Configuring and Verifying the Enable Password, page 20](#) (optional)
- [Configuring Password Encryption for Clear Text Passwords, page 22](#) (optional)
- [Configuring and Verifying the Enable Secret Password, page 23](#) (recommended)

Configuring and Verifying the Enable Password

Cisco no longer recommends that you use the **enable password** command to configure a password for privileged EXEC mode. The password that you enter with the **enable password** command is stored as plain text in the configuration file of the networking device. You can encrypt the password for the **enable password** command in the configuration file of the networking device using the **service password-encryption** command. However the encryption level used by the **service password-encryption** command can be decrypted using tools available on the Internet.

Instead of using the **enable password** command, Cisco recommends using the **enable secret** command because it encrypts the password that you configure with it with strong encryption . For more information on password encryption issues see the [“Cisco IOS Password Encryption Levels” section on page 11](#). For information on configuring the **enable secret** command see the [“Configuring and Verifying the Enable Secret Password” section on page 23](#).

Restrictions

The networking device must not have a password configured by the **enable secret** command in order to perform this task successfully. If you have already configured a password for privileged EXEC mode using the **enable secret** command, the password configured takes precedences over the password that you configure in this task using the **enable password** command.

You cannot use the same password for the **enable secret** command and the **enable password** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **enable password** *password*
4. **end**
5. **exit**
6. **enable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	enable password password Example: Router(config)# enable password t6D77CdKq	The argument <i>password</i> is a character string that specifies the enable password. The following rules apply to the <i>password</i> argument: <ul style="list-style-type: none"> Must contain from 1 to 25 uppercase and lowercase alphanumeric characters. Must not have a number as the first character. Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized. Can contain the question mark (?) character if you precede the question mark with the key combination Ctrl-v when you create the password; for example, to create the password abc?123, do the following: <ul style="list-style-type: none"> Enter abc Type Ctrl-v Enter ?123
Step 4	end Example: Router(config)# end	Exits the current configuration mode and returns to privileged EXEC mode.
Step 5	exit Example: Router# exit	Exits privileged EXEC mode.
Step 6	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter the password you configured in step 3.

Troubleshooting Tips

If your new password is not accepted, proceed to the [“Recovering from a Lost or Misconfigured Passwords for Privileged EXEC Mode”](#) section on page 35 for instructions on what to do next.

What to Do Next

Encrypt the clear text enable password in the configuration file of the networking device using the procedure described in [“Configuring Password Encryption for Clear Text Passwords” section on page 22](#).

Configuring Password Encryption for Clear Text Passwords

Cisco IOS stores passwords in clear text in network device configuration files for several features such as passwords for local and remote CLI sessions, and passwords for neighbor authentication for routing protocols. Clear text passwords are a security risk because anybody with access to archived copies of the configuration files can discover the passwords that are stored as clear text. The **service password-encryption** command can be used to encrypt clear text commands in the configuration files of networking devices. See the [“Cisco IOS Password Encryption Levels” section on page 11](#) for more information.

Perform the following steps to configure password encryption for passwords that are stored as clear text in the configuration files of your networking device.

Prerequisites

You must have at least one feature that uses clear text passwords configured on your networking device for this command to have any immediate effect.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service password-encryption**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	service password-encryption Example: Router(config)# service password-encryption	Enables Password encryption for all passwords clear text passwords, including username passwords, authentication key passwords, the privileged command password, console and virtual terminal line access passwords, and Border Gateway Protocol neighbor passwords.
Step 4	end Example: Router(config)# end	Exits the current configuration mode and returns to privileged EXEC mode.

Configuring and Verifying the Enable Secret Password

Cisco recommends that you use the **enable secret** command, instead of the **enable password** command to configure a password for privileged EXEC mode. The password created by the **enable secret** command is encrypted with the more secure MD5 algorithm.

Restrictions

You cannot use the same password for the **enable secret** command and the **enable password** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **enable secret** *password*
or
enable secret *5 previously-encrypted-password*
4. **end**
5. **exit**
6. **enable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	enable secret password or enable secret 5 previously-encrypted-password Example: Router(config)# enable secret t6D77CdKq or Example: Router(config)# enable secret 5 \$1\$/x6H\$RhndI3yLC4GA01aJnHLQ4/	<p>The argument <i>password</i> is a character string that specifies the enable secret password. The following rules apply to the <i>password</i> argument:</p> <ul style="list-style-type: none"> Must contain from 1 to 25 uppercase and lowercase alphanumeric characters. Must not have a number as the first character. Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized. Can contain the question mark (?) character if you precede the question mark with the key combination Ctrl-v when you create the password; for example, to create the password abc?123, do the following: <ul style="list-style-type: none"> Enter abc Type Ctrl-v Enter ?123 <p>or</p> <p>Sets a previously encrypted password for privileged EXEC mode by entering the number 5 before the previously encrypted string. You must enter an exact copy of a password from a configuration file that was previously encrypted by the enable secret command to use this method.</p>
Step 4	end Example: Router(config)# end	Exits the current configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 5	exit Example: Router# exit	Exits privileged EXEC mode.
Step 6	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter the password that you configured in Step 3.

Troubleshooting Tips

If your new password is not accepted proceed to the [“Recovering from a Lost or Misconfigured Passwords for Privileged EXEC Mode”](#) section on page 35 for instructions on what to do next.

What to Do Next

If you have finished configuring passwords for local and remote CLI sessions and you want to configure additional security features, such as usernames, and privilege levels proceed to the [“Configuring Security Options with Passwords, Privilege Levels and usernames to Manage Access to CLI Sessions and CLI Commands”](#) section on page 25.

Configuring Security Options with Passwords, Privilege Levels and usernames to Manage Access to CLI Sessions and CLI Commands

The tasks in this section describe how to configure your networking device to permit the use of a subset of privileged EXEC mode commands by users who should not have access to all of the commands available in privileged EXEC mode.

These tasks are beneficial for companies that have multiple levels of network support staff and the company wants the staff at each level to have access to a different subset of the privileged EXEC mode commands.

In this task the users who should not have access to all of the commands available in privileged EXEC mode are referred to as the first-line technical support staff.

This section contains the following procedures:

- [Configuring the Networking Device for the First-Line Technical Support Staff, page 25](#)
- [Verifying the Configuration for the First-Line Technical Support Staff, page 28](#)
- [Configuring and Verifying the Networking Device to Require a Username for the First-Line Technical Support Staff, page 30](#)

Configuring the Networking Device for the First-Line Technical Support Staff

This task describes how to configure the networking device for first-line technical support users. First-line technical support staff are usually not allowed to run all of the commands available in privileged EXEC mode (privilege level 15) on a networking device. They are prevented from running commands that they are not authorized for by not being granted access to the password assigned to privileged EXEC mode or to other roles that have been configured on the networking device.

The **privilege** command is used to move commands from one privilege level to another in order to create the additional levels of administration of a networking device that is required by companies that have different levels of network support staff with different skill levels.

The default configuration of a Cisco IOS device permits two types of users to access the CLI. The first type of user is a person who is only allowed to access user EXEC mode. The second type of user is a person who is allowed access to privileged EXEC mode. A user who is only allowed to access user EXEC mode is not allowed to view or change the configuration of the networking device, or to make any changes to the operational status of the networking device. On the other hand, a user who is allowed access to privileged EXEC mode can make any change to a networking device that is allowed by the CLI.

In this task the two commands that normally run at privilege level 15 are reset to privilege level 7 using the **privilege** command in order that first-line technical support users will be allowed to run the two commands. The two commands for which the privilege levels will be reset are the **clear counters** command and **reload** command.

- The **clear counters** command is used to reset the counter fields on interfaces for statistics such as packets received, packets transmitted, and errors. When a first-line technical support user is troubleshooting an interface related connectivity issue between networking devices, or with remote users connecting to the network, it is useful to reset the interface statistics to zero and then monitor the interfaces for a period of time to see if the values in the interface statistics counters change.
- The **reload** command is used to initiate a reboot sequence for the networking device. One common use of the reload command by first-line technical support staff is to cause the networking device to reboot during a maintenance window so that it loads a new operating system that was previously copied onto the networking device's file system by a user with a higher level of authority.

Any user that is permitted to know the **enable secret** password that is assigned to the first-line technical support user role privilege level can access the networking device as a first-line technical support user. You can add an additional level of security by configuring a username on the networking device and requiring that the users know the username and the password. Configuring a username as an additional level of security is described in the [“Configuring and Verifying the Networking Device to Require a Username for the First-Line Technical Support Staff”](#) section on page 30.

Privilege Command Enhancement

Before Cisco IOS Releases 12.0(22)S and 12.2(13)T, each command in a privilege level had to be specified with a separate **privilege** command. In Cisco IOS Releases 12.0(22)S, 12.2(13)T, and later releases, a “wildcard” option specified by the new keyword **all** was introduced that allows you to configure access to multiple commands with only one **privilege** command. By using the new **all** keyword, you can specify a privilege level for all commands which begin with the string you enter. In other words, the **all** keyword allows you to grant access to all command-line options and suboptions for a specified command.

For example, if you wanted to create a privilege level to allow users to configure all commands which begin with **service-module t1** (such as **service-module t1 linecode** or **service-module t1 clock source**) you can use the **privilege interface all level 2 service-module t1** command instead of having to specify each **service-module t1** command separately.

If the command specified in the privilege command (used with the **all** keyword) enables a configuration submode, all commands in the submode of that command will also be set to the specified privilege level.

Restrictions

The **all** “wildcard” keyword option for the **privilege** command is not supported in versions of Cisco IOS software prior to Cisco IOS Releases 12.0(22)S and, 12.2(13)T.

You must not have the **aaa new-model** command enabled on the networking device. You must not have the **login local** command configured for the local CLI sessions over the console port or the remote CLI sessions.

**Note**

For clarity, only the arguments and keywords that are relevant for each step are shown in the syntax for the steps in this task. See the Cisco IOS command reference book for your Cisco IOS release for further information on the additional arguments and keywords that can be used with these commands.

**Caution**

Do not use the **no** form of the **privilege** command to reset the privilege level of a command to its default because it might not return the configuration to the correct default state. Use the **reset** keyword for the **privilege** command instead to return a command to its default privilege level. For example, to remove the **privilege exec level reload** command from the configuration and return the **reload** command to its default privilege of 15, use the **privilege exec reset reload** command.

SUMMARY STEPS

1. **enable** *password*
2. **configure terminal**
3. **enable secret level** *level password*
4. **privilege exec level** *level command-string*
5. **privilege exec all level** *level command-string*
6. **end**

DETAILED STEPS

- | | |
|---------------|---|
| Step 1 | enable <i>password</i>
Enters privileged EXEC mode. Enter the password when prompted.
Router> enable |
| Step 2 | configure terminal
Enters global configuration mode.
Router# configure terminal |
| Step 3 | enable secret level <i>level password</i>
Configures a new enable secret password for privilege level 7.
Router(config)# enable secret level 7 Zy72sKj |
| Step 4 | privilege exec level <i>level command-string</i>
Changes the privilege level of the clear counters command from privilege level 15 to privilege level 7.
Router(config)# privilege exec level 7 clear counters |
| Step 5 | privilege exec all level <i>level command-string</i>
Changes the privilege level of the reload command from privilege level 15 to privilege level 7.
Router(config)# privilege exec all level 7 reload |

Step 6 **end**

Exits global configuration mode.

```
Router(config)# end
```

Verifying the Configuration for the First-Line Technical Support Staff

This task describes how to verify that the network device is configured correctly for the first-line technical support staff.

Prerequisites

The following commands must have been modified to run at privilege level 7 for this task:

- **clear counters**
- **reload**

SUMMARY STEPS

1. **enable level password**
2. **show privilege**
3. **clear counters**
4. **clear ip route ***
5. **reload in time**
6. **reload cancel**
7. **disable**
8. **show privilege**

DETAILED STEPS

Step 1 **enable level password**

Logs the user into the networking device at the privilege level specified for the level argument.

```
Router> enable 7 Zy72sKj
```

Step 2 **show privilege**

Displays the privilege level of the current CLI session

```
Router# show privilege
Current privilege level is 7
```

Step 3 **clear counters**

The clear counters command clears the interface counters. This command has been changed from privilege level 15 to privilege level 7.

```
Router# clear counters
Clear "show interface" counters on all interfaces [confirm]
Router#
02:41:37: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console
```

Step 4 **clear ip route ***

The *ip route* argument string for the **clear** command should not be allowed because it was not changed from privilege level 15 to privilege level 7.

```
Router# clear ip route *
      ^
% Invalid input detected at '^' marker.

Router#
```

Step 5 **reload in time**

The **reload** command causes the networking device to reboot.

```
Router# reload in 10
Reload scheduled in 10 minutes by console
Proceed with reload? [confirm]
Router#

***
*** --- SHUTDOWN in 0:10:00 ---
***

02:59:50: %SYS-5-SCHEDULED_RELOAD: Reload requested for 23:08:30 PST Sun Mar 20
```

Step 6 **reload cancel**

The **reload cancel** terminates a reload that was previously setup with the the **reload in time** command.

```
Router# reload cancel

***
*** --- SHUTDOWN ABORTED ---
***

04:34:08: %SYS-5-SCHEDULED_RELOAD_CANCELLED: Scheduled reload cancelled at 15:38:46 PST
Sun Mar 27 2005
```

Step 7 **disable**

Exits the current privilege level and returns to privilege level 1.

```
Router# disable
```

Step 8 **show privilege**

Displays the privilege level of the current CLI session

```
Router> show privilege
Current privilege level is 1
```

Troubleshooting Tips

If your configuration does not work the way that you want it to and you want to remove the privilege commands from the configuration, use the **reset** keyword for the **privilege** command to return the commands to their default privilege level. For example, to remove the command **privilege exec level reload** command from the configuration and return the **reload** command to its default privilege of 15 use the **privilege exec reset reload** command.

What to Do Next

If you want to add an additional level of security by requiring that the first level technical staff use a login name, proceed to the [“Configuring and Verifying the Networking Device to Require a Username for the First-Line Technical Support Staff”](#) section on page 30.

Configuring and Verifying the Networking Device to Require a Username for the First-Line Technical Support Staff

This task configures the networking device to require that the first-line technical support staff login to the networking device with a login name of admin. The admin username configured in this task is assigned the privilege level 0f 7 which will allow users who log in with this name to run the commands that were reassigned to privilege level 7 in the previous task. When a user successfully logs in with the admin username, the CLI session will automatically enter privilege level 7.

Enhanced Username Password Security

Before Cisco IOS Releases 12.0(18)S and 12.2(8)T, two types of passwords were associated with usernames: Type 0, which is a clear text password visible to any user who has access to privileged mode on the router, and type 7, which has a password encrypted by the **service password encryption** command.

In Cisco IOS Releases 12.0(18)S, 12.2(8)T, and later releases, the new **secret** keyword for the **username** command allows you to configure Message Digest 5 (MD5) encryption for username passwords.

Prerequisites

The following commands must have been modified to run at privilege level 7 for this task:

- **clear counters**
- **reload**

See the [“Configuring the Networking Device for the First-Line Technical Support Staff”](#) section on page 25 for instructions on how to change the privilege level for a command.

Restrictions

MD5 encryption for the **username** command is not supported in versions of Cisco IOS software prior to Cisco IOS Releases 12.0(18)S and 12.2(8)T.

You must not have the **aaa-new model** command enabled on the networking device. You must not have the **login local** command configured for the local CLI sessions over the console port or the remote CLI sessions.



Note

For clarity, only the arguments and keywords that are relevant for each step are shown in the syntax for the steps in this task. Refer to the Cisco IOS command reference book for your Cisco IOS release for further information on the additional arguments and keywords that can be used with these commands.

SUMMARY STEPS

1. **enable password**
2. **configure terminal**

3. **username** *username* **privilege** *level* **secret** *password*
4. **end**
5. **disable**
6. **login** *username* *password*
7. **show privilege**
8. **clear counters**
9. **clear ip route ***
10. **reload in 10**
11. **reload cancel**
12. **disable**
13. **show privilege**

DETAILED STEPS

Step 1 **enable** *t6D77CdKq*

Enters privileged EXEC mode. Enter the password when prompted.

Router> **enable**

Step 2 **configure terminal**

Enters global configuration mode.

Router# **configure terminal**

Step 3 **username** *username* **privilege** *level* **secret** *password*

Creates a username and applies MD5 encryption to the *password* text string.

Router(config)# **username** *admin* **privilege** 7 **secret** *Kd65xZa*

Step 4 **end**

Exits global configuration mode.

Router(config)# **end**

Step 5 **disable**

Exits the current privilege level and returns to user EXEC mode.

Router# **disable**

Step 6 **login** *username*

Logs in the user. Enter the username and password you configured in step 3 when prompted.

Router> **login** *admin*

Step 7 **show privilege**

The **show privilege** command displays the privilege level of the CLI session.

Router# **show privilege**

Current privilege level is 7

Step 8 **clear counters**

The **clear counters** command clears the interface counters. This command has been changed from privilege level 15 to privilege level 7.

```
Router# clear counters
Clear "show interface" counters on all interfaces [confirm]
Router#
02:41:37: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console
```

Step 9 **clear ip route ***

The *ip route* argument string for the **clear** command is not allowed because it was not changed from privilege level 15 to privilege level 7.

```
Router# clear ip route *
          ^
% Invalid input detected at '^' marker.

Router#
```

Step 10 **reload in time**

The reload command causes the networking device to reboot.

```
Router# reload in 10
Reload scheduled in 10 minutes by console
Proceed with reload? [confirm]
Router#

***
*** --- SHUTDOWN in 0:10:00 ---
***

02:59:50: %SYS-5-SCHEDULED_RELOAD: Reload requested for 23:08:30 PST Sun Mar 20
```

Step 11 **reload cancel**

The **reload cancel** command terminates a reload that was previously setup with the the **reload in time** command.

```
Router# reload cancel

***
*** --- SHUTDOWN ABORTED ---
***

04:34:08: %SYS-5-SCHEDULED_RELOAD_CANCELLED: Scheduled reload cancelled at 15:38:46 PST
Sun Mar 27 2005
```

Step 12 **disable**

Exits the current privilege level and returns to user EXEC mode.

```
Router# disable
```

Step 13 **show privilege**

Displays the privilege level of the current CLI session

```
Router> show privilege
Current privilege level is 1
```

Recovering from a Lost or Misconfigured Password for Local CLI Sessions

There are three methods that can be used to recover from a lost or misconfigured password for local CLI sessions over console port. The method that you will use depends on the current configuration of your networking device.

- [Networking Device Is Configured to Allow Remote CLI Sessions, page 33](#)
- [Networking Device Is Not Configured to Allow Remote CLI Sessions and the Local CLI Session Password Has Not Been Saved to the Startup Configuration File, page 33](#)
- [Networking Device is not Configured to Allow Remote CLI Sessions and the Local CLI Session Password Has Been Saved to the Startup Configuration File, page 33](#)

Networking Device Is Configured to Allow Remote CLI Sessions

The fastest method to recover from a lost, or misconfigured password for local CLI sessions is to establish a remote CLI session with the networking device and repeat the “[Configuring and Verifying a Password for Local CLI Sessions](#)” section on [page 18](#). Your networking device must be configured to allow remote CLI sessions and you must know the remote CLI session password to perform this procedure.

Networking Device Is Not Configured to Allow Remote CLI Sessions and the Local CLI Session Password Has Not Been Saved to the Startup Configuration File

If you cannot establish a remote session to your networking device, and you have not saved the misconfigured local CLI session password to the startup configuration, you can restart the networking device. When the networking device starts up again it will read the startup configuration file. The previous local CLI session password is restored.

**Caution**

Restarting a networking device will cause it to stop forwarding traffic. This will also cause an interruption in any services that are running on the networking device, such as a DHCP server service, to stop. You should only restart a networking device during a period of time that has been allocated for network maintenance.

Networking Device is not Configured to Allow Remote CLI Sessions and the Local CLI Session Password Has Been Saved to the Startup Configuration File

If you can not establish a remote CLI session with the networking device, and you have saved the misconfigured local CLI session password to the startup configuration, or you have lost the local CLI session password, you must perform a password recovery procedure. Password recovery procedures are device specific. You must locate the document that describes the procedure for your type of networking device.

There are three methods for locating a password recovery procedure document for your networking device:

- Many networking devices have a Password Recovery subsection in the Troubleshoot and Alerts section of their product support page on Cisco’s Technical Support website (<http://www.cisco.com/tac>). Navigate to the Troubleshoot and Alerts section of the product support page for your networking device and look for the Password Recovery subsection.

- If you do not find the password recovery document for your networking device on its product support page try searching for the text string **“password recovery”** on Cisco’s Technical Support website (<http://www.cisco.com/tac>). Enclose the text string in double quotes. You can improve the search results by adding an additional text string that matches the model number, series number or platform name for your networking device, For example searching on the string **“password recovery” 12000** will provide search results that give documents with the words **password**, **recovery** and **12000** in the title a higher ranking.
- If the product support page for your networking device does not have a password recovery document, and you can not find the correct document by searching for it, you can try the Cisco’s Network Professionals Connection (<http://www.cisco.com/go/netpro>).

Recovering from a Lost or Misconfigured Password for Remote CLI Sessions

There are three methods that can be used to recover from a lost, or misconfigured remote CLI session password. The method that you will use depends on the current configuration of your networking device.

- [Networking Device Is Configured to Allow Local CLI Sessions, page 34](#)
- [Networking Device Is Not Configured to Allow Local CLI Sessions and the Remote CLI Session Password Has Not Been Saved to the Startup Configuration File, page 34](#)
- [Networking Device Is Not Configured to Allow Local CLI Sessions and the Remote CLI Session Password Has Been Saved to the Startup Configuration File, page 35](#)

Networking Device Is Configured to Allow Local CLI Sessions

The fastest method to recover from a lost, or misconfigured password for remote CLI sessions is to establish a local CLI session with the networking device and repeat the [“Configuring and Verifying a Password for Remote CLI Sessions” section on page 15](#). Your networking device must be configured to allow local CLI sessions and you must know the local CLI session password to perform this procedure.

Networking Device Is Not Configured to Allow Local CLI Sessions and the Remote CLI Session Password Has Not Been Saved to the Startup Configuration File

If you cannot establish a local CLI session to your networking device, and you have not saved the misconfigured remote CLI session password to the startup configuration, you can restart the networking device. When the networking device starts up again it will read the startup configuration file. The previous remote CLI session password is restored.



Caution

Restarting a networking device will cause it to stop forwarding traffic. This will also cause an interruption in any services that are running on the networking device, such as a DHCP server service, to stop. You should only restart a networking device during a period of time that has been allocated for network maintenance.

Networking Device Is Not Configured to Allow Local CLI Sessions and the Remote CLI Session Password Has Been Saved to the Startup Configuration File

If you can not establish a local CLI session with the networking device, and you have saved the misconfigured remote CLI session password to the startup configuration, or you have lost the remote CLI session password, you must perform a password recovery procedure. Password recovery procedures are device specific. You must locate the document that describes the procedure for your type of networking device.

There are three methods for locating a password recovery procedure document for your networking device:

- Many networking devices have a Password Recovery subsection in the Troubleshoot and Alerts section of their product support page on Cisco's Technical Support website (<http://www.cisco.com/tac>). Navigate to the Troubleshoot and Alerts section of the product support page for your networking device and look for the Password Recovery subsection.
- If you do not find the password recovery document for your networking device on its product support page try searching for the text string **"password recovery"** on Cisco's Technical Support website (<http://www.cisco.com/tac>). Enclose the text string in double quotes. You can improve the search results by adding an additional text string that matches the model number, series number or platform name for your networking device. For example searching on the string **"password recovery" 12000** will provide search results that give documents with the words **password**, **recovery** and **12000** in the title a higher ranking.
- If the product support page for your networking device does not have a password recovery document, and you can not find the correct document by searching for it, you can try the Cisco's Network Professionals Connection (<http://www.cisco.com/go/netpro>).

Recovering from a Lost or Misconfigured Passwords for Privileged EXEC Mode

There are two methods that can be used to recover from a lost, or misconfigured Privileged EXEC Mode password. The method that you will use depends on the current configuration of your networking device.

- [A Misconfigured Privileged EXEC Mode Password Has Not Been Saved to the Startup Configuration File, page 35](#)
- [A Misconfigured Privileged EXEC Mode Password Has Been Saved to the Startup Configuration File, or the Privileged EXEC Mode Password Has Been Lost, page 36](#)

A Misconfigured Privileged EXEC Mode Password Has Not Been Saved to the Startup Configuration File

If you have not saved the misconfigured privileged EXEC mode password to the startup configuration, you can restart the networking device. When the networking device starts up again it will read the startup configuration file. The previous privileged EXEC mode password is restored.



Caution

Restarting a networking device will cause it to stop forwarding traffic. This will also cause an interruption in any services that are running on the networking device, such as a DHCP server service, to stop. You should only restart a networking device during a period of time that has been allocated for network maintenance.

A Misconfigured Privileged EXEC Mode Password Has Been Saved to the Startup Configuration File, or the Privileged EXEC Mode Password Has Been Lost

If you have saved the misconfigured privileged EXEC mode password to the startup configuration, or you have lost the privileged EXEC mode password, you must perform a password recovery procedure. Password recovery procedures are device specific. You must locate the document that describes the procedure for your type of networking device.

There are three methods for locating a password recovery procedure document for your networking device:

- Many networking devices have a Password Recovery subsection in the Troubleshoot and Alerts section of their product support page on Cisco's Technical Support website (<http://www.cisco.com/tac>). Navigate to the Troubleshoot and Alerts section of the product support page for your networking device and look for the Password Recovery subsection.
- If you do not find the password recovery document for your networking device on its product support page try searching for the text string **"password recovery"** on Cisco's Technical Support website (<http://www.cisco.com/tac>). Enclose the text string in double quotes. You can improve the search results by adding an additional text string that matches the model number, series number or platform name for your networking device. For example searching on the string **"password recovery" 12000** will provide search results that give documents with the words **password, recovery** and **12000** in the title a higher ranking.
- If the product support page for your networking device does not have a password recovery document, and you can not find the correct document by searching for it, you can try the Cisco's Network Professionals Connection (<http://www.cisco.com/go/netpro>).

Configuration Examples for Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices

This section contains the following configuration examples:

- [Configuring and Verifying a Networking Device to Allow Non Administrative Users to Clear Remote CLI Sessions: Example, page 37](#)
- [Configuring and Verifying a Networking Device to Allow Non Administrative Users to View the Running Configuration Automatically: Example, page 38](#)
- [Configuring and Verifying a Networking Device to Allow Non Administrative Users to Shutdown and Enable Interfaces: Example, page 38](#)

Configuring and Verifying a Networking Device to Allow Non Administrative Users to Clear Remote CLI Sessions: Example

The following example shows how to configure a networking device to allow a non administrative user to clear remote CLI session virtual terminal (VTY) lines.

The first section is an excerpt of the running configuration for this example. The following sections show you how this example is used.

The following section is an excerpt of the running-configuration:

```
!
privilege exec level 7 clear line
!
no aaa new-model
!
!
username admin privilege 7 secret 5 $1$tmIw$1aM7sadKhWMpkVTzxNw1J.
!
privilege exec level 7 clear line
!
! the privilege exec level 7 clear command below is entered automatically
! when you enter the privilege exec level 7 clear line command above, do
! not enter it again
!
privilege exec level 7 clear
!
```

The following section using the **login** command shows the user logging in to the networking device with the username of admin:

```
R1> login
Username: admin
Password:
```

The following section using the **show privilege** command shows that the current privilege level is 7:

```
R1# show privilege
Current privilege level is 7
R1#
```

The following section using the **show user** command shows that two users (admin and root) are currently logged in to the networking device:

```
R1# show user
```

	Line	User	Host(s)	Idle	Location
*	0 con 0	admin	idle	00:00:00	
	2 vty 0	root	idle	00:00:17	172.16.6.2

Interface	User	Mode	Idle	Peer Address
-----------	------	------	------	--------------

The following section using the **clear line 2** command terminates the remote CLI session in use by the username root:

```
R1# clear line 2
[confirm]
[OK]
```

The following section using the **show user** command shows that admin is the only user currently logged in to the networking device:


```

R1# show user
      Line      User      Host(s)      Idle      Location
*   0 con 0      admin      idle        00:00:00

      Interface      User      Mode      Idle      Peer Address

```

Configuring and Verifying a Networking Device to Allow Non Administrative Users to View the Running Configuration Automatically: Example

The following example shows how to configure the networking device to allow a non administrative users (no access to privileged EXEC mode) to view the running configuration automatically. This example requires that the username is configured for privilege level 15 because many of the commands in the configuration file can be viewed only by users who have access to privilege level 15.

The solution is to temporarily allow the user access to privilege level 15 while running the **show running-config** command and then terminating the CLI session when the end of the configuration file has been viewed. In this example the networking device will automatically terminate the CLI session when the end of the configuration file has been viewed. No further configuration steps are required.



Caution

You must include the **noescape** keyword for the **username** command to prevent the user from entering an escape character that will terminate viewing the configuration file and leave the session running at privilege level 15.

```

!
!
username viewconf privilege 15 noescape secret 5 $1$zA9C$TDWD/Q0zwp/5xRwRqdgc/.
username viewconf autocommand show running-config
!

```

Configuring and Verifying a Networking Device to Allow Non Administrative Users to Shutdown and Enable Interfaces: Example

The following example shows how to configure a networking device to allow non administrative users to shutdown and enable interfaces.

The first section is an excerpt of the running configuration for this example. The following sections show you how this example is used.

The following section is an excerpt of the running-configuration:

```

!
no aaa new-model
!
username admin privilege 7 secret 5 $1$tmIw$1aM7sadKhWmpkVTzxNw1J.
!
privilege interface all level 7 shutdown
privilege interface all level 7 no shutdown
privilege configure level 7 interface
privilege exec level 7 configure terminal
!
! the privilege exec level 7 configure command below is entered automatically
! when you enter the privilege exec level 7 configure terminal command above, do
! not enter it again
!

```

```
privilege exec level 7 configure
!
```

The following section using the **login** command shows the user logging in to the networking device with the username of admin:

```
R1> login
Username: admin
Password:
```

The following section using the **show privilege** command shows that the current privilege level is 7:

```
R1# show privilege
Current privilege level is 7
R1#
```

The following section using the **show user** command shows that admin is the only user currently logged in to the networking device:

```
R1# show user
```

Line	User	Host(s)	Idle	Location
* 0 con 0	admin	idle	00:00:00	

Interface	User	Mode	Idle	Peer Address
-----------	------	------	------	--------------

The following section shows that the admin user is permitted to shutdown and enable an interface:

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# interface ethernet 1/0
R1(config-if)# shutdown
R1(config-if)# no shutdown
R1(config-if)# exit
R1#
```

Where to Go Next

Once you have established a baseline of security for your networking devices you can consider more advanced options such as:

- **Role-Based CLI Access**—The role-based CLI access feature offers a more comprehensive set of options than the **privilege** command (described in this document) for network managers who want to allow different levels of technical support staff to have different levels of access to CLI commands.
- **AAA Security**—Many Cisco networking devices offer an advanced level of security using authentication, authorization and accounting (AAA) features. All of the tasks described in this document, and other - more advanced security features - can be implemented using AAA on the networking device in conjunction with a remote TACACS+ or RADIUS server. For information how to configure AAA security features that can be run locally on a networking device, or for information on how to configure remote AAA security using TACACS+ or RADIUS servers, see the [Cisco IOS Security Configuration Guide](#), Release 12.4.

Additional References

The following sections provide references related to Configuring Security with Passwords and, Login Usernames for CLI Sessions on Networking Devices.

Related Documents

Related Topic	Document Title
Managing user access to CLI commands and configuration information	Role-Based CLI Access
AAA Security Features	<i>Cisco IOS Security Configuration Guide</i> , Release 12.4
Configuring MD5 secure neighbor authentication for protocols such as OSPF and BGP	Neighbor Router Authentication: Overview and Guidelines
Assigning privilege levels with TACACS+ and RADIUS	How to Assign Privilege Levels with TACACS+ and RADIUS

Standards

Standard	Title
No new or modified RFCs are supported by this functionality, and support for existing RFCs has not been modified.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this functionality, and support for existing RFCs has not been modified.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices

Table 70 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Releases 12.2(1) or 12.0(3)S or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific command was introduced, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Note

Table 70 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 70 *Feature Information for Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices*

Feature Name	Releases	Feature Configuration Information
Enhanced Password Security	12.0(18)S 12.2(8)T	<p>Using the Enhanced Password Security feature, you can configure MD5 encryption for username passwords. MD5 encryption is a one-way hash function that makes reversal of an encrypted password impossible, providing strong encryption protection. Using MD5 encryption, you cannot retrieve clear text passwords. MD5 encrypted passwords cannot be used with protocols that require that the clear text password be retrievable, such as Challenge Handshake Authentication Protocol (CHAP).</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Configuring and Verifying the Networking Device to Require a Username for the First-Line Technical Support Staff, page 30
Privilege Command Enhancement	12.0(22)S 12.2(13)T	<p>The keyword all was added to the privilege command as a wild card to reduce the number of times you need to enter the privilege command when you are changing the privilege level of several keywords for the same command.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Privilege Command Enhancement, page 26

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



No Service Password-Recovery

The No Service Password-Recovery feature is a security enhancement that prevents anyone with console access from accessing the router configuration and clearing the password. It also prevents anyone from changing the configuration register values and accessing NVRAM.

Feature History for the No Service Password-Recovery Feature

Release	Modification
12.3(8)YA	This feature was introduced.
12.3(14)T	This feature was integrated into Cisco IOS Release 12.3(14)T.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for No Service Password-Recovery, page 1](#)
- [Information About No Service Password-Recovery, page 2](#)
- [How to Enable No Service Password-Recovery, page 2](#)
- [Configuration Examples for No Service Password-Recovery, page 10](#)
- [Additional References, page 12](#)
- [Command Reference, page 13](#)

Prerequisites for No Service Password-Recovery

You are required to download and install ROM monitor (ROMMON) version 12.2(11)YV1 before you can use this feature.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Information About No Service Password-Recovery

To configure the No Service Password-Recovery feature, you should understand the following concepts:

- [Cisco Password Recovery Procedure, page 2](#)
- [Configuration Registers and System Boot Configuration, page 2](#)

Cisco Password Recovery Procedure

The Cisco IOS software provides a password recovery procedure that relies upon gaining access to ROMMON mode using the Break key during system startup. In ROMMON mode, the router software can be reloaded at which time prompting a new system configuration that includes a new password.

The current password recovery procedure enables anyone with console access, the ability to access the router and its network. The No Service Password-Recovery feature prevents the completion of the Break key sequence and the entering of ROMMON mode during system startups and reloads.

Configuration Registers and System Boot Configuration

The lowest four bits of the configuration register (bits 3, 2, 1, and 0) form the boot field. The boot field determines if the router boots manually from ROM or automatically from Flash or the network. For example, when the configuration register boot field value is set to any value from 0x2 to 0xF, the router uses the boot field value to form a default boot filename for autobooting from a network server.

Bit 6, when set, ignores the startup configuration, while bit 8 enables a break. To use this feature, the configuration register must be set to autoboot before it can be enabled. Any other configuration register setting will prevent the feature from being enabled.

**Note**

By default, the no confirm prompt and message are not displayed after reloads.

How to Enable No Service Password-Recovery

This section contains the following procedures:

- [Upgrading the ROMMON Version, page 3](#) (required)
- [Verifying the Upgraded ROMMON Version, page 5](#) (optional)
- [Enabling No Service Password-Recovery, page 5](#) (required)
- [Recovering a Device, page 6](#) (required)

Upgrading the ROMMON Version

If your router or access server does not find a valid system image to load, the system will enter ROMMON mode. ROMMON mode can also be accessed by interrupting the boot sequence during startup.

Another method for entering ROMMON mode is to set the configuration register so that the router automatically enters ROMMON mode when it boots. For information about setting the configuration register value, refer to the [Cisco IOS Configuration Fundamentals and Network Management Configuration Guide](#), Release 12.3.

Perform this task to upgrade your version of ROMMON.

SUMMARY STEPS

1. reload
2. set *tftp-file ip-address ip-subnet-mask default-gateway tftp-server*
3. sync
4. tftpdnld -u
5. boot

DETAILED STEPS

	Command or Action	Purpose
Step 1	reload Example: Router> reload	Reloads a Cisco IOS image. After issuing this command and responding to the system prompts as necessary, the system will begin reloading the system software image. While the system is reloading, press the Break key or a Break key-combination during the first 60 seconds of system startup. Pressing the Break key interrupts the boot sequence and puts the router into ROMMON mode. Note The default Break key combination is Ctrl-C, but this may be configured differently on your system.
Step 2	set tftp-file ip-address ip-subnet-mask default-gateway tftp-server Example: ROMMON> set tftpabc 10.10.0.0 255.0.0.0 10.1.1.0 10.29.32.0	Displays all the created variables. The arguments are as follows: <ul style="list-style-type: none"> <i>tftp-file</i>—Location of the new ROMMON image on the TFTP server. The length of the filename is a maximum of 45 characters. <i>ip-address</i>—IP address on the router to connect to the TFTP server. <i>ip-subnet-mask</i>—IP subnet mask of the router. <i>default-gateway</i>—IP address of the gateway of the TFTP server. <i>tftp-server</i>—IP address of the TFTP server from which the image will be downloaded. Note This command is not supported on the Cisco 800 series routers.
Step 3	sync Example: ROMMON> sync	Saves the changes to the image.
Step 4	tftpdnld -u Example: ROMMON> tftpdnld -u	Downloads the new ROMMON image from the TFTP server. Reset if prompted.
Step 5	boot Example: ROMMON> boot	Boots the router with the Cisco IOS image in flash memory.

Verifying the Upgraded ROMMON Version

To verify that you have downloaded a new version of ROMMON, use the **show version** command:

```
Router# show version
```

```
Cisco IOS Software, C828 Software (C828-K9OS&6-M), Version 12.3 (20040702:094716)  
[userid 168]
```

```
Copyright (c) 1986-2004 by Cisco Systems, Inc.
```

```
ROM: System Bootstrap, Version 12.2(11)YV1, Release Software (fc1)
```

```
Router uptime is 22 minutes  
System returned to ROM by reload  
.  
.  
.
```

Enabling No Service Password-Recovery

Perform this task to enable the No Service Password-Recovery feature.



Note

As a precaution, a valid Cisco IOS image should reside in flash memory before this feature is enabled.

If you plan to enter the **no service password-recovery** command, we recommend that you save a copy of the system configuration file in a location away from the switch or router. If you are using a switch that is operating in VTP transparent mode, we recommend that you also save a copy of the vlan.dat file in a location away from the switch.

Prerequisites

Always disable the feature before downgrading to an image that does not support this feature, because you cannot reset after the downgrade.

The configuration register boot bit must be enabled so that there is no way to break into ROMMON when this command is configured. Cisco IOS software should prevent the user from configuring the boot field in the config register.

Bit 6, which ignores the startup configuration and bit 8, which enables a break, should be set.

The Break key should be disabled while the router is booting up and disabled in Cisco IOS software when this feature is enabled.

SUMMARY STEPS

1. **enable**
2. **show version**
3. **configure terminal**

4. **config-register** *value*
5. **no service password-recovery**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	show version Example: Router# show version	Displays information about the system software, including configuration register settings. The configuration register must be set to autoboot before entering the no service password-recovery command.
Step 3	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 4	config-register <i>value</i> Example: Router(config)# config-register 0x2012	(Optional) Changes the configuration register setting. <ul style="list-style-type: none">• If necessary, change the configuration register setting so the router is set to autoboot.
Step 5	no service password-recovery Example: Router(config)# no service password-recovery	Disables password-recovery capability at the system console.
Step 6	exit Example: Router(config)# exit	Exits global configuration mode and returns to EXEC mode.

Recovering a Device

To recover a device once the No Service Password-Recovery feature has been enabled, press the Break key within 5 seconds after the image decompresses during the boot. You are prompted to confirm the Break key action. When you confirm the action, the startup configuration is erased, the password-recovery procedure is enabled, and the router boots with the factory default configuration.

If you do not confirm the Break key action, the router boots normally with the No Service Password-Recovery feature enabled.

Examples

This section provides the following examples of the process:

- [Confirmed Break, page 7](#)
- [Unconfirmed Break, page 8](#)

Confirmed Break

```
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
program load complete, entry point: 0x80013000, size: 0x8396a8
Self decompressing the image :
#####
##### [OK]
!The 5 second window starts now.
```

```
telnet> send break
telnet> send break
telnet> send break
```

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software, C831 Software (C831-K9O3SY6-M), Version 12.3(8)YA
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Fri 13-Aug-04 03:21
Image text-base: 0x80013200, data-base: 0x81020514

PASSWORD RECOVERY IS DISABLED.

Do you want to reset the router to factory default configuration and proceed [y/n] ?
!The user enters "Y" here.

Reset router configuration to factory default.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption.

Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

Cisco C831 (MPC857DSL) processor (revision 0x00) with 46695K/2457K bytes of memory.
Processor board ID 0000 (1314672220), with hardware revision 0000 CPU rev number 7
3 Ethernet interfaces
4 FastEthernet interfaces
128K bytes of NVRAM.

```
24576K bytes of processor board System flash (Read/Write)
2048K bytes of processor board Web flash (Read/Write)
```

```
--- System Configuration Dialog ---
```

```
Would you like to enter the initial configuration dialog? [yes/no]: no
!Start up configuration is erased.
```

```
SETUP: new interface FastEthernet1 placed in "up" state
SETUP: new interface FastEthernet2 placed in "up" state
SETUP: new interface FastEthernet3 placed in "up" state
SETUP: new interface FastEthernet4 placed in "up" state
```

```
Press RETURN to get started!
```

```
Router>
Router> enable
Router# show startup configuration
```

```
startup-config is not present
```

```
Router# show running-config | incl service
```

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```
!The "no service password-recovery" is disabled.
```

Unconfirmed Break

```
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
```

```
telnet> send break
program load complete, entry point: 0x80013000, size: 0x8396a8
Self decompressing the image :
##### [OK]
```

```
telnet> send break
telnet> send break
```

```
Restricted Rights Legend
```

```
Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
```

```
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
```

```
Cisco IOS Software, C831 Software (C831-K903SY6-M), Version 12.3(8)YA
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Fri 13-Aug-04 03:21
Image text-base: 0x80013200, data-base: 0x81020514
```

```
PASSWORD RECOVERY IS DISABLED.
Do you want to reset the router to factory default configuration and proceed [y/n] ?
!The user enters "N" here.
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption.

Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.
Cisco C831 (MPC857DSL) processor (revision 0x00) with 46695K/2457K bytes of memory.
Processor board ID 0000 (1314672220), with hardware revision 0000
CPU rev number 7
3 Ethernet interfaces
4 FastEthernet interfaces
128K bytes of NVRAM.
24576K bytes of processor board System flash (Read/Write)
2048K bytes of processor board Web flash (Read/Write)

Press RETURN to get started!
!The Cisco IOS software boots as if it is not interrupted.

```
Router> enable
Router#
Router# show startup config
```

```
Using 984 out of 131072 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
no service password-recovery
!
hostname Router
!
boot-start-marker
boot-end-marker
!
memory-size iomem 5
!
no aaa new-model
ip subnet-zero
!
ip ips po max-events 100
no ftp-server write-enable
!
interface Ethernet0
 no ip address
 shutdown
!
interface Ethernet1
 no ip address
 shutdown
 duplex auto
!
interface Ethernet2
 no ip address
 shutdown
```



```

!
interface FastEthernet1
  no ip address
  duplex auto
  speed auto
!
interface FastEthernet2
  no ip address
  duplex auto
  speed auto
!
interface FastEthernet3
  no ip address
  duplex auto
  speed auto
!
interface FastEthernet4
  no ip address
  duplex auto
  speed auto
!
ip classless
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
  no modem enable
  transport preferred all
  transport output all
line aux 0
line vty 0 4
!
scheduler max-task-time 5000
end

Router# show running-config | incl service

no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
no service password-recovery
end

```

Configuration Examples for No Service Password-Recovery

This section provides the following configuration example:

- [Disabling Password Recovery: Example, page 11](#)

Disabling Password Recovery: Example

The following example shows how to obtain the configuration register setting (which is set to autoboot), disable password recovery capability, and then verify that the configuration persists through a system reload:

```
Router# show version
```

```
Cisco Internetwork Operating System Software
IOS (tm) 5300 Software (C7200-P-M), Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Wed 05-Mar-04 10:16 by xxx
Image text-base: 0x60008954, data-base: 0x61964000
```

```
ROM: System Bootstrap, Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
```

```
.
.
.
```

```
125440K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
```

```
8192K bytes of Flash internal SIMM (Sector size 256K).
```

```
Configuration register is 0x2102
```

```
Router# configure terminal
```

```
Router(config)# no service password-recovery
```

```
WARNING:
```

```
Executing this command will disable the password recovery mechanism.
```

```
Do not execute this command without another plan for password recovery.
```

```
Are you sure you want to continue? [yes/no]: yes
```

```
.
.
.
```

```
Router(config)# exit
```

```
Router#
```

```
Router# reload
```

```
Proceed with reload? [confirm] yes
```

```
00:01:54: %SYS-5-RELOAD: Reload requested
```

```
System Bootstrap, Version 12.3...
```

```
Copyright (c) 1994-2004 by cisco Systems, Inc.
```

```
C7400 platform with 262144 Kbytes of main memory
```

```
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
```

```
.
.
.
```

Additional References

The following sections provide references related to the No Service Password-Recovery feature.

Related Documents

Related Topic	Document Title
Setting, changing, and recovering lost passwords	Refer to the “Configuring Passwords and Privileges” chapter in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.3
Loading system images and rebooting	Refer to the “File Management” section in the <i>Cisco IOS Configuration Fundamentals and Network Management Configuration Guide</i> , Release 12.3
Security commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Refer to the <i>Cisco IOS Security Command Reference</i> , Release 12.3T

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **service password-recovery**

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Appendixes



RADIUS Attributes



RADIUS Attributes Overview and RADIUS IETF Attributes

Feature History

Release	Modification
Cisco IOS	For information about feature support in Cisco IOS software, use Cisco Feature Navigator.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Remote Authentication Dial-In User Service (RADIUS) attributes are used to define specific authentication, authorization, and accounting (AAA) elements in a user profile, which is stored on the RADIUS daemon. This appendix lists the RADIUS attributes currently supported.

In This Appendix

This appendix contains the following sections:

- [RADIUS Attributes Overview](#)
- [RADIUS IETF Attributes](#)
- [RADIUS Vendor-Proprietary Attributes](#)
- [RADIUS Vendor-Specific Attributes \(VSA\) and RADIUS Disconnect-Cause Attribute Values](#)
- [RADIUS Disconnect-Cause Attribute Values](#)

RADIUS Attributes Overview

This section contains information important to understanding how RADIUS attributes exchange AAA information between a client and server and includes the following sections:

- [IETF Attributes Versus VSAs](#)
- [RADIUS Packet Format](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [RADIUS Files](#)
- [Supporting Documentation](#)

IETF Attributes Versus VSAs

RADIUS Internet Engineering Task Force (IETF) attributes are the original set of 255 standard attributes that are used to communicate AAA information between a client and a server. Because IETF attributes are standard, the attribute data is predefined and well known; thus all clients and servers who exchange AAA information via IETF attributes must agree on attribute data such as the exact meaning of the attributes and the general bounds of the values for each attribute.

RADIUS vendor-specific attributes (VSAs) derived from one IETF attribute—vendor-specific (attribute 26). Attribute 26 allows a vendor to create an additional 255 attributes however they wish. That is, a vendor can create an attribute that does not match the data of any IETF attribute and encapsulate it behind attribute 26; thus, the newly created attribute is accepted if the user accepts attribute 26.

For more information on VSAs, refer to the section “[RADIUS Vendor-Specific Attributes \(VSA\) and RADIUS Disconnect-Cause Attribute Values](#)” later in this appendix.

RADIUS Packet Format

The data between a RADIUS server and a RADIUS client is exchanged in RADIUS packets. The data fields are transmitted from left to right.

[Figure 125](#) shows the fields within a RADIUS packet.



Note

For a diagram of VSAs, which is an extension of [Figure 125](#), refer to [Figure 1](#).

Figure 125 **RADIUS Packet Diagram**



Each RADIUS packet contains the following information:

- Code—The code field is one octet; it identifies one of the following types of RADIUS packets:
 - Access-Request (1)
 - Access-Accept (2)
 - Access-Reject (3)
 - Accounting-Request (4)
 - Accounting-Response (5)

- Identifier—The identifier field is one octet; it helps the RADIUS server match requests and responses and detect duplicate requests.
- Length—The length field is two octets; it specifies the length of the entire packet.
- Authenticator—The authenticator field is 16 octets. The most significant octet is transmitted first; it is used to authenticate the reply from the RADIUS server. Two types of authenticators are as follows:
 - Request-Authentication: Available in Access-Request and Accounting-Request packets
 - Response-Authenticator: Available in Access-Accept, Access-Reject, Access-Challenge, and Accounting-Response packets

RADIUS Packet Types

The following list defines the various types of RADIUS packet types that can contain attribute information:

Access-Request—Sent from a client to a RADIUS server. The packet contains information that allows the RADIUS server to determine whether to allow access to a specific network access server (NAS), which will allow access to the user. Any user performing authentication *must* submit an Access-Request packet. Once an Access-Request packet is received, the RADIUS server *must* forward a reply.

Access-Accept—Once a RADIUS server receives an Access-Request packet, it must send an Access-Accept packet if all attribute values in the Access-Request packet are acceptable. Access-Accept packets provide the configuration information necessary for the client to provide service to the user.

Access-Reject—Once a RADIUS server receives an Access-Request packet, it must send an Access-Reject packet if any of the attribute values are not acceptable.

Access-Challenge—Once the RADIUS server receives an Access-Accept packet, it can send the client an Access-Challenge packet, which requires a response. If the client does not know how to respond or if the packets are invalid, the RADIUS server discards the packets. If the client responds to the packet, a new Access-Request packet should be sent with the original Access-Request packet.

Accounting-Request—Sent from a client to a RADIUS accounting server, which provides accounting information. If the RADIUS server successfully records the Accounting-Request packet, it must submit an Accounting Response packet.

Accounting-Response—Sent by the RADIUS accounting server to the client to acknowledge that the Accounting-Request has been received and recorded successfully.

RADIUS Files

Understanding the types of files used by RADIUS is important for communicating AAA information from a client to a server. Each file defines a level of authentication or authorization for the user: The dictionary file defines which attributes the user's NAS can implement; the clients file defines which users are allowed to make requests to the RADIUS server; the users file defines which user requests the RADIUS server will authenticate based on security and configuration data.

- [Dictionary File](#)
- [Clients File](#)
- [Users File](#)

Dictionary File

A dictionary file provides a list of attributes that are dependent upon which attributes your NAS supports. However, you can add your own set of attributes to your dictionary for custom solutions. It defines attribute values, thereby allowing you to interpret attribute output such as parsing requests. A dictionary file contains the following information:

- Name—The ASCII string “name” of the attribute, such as User-Name.
- ID—The numerical “name” of the attribute; for example, User-Name attribute is attribute 1.
- Value type—Each attribute can be specified as one of the following five value types:
 - binary—0 to 254 octets.
 - date—32-bit value in big endian order. For example, seconds since 00:00:00 GMT, JAN. 1, 1970.
 - ipaddr—4 octets in network byte order.
 - integer—32-bit value in big endian order (high byte first).
 - string—0 to 253 octets.

When the data type for a particular attribute is an integer, you can optionally expand the integer to equate to some string. The follow sample dictionary includes an integer-based attribute and its corresponding values:

```
# dictionary sample of integer entry
#
ATTRIBUTE      Service-Type      6          integer
VALUE          Service-Type      Login       1
VALUE          Service-Type      Framed      2
VALUE          Service-Type      Callback-Login  3
VALUE          Service-Type      Callback-Framed  4
VALUE          Service-Type      Outbound    5
VALUE          Service-Type      Administrative  6
VALUE          Service-Type      NAS-Prompt  7
VALUE          Service-Type      Authenticate-Only  8
VALUE          Service-Type      Callback-NAS-Prompt  9
VALUE          Service-Type      Call-Check  10
VALUE          Service-Type      Callback-Administrative 11
```

Clients File

A clients file is important because it contains a list of RADIUS clients that are allowed to send authentication and accounting requests to the RADIUS server. To receive authentication, the name and authentication key the client sends the server must be an exact match with the data contained in clients file.

The following is an example of a clients file. The key, as shown in this example, must be the same as the **radius-server key** *SomeSecret* command.

```
#Client Name      Key
#-----
10.1.2.3:256      test
nas01             bananas
nas02             MoNkEys
nas07.foo.com     SomeSecret
```

Users File

A RADIUS users file contains an entry for each user that the RADIUS server will authenticate; each entry, which is also referred to as a user profile, establishes an attribute the user can access.

The first line in any user profile is always a “user access” line; that is, the server must check the attributes on the first line before it can grant access to the user. The first line contains the name of the user, which can be up to 252 characters, followed by authentication information such as the password of the user.

Additional lines, which are associated with the user access line, indicate the attribute reply that is sent to the requesting client or server. The attributes sent in the reply must be defined in the dictionary file.

When looking at a user file, please note the the data to the left of the equal (=) character is an attribute defined in the dictionary file, and the data to the right of the equal character is the configuration data.

**Note**

A blank line cannot appear anywhere within a user profile.

The following is an example of a RADIUS user profile (Merit Daemon format). In this example, the user name is cisco.com, the password is cisco, and the user can access five tunnel attributes.

```
# This user profile includes RADIUS tunneling attributes
cisco.com Password="cisco" Service-Type=Outbound
    Tunnel-Type = :1:L2TP
    Tunnel-Medium-Type = :1:IP
    Tunnel-Server-Endpoint = :1:10.0.0.1
    Tunnel-Password = :1:"welcome"
    Tunnel-Assignment-ID = :1:"nas"
```

Supporting Documentation

For more information on RADIUS IETF and Vendor-Proprietary Attributes, refer to the following documents:

- Cisco AAA Implementation Case Study
- “[Configuring RADIUS](#)” “[Configuring Authentication](#),” “[Configuring Authorization](#)” and “[Configuring Accounting](#)” chapters in this book.

Refer to these chapters for information on how RADIUS is used with AAA.

- IETF RADIUS RFCs
 - RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*
 - RFC 2866, *RADIUS Accounting*
 - RFC 2867, *RADIUS Accounting Modifications for Tunnel Protocol Support*
 - RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*
 - RFC 2869, *RADIUS Extensions*
- RADIUS Vendor-Specific Attributes Voice Implementation Guide

RADIUS IETF Attributes



Note

In the Cisco IOS Release 12.2 for RADIUS tunnel attributes, 32 tagged tunnel sets are supported for L2TP.

This section contains the following sections:

- [Supported RADIUS IETF Attributes](#)
- [Comprehensive List of RADIUS Attribute Descriptions](#)

Supported RADIUS IETF Attributes

[Table 71](#) lists Cisco-supported IETF RADIUS attributes and the Cisco IOS release in which they are implemented. In cases where the attribute has a security server-specific format, the format is specified.

Refer to [Table 72](#) for a description of each listed attribute.



Note

Attributes implemented in special (AA) or early development (T) releases will be added to the next mainline image.

Table 71 *Supported RADIUS IETF Attributes*

Number	IETF Attribute	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
1	User-Name	yes	yes	yes	yes	yes	yes	yes	yes
2	User-Password	yes	yes	yes	yes	yes	yes	yes	yes
3	CHAP-Password	yes	yes	yes	yes	yes	yes	yes	yes
4	NAS-IP Address	yes	yes	yes	yes	yes	yes	yes	yes
5	NAS-Port	yes	yes	yes	yes	yes	yes	yes	yes
6	Service-Type	yes	yes	yes	yes	yes	yes	yes	yes
7	Framed-Protocol	yes	yes	yes	yes	yes	yes	yes	yes
8	Framed-IP-Address	yes	yes	yes	yes	yes	yes	yes	yes
9	Framed-IP-Netmask	yes	yes	yes	yes	yes	yes	yes	yes
10	Framed-Routing	yes	yes	yes	yes	yes	yes	yes	yes
11	Filter-Id	yes	yes	yes	yes	yes	yes	yes	yes
12	Framed-MTU	yes	yes	yes	yes	yes	yes	yes	yes
13	Framed-Compression	yes	yes	yes	yes	yes	yes	yes	yes
14	Login-IP-Host	yes	yes	yes	yes	yes	yes	yes	yes
15	Login-Service	yes	yes	yes	yes	yes	yes	yes	yes
16	Login-TCP-Port	yes	yes	yes	yes	yes	yes	yes	yes
18	Reply-Message	yes	yes	yes	yes	yes	yes	yes	yes
19	Callback-Number	no	no	no	no	no	no	yes	yes

Table 71 **Supported RADIUS IETF Attributes (continued)**

Number	IETF Attribute	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
20	Callback-ID	no	no	no	no	no	no	no	no
22	Framed-Route	yes	yes	yes	yes	yes	yes	yes	yes
23	Framed-IPX-Network	no	no	no	no	no	no	no	no
24	State	yes	yes	yes	yes	yes	yes	yes	yes
25	Class	yes	yes	yes	yes	yes	yes	yes	yes
26	Vendor-Specific	yes	yes	yes	yes	yes	yes	yes	yes
27	Session-Timeout	yes	yes	yes	yes	yes	yes	yes	yes
28	Idle-Timeout	yes	yes	yes	yes	yes	yes	yes	yes
29	Termination-Action	no	no	no	no	no	no	no	no
30	Called-Station-Id	yes	yes	yes	yes	yes	yes	yes	yes
31	Calling-Station-Id	yes	yes	yes	yes	yes	yes	yes	yes
32	NAS-Identifier	no	no	no	no	no	no	no	yes
33	Proxy-State	no	no	no	no	no	no	no	no
34	Login-LAT-Service	yes	yes	yes	yes	yes	yes	yes	yes
35	Login-LAT-Node	no	no	no	no	no	no	no	yes
36	Login-LAT-Group	no	no	no	no	no	no	no	no
37	Framed-AppleTalk-Link	no	no	no	no	no	no	no	no
38	Framed-AppleTalk- Network	no	no	no	no	no	no	no	no
39	Framed-AppleTalk-Zone	no	no	no	no	no	no	no	no
40	Acct-Status-Type	yes	yes	yes	yes	yes	yes	yes	yes
41	Acct-Delay-Time	yes	yes	yes	yes	yes	yes	yes	yes
42	Acct-Input-Octets	yes	yes	yes	yes	yes	yes	yes	yes
43	Acct-Output-Octets	yes	yes	yes	yes	yes	yes	yes	yes
44	Acct-Session-Id	yes	yes	yes	yes	yes	yes	yes	yes
45	Acct-Authentic	yes	yes	yes	yes	yes	yes	yes	yes
46	Acct-Session-Time	yes	yes	yes	yes	yes	yes	yes	yes
47	Acct-Input-Packets	yes	yes	yes	yes	yes	yes	yes	yes
48	Acct-Output-Packets	yes	yes	yes	yes	yes	yes	yes	yes
49	Acct-Terminate-Cause	no	no	no	yes	yes	yes	yes	yes
50	Acct-Multi-Session-Id	no	yes	yes	yes	yes	yes	yes	yes
51	Acct-Link-Count	no	yes	yes	yes	yes	yes	yes	yes
52	Acct-Input-Gigawords	no	no	no	no	no	no	no	no
53	Acct-Output-Gigawords	no	no	no	no	no	no	no	no
55	Event-Timestamp	no	no	no	no	no	no	no	yes
60	CHAP-Challenge	yes	yes	yes	yes	yes	yes	yes	yes
61	NAS-Port-Type	yes	yes	yes	yes	yes	yes	yes	yes

Table 71 **Supported RADIUS IETF Attributes (continued)**

Number	IETF Attribute	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
62	Port-Limit	yes	yes	yes	yes	yes	yes	yes	yes
63	Login-LAT-Port	no	no	no	no	no	no	no	no
64	Tunnel-Type ¹	no	no	no	no	no	no	yes	yes
65	Tunnel-Medium-Type ¹	no	no	no	no	no	no	yes	yes
66	Tunnel-Client-Endpoint	no	no	no	no	no	no	yes	yes
67	Tunnel-Server-Endpoint ¹	no	no	no	no	no	no	yes	yes
68	Acct-Tunnel-Connection-ID	no	no	no	no	no	no	yes	yes
69	Tunnel-Password ¹	no	no	no	no	no	no	yes	yes
70	ARAP-Password	no	no	no	no	no	no	no	no
71	ARAP-Features	no	no	no	no	no	no	no	no
72	ARAP-Zone-Access	no	no	no	no	no	no	no	no
73	ARAP-Security	no	no	no	no	no	no	no	no
74	ARAP-Security-Data	no	no	no	no	no	no	no	no
75	Password-Retry	no	no	no	no	no	no	no	no
76	Prompt	no	no	no	no	no	no	yes	yes
77	Connect-Info	no	no	no	no	no	no	no	yes
78	Configuration-Token	no	no	no	no	no	no	no	no
79	EAP-Message	no	no	no	no	no	no	no	no
80	Message-Authenticator	no	no	no	no	no	no	no	no
81	Tunnel-Private-Group-ID	no	no	no	no	no	no	no	no
82	Tunnel-Assignment-ID ¹	no	no	no	no	no	no	yes	yes
83	Tunnel-Preference	no	no	no	no	no	no	no	yes
84	ARAP-Challenge-Response	no	no	no	no	no	no	no	no
85	Acct-Interim-Interval	no	no	no	no	no	no	yes	yes
86	Acct-Tunnel-Packets-Lost	no	no	no	no	no	no	no	no
87	NAS-Port-ID	no	no	no	no	no	no	no	no
88	Framed-Pool	no	no	no	no	no	no	no	no
90	Tunnel-Client-Auth-ID ²	no	no	no	no	no	no	no	yes
91	Tunnel-Server-Auth-ID	no	no	no	no	no	no	no	yes
200	IETF-Token-Immediate	no	no	no	no	no	no	no	no

1. This RADIUS attribute complies with the following two draft IETF documents: RFC 2868 *RADIUS Attributes for Tunnel Protocol Support* and RFC 2867 *RADIUS Accounting Modifications for Tunnel Protocol Support*.
2. This RADIUS attribute complies with RFC 2865 and RFC 2868.

Comprehensive List of RADIUS Attribute Descriptions

Table 72 lists and describes IETF RADIUS attributes. In cases where the attribute has a security server-specific format, the format is specified.

Table 72 **RADIUS IETF Attributes**

Number	IETF Attribute	Description
1	User-Name	Indicates the name of the user being authenticated by the RADIUS server.
2	User-Password	Indicates the user's password or the user's input following an Access-Challenge. Passwords longer than 16 characters are encrypted using RFC 2865 specifications.
3	CHAP-Password	Indicates the response value provided by a PPP Challenge-Handshake Authentication Protocol (CHAP) user in response to an Access-Challenge.
4	NAS-IP Address	Specifies the IP address of the network access server that is requesting authentication. The default value is 0.0.0.0/0.
5	NAS-Port	<p>Indicates the physical port number of the network access server that is authenticating the user. The NAS-Port value (32 bits) consists of one or two 16-bit values (depending on the setting of the radius-server extended-portnames command). Each 16-bit number should be viewed as a 5-digit decimal integer for interpretation as follows:</p> <p>For asynchronous terminal lines, async network interfaces, and virtual async interfaces, the value is 00ttt, where ttt is the line number or async interface unit number.</p> <p>For ordinary synchronous network interface, the value is 10xxx.</p> <p>For channels on a primary rate ISDN interface, the value is 2ppcc.</p> <p>For channels on a basic rate ISDN interface, the value is 3bb0c.</p> <p>For other types of interfaces, the value is 6nnss.</p>

Table 72 RADIUS IETF Attributes (continued)

Number	IETF Attribute	Description
6	Service-Type	<p>Indicates the type of service requested or the type of service to be provided.</p> <ul style="list-style-type: none"> In a request: <ul style="list-style-type: none"> Framed for known PPP or SLIP connection. Administrative-user for enable command. In response: <ul style="list-style-type: none"> Login—Make a connection. Framed—Start SLIP or PPP. Administrative User—Start an EXEC or enable ok. <p>Exec User—Start an EXEC session.</p> <p>Service type is indicated by a particular numeric value as follows:</p> <ul style="list-style-type: none"> 1: Login 2: Framed 3: Callback-Login 4: Callback-Framed 5: Outbound 6: Administrative 7: NAS-Prompt 8: Authenticate Only 9: Callback-NAS-Prompt
7	Framed-Protocol	<p>Indicates the framing to be used for framed access. No other framing is allowed.</p> <p>Framing is indicated by a numeric value as follows:</p> <ul style="list-style-type: none"> 1: PPP 2: SLIP 3: ARA 4: Gandalf-proprietary single-link/multilink protocol 5: Xylogics-proprietary IPX/SLIP
8	Framed-IP-Address	<p>Indicates the IP address to be configured for the user, by sending the IP address of a user to the RADIUS server in the access-request. To enable this command, use the radius-server attribute 8 include-in-access-req command in global configuration mode.</p>
9	Framed-IP-Netmask	<p>Indicates the IP netmask to be configured for the user when the user is a router to a network. This attribute value results in a static route being added for Framed-IP-Address with the mask specified.</p>

Table 72 **RADIUS IETF Attributes (continued)**

Number	IETF Attribute	Description
10	Framed-Routing	<p>Indicates the routing method for the user when the user is a router to a network. Only “None” and “Send and Listen” values are supported for this attribute.</p> <p>Routing method is indicated by a numeric value as follows:</p> <ul style="list-style-type: none"> • 0: None • 1: Send routing packets • 2: Listen for routing packets • 3: Send routing packets and listen for routing packets
11	Filter-Id	<p>Indicates the name of the filter list for the user and is formatted as follows: %d, %d.in, or %d.out. This attribute is associated with the most recent service-type command. For login and EXEC, use %d or %d.out as the line access list value from 0 to 199. For Framed service, use %d or %d.out as interface output access list, and %d.in for input access list. The numbers are self-encoding to the protocol to which they refer.</p>
12	Framed-MTU	<p>Indicates the maximum transmission unit (MTU) that can be configured for the user when the MTU is not negotiated by PPP or some other means.</p>
13	Framed-Compression	<p>Indicates a compression protocol used for the link. This attribute results in a “/compress” being added to the PPP or SLIP autocommand generated during EXEC authorization. Not currently implemented for non-EXEC authorization.</p> <p>Compression protocol is indicated by a numeric value as follows:</p> <ul style="list-style-type: none"> • 0: None • 1: VJ-TCP/IP header compression • 2: IPX header compression
14	Login-IP-Host	<p>Indicates the host to which the user will connect when the Login-Service attribute is included. (This begins immediately after login.)</p>
15	Login-Service	<p>Indicates the service that should be used to connect the user to the login host.</p> <p>Service is indicated by a numeric value as follows:</p> <ul style="list-style-type: none"> • 0: Telnet • 1: Rlogin • 2: TCP-Clear • 3: PortMaster • 4: LAT
16	Login-TCP-Port	<p>Defines the TCP port with which the user is to be connected when the Login-Service attribute is also present.</p>
18	Reply-Message	<p>Indicates text that might be displayed to the user via the RADIUS server. You can include this attribute in user files; however, you cannot exceed a maximum of 16 Reply-Message entries per profile.</p>
19	Callback-Number	<p>Defines a dialing string to be used for callback.</p>
20	Callback-ID	<p>Defines the name (consisting of one or more octets) of a place to be called, to be interpreted by the network access server.</p>

Table 72 **RADIUS IETF Attributes (continued)**

Number	IETF Attribute	Description
22	Framed-Route	Provides routing information to be configured for the user on this network access server. The RADIUS RFC format (net/bits [router [metric]]) and the old style dotted mask (net mask [router [metric]]) are supported. If the router field is omitted or 0, the peer IP address is used. Metrics are currently ignored. This attribute is access-request packets.
23	Framed-IPX-Network	Defines the IPX network number configured for the user.
24	State	Allows state information to be maintained between the network access server and the RADIUS server. This attribute is applicable only to CHAP challenges.
25	Class	(Accounting) Arbitrary value that the network access server includes in all accounting packets for this user if supplied by the RADIUS server.
26	Vendor-Specific	<p>Allows vendors to support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option has vendor-type 1, which is named "cisco-avpair." The value is a string of the format:</p> <pre>protocol : attribute sep value</pre> <p>"Protocol" is a value of the Cisco "protocol" attribute for a particular type of authorization. "Attribute" and "value" are an appropriate AV pair defined in the Cisco TACACS+ specification, and "sep" is "=" for mandatory attributes and "*" for optional attributes. This allows the full set of features available for TACACS+ authorization to also be used for RADIUS. For example:</p> <pre>cisco-avpair= "ip:addr-pool=first" cisco-avpair= "shell:priv-lvl=15"</pre> <p>The first example causes Cisco's "multiple named ip address pools" feature to be activated during IP authorization (during PPP's IPCP address assignment). The second example causes a user logging in from a network access server to have immediate access to EXEC commands.</p> <p>Table 71 lists supported vendor-specific RADIUS attributes (IETF attribute 26). The "TACACS+ Attribute-Value Pairs" appendix provides a complete list of supported TACACS+ attribute-value (AV) pairs that can be used with IETF attribute 26. (RFC 2865)</p>
27	Session-Timeout	Sets the maximum number of seconds of service to be provided to the user before the session terminates. This attribute value becomes the per-user "absolute timeout."
28	Idle-Timeout	Sets the maximum number of consecutive seconds of idle connection allowed to the user before the session terminates. This attribute value becomes the per-user "session-timeout."
29	Termination-Action	<p>Termination is indicated by a numeric value as follows:</p> <ul style="list-style-type: none"> 0: Default 1: RADIUS request
30	Called-Station-Id	(Accounting) Allows the network access server to send the telephone number the user called as part of the Access-Request packet (using Dialed Number Identification Service [DNIS] or similar technology). This attribute is only supported on ISDN, and modem calls on the Cisco AS5200 if used with PRI.

Table 72 RADIUS IETF Attributes (continued)

Number	IETF Attribute	Description
31	Calling-Station-Id	(Accounting) Allows the network access server to send the telephone number the call came from as part of the Access-Request packet (using Automatic Number Identification or similar technology). This attribute has the same value as “remote-addr” from TACACS+. This attribute is only supported on ISDN, and modem calls on the Cisco AS5200 if used with PRI.
32	NAS-Identifier	String identifying the network access server originating the Access-Request. Use the radius-server attribute 32 include-in-access-req global configuration command to send RADIUS attribute 32 in an Access-Request or Accounting-Request. By default, the FQDN is sent in the attribute when the format is not specified.
33	Proxy-State	Attribute that can be sent by a proxy server to another server when forwarding Access-Requests; this must be returned unmodified in the Access-Accept, Access-Reject or Access-Challenge and removed by the proxy server before sending the response to the network access server.
34	Login-LAT-Service	Indicates the system with which the user is to be connected by LAT. This attribute is only available in the EXEC mode.
35	Login-LAT-Node	Indicates the node with which the user is to be automatically connected by LAT.
36	Login-LAT-Group	Identifies the LAT group codes that this user is authorized to use.
37	Framed-AppleTalk-Link	Indicates the AppleTalk network number that should be used for serial links to the user, which is another AppleTalk router.
38	Framed-AppleTalk-Network	Indicates the AppleTalk network number that the network access server uses to allocate an AppleTalk node for the user.
39	Framed-AppleTalk-Zone	Indicates the AppleTalk Default Zone to be used for this user.
40	Acct-Status-Type	(Accounting) Indicates whether this Accounting-Request marks the beginning of the user service (start) or the end (stop).
41	Acct-Delay-Time	(Accounting) Indicates how many seconds the client has been trying to send a particular record.
42	Acct-Input-Octets	(Accounting) Indicates how many octets have been received from the port over the course of this service being provided.
43	Acct-Output-Octets	(Accounting) Indicates how many octets have been sent to the port in the course of delivering this service.
44	Acct-Session-Id	(Accounting) A unique accounting identifier that makes it easy to match start and stop records in a log file. Acct-Session ID numbers restart at 1 each time the router is power cycled or the software is reloaded. To send this attribute in access-request packets, use the radius-server attribute 44 include-in-access-req command in global configuration mode.
45	Acct-Authentic	(Accounting) Indicates how the user was authenticated, whether by RADIUS, the network access server itself, or another remote authentication protocol. This attribute is set to “radius” for users authenticated by RADIUS; “remote” for TACACS+ and Kerberos; or “local” for local, enable, line, and if-needed methods. For all other methods, the attribute is omitted.
46	Acct-Session-Time	(Accounting) Indicates how long (in seconds) the user has received service.
47	Acct-Input-Packets	(Accounting) Indicates how many packets have been received from the port over the course of this service being provided to a framed user.

Table 72 **RADIUS IETF Attributes (continued)**

Number	IETF Attribute	Description
48	Acct-Output-Packets	(Accounting) Indicates how many packets have been sent to the port in the course of delivering this service to a framed user.
49	Acct-Terminate-Cause	<p>(Accounting) Reports details on why the connection was terminated. Termination causes are indicated by a numeric value as follows:</p> <ol style="list-style-type: none"> 1. User request 2. Lost carrier 3. Lost service 4. Idle timeout 5. Session timeout 6. Admin reset 7. Admin reboot 8. Port error 9. NAS error 10. NAS request 11. NAS reboot 12. Port unneeded 13. Port pre-empted 14. Port suspended 15. Service unavailable 16. Callback 17. User error 18. Host request <p>Note For attribute 49, Cisco IOS supports values 1 to 6, 9, 12, and 15 to 18.</p>
50	Acct-Multi-Session-Id	<p>(Accounting) A unique accounting identifier used to link multiple related sessions in a log file.</p> <p>Each linked session in a multilink session has a unique Acct-Session-Id value, but shares the same Acct-Multi-Session-Id.</p>
51	Acct-Link-Count	(Accounting) Indicates the number of links known in a given multilink session at the time an accounting record is generated. The network access server can include this attribute in any accounting request that might have multiple links.
52	Acct-Input-Gigawords	Indicates how many times the Acct-Input-Octets counter has wrapped around 2 ³² over the course of the provided service.
53	Acct-Output-Gigawords	Indicates how many times the Acct-Output-Octets counter has wrapped around 2 ³² while delivering service.

Table 72 RADIUS IETF Attributes (continued)

Number	IETF Attribute	Description
55	Event-Timestamp	<p>Records the time that the event occurred on the NAS; the timestamp sent in attribute 55 is in seconds since January 1, 1970 00:00 UTC. To send RADIUS attribute 55 in accounting packets, use the radius-server attribute 55 include-in-acct-req command.</p> <p>Note Before the Event-Timestamp attribute can be sent in accounting packets, you <i>must</i> configure the clock on the router. (For information on setting the clock on your router, refer to section “Performing Basic System Management” in the chapter “System Management” of the <i>Cisco IOS Configuration Fundamentals Configuration Guide</i>.)</p> <p>To avoid configuring the clock on the router every time the router is reloaded, you can enable the clock calendar-valid command. (For information on this command, refer to the chapter “Basic System Management Commands” in the <i>Cisco IOS Configuration Fundamentals Command Reference</i>.)</p>
60	CHAP-Challenge	Contains the Challenge Handshake Authentication Protocol challenge sent by the network access server to a PPP CHAP user.
61	NAS-Port-Type	<p>Indicates the type of physical port the network access server is using to authenticate the user. Physical ports are indicated by a numeric value as follows:</p> <ul style="list-style-type: none"> • 0: Asynchronous • 1: Synchronous • 2: ISDN-Synchronous • 3: ISDN-Asynchronous (V.120) • 4: ISDN-Asynchronous (V.110) • 5: Virtual
62	Port-Limit	Sets the maximum number of ports provided to the user by the NAS.
63	Login-LAT-Port	Defines the port with which the user is to be connected by LAT.
64	Tunnel-Type ¹	Indicates the tunneling protocol(s) used. Cisco IOS software supports two possible values for this attribute: L2TP and L2F. If this attribute is not set, L2F is used as a default.
65	Tunnel-Medium-Type ¹	Indicates the transport medium type to use to create a tunnel. This attribute has only one available value for this release: IP. If no value is set for this attribute, IP is used as the default.

Table 72 RADIUS IETF Attributes (continued)

Number	IETF Attribute	Description
66	Tunnel-Client-Endpoint	<p>Contains the address of the initiator end of the tunnel. It <i>may</i> be included in both Access-Request and Access-Accept packets to indicate the address from which a new tunnel is to be initiated. If the Tunnel-Client-Endpoint attribute is included in an Access-Request packet, the RADIUS server should take the value as a hint; the server is not obligated to honor the hint, however. This attribute <i>should</i> be included in Accounting-Request packets that contain Acct-Status-Type attributes with values of either Start or Stop, in which case it indicates the address from which the tunnel was initiated. This attribute, along with the Tunnel-Server-Endpoint and Acct-Tunnel-Connection-ID attributes, may be used to provide a globally unique means to identify a tunnel for accounting and auditing purposes.</p> <p>An enhancement has been added for the network access server to accept a value of 127.0.0.X for this attribute such that:</p> <ul style="list-style-type: none"> 127.0.0.0 would indicate that loopback0 IP address is to be used 127.0.0.1 would indicate that loopback1 IP address is to be used ... 127.0.0.X would indicate that loopbackX IP address is to be used <p>for the actual tunnel client endpoint IP address. This enhancement adds scalability across multiple network access servers.</p>
67	Tunnel-Server-Endpoint ¹	Indicates the address of the server end of the tunnel. The format of this attribute varies depending on the value of Tunnel-Medium-Type. Because this release only supports IP as a tunnel medium type, the IP address or the host name of LNS is valid for this attribute.
68	Acct-Tunnel-Connection-ID	Indicates the identifier assigned to the tunnel session. This attribute <i>should</i> be included in Accounting-Request packets that contain an Acct-Status-Type attribute having the value Start, Stop, or any of the values described above. This attribute, along with the Tunnel-Client-Endpoint and Tunnel-Server-Endpoint attributes, may be used to provide a means to uniquely identify a tunnel session for auditing purposes.
69	Tunnel-Password ¹	<p>Defines the password to be used to authenticate to a remote server. This attribute is converted into different AAA attributes based on the value of Tunnel-Type: AAA_ATTR_l2tp_tunnel_pw (L2TP), AAA_ATTR_nas_password (L2F), and AAA_ATTR_gw_password (L2F).</p> <p>By default, all passwords received are encrypted, which can cause authorization failures when a NAS attempts to decrypt a non-encrypted password. To enable attribute 69 to receive non-encrypted passwords, use the radius-server attribute 69 clear global configuration command.</p>
70	ARAP-Password	Identifies an Access-Request packet containing a Framed-Protocol of ARAP.
71	ARAP-Features	Includes password information that the NAS should send to the user in an ARAP "feature flags" packet.
72	ARAP-Zone-Access	Indicates how the ARAP zone list for the user should be used.
73	ARAP-Security	Identifies the ARAP Security Module to be used in an Access-Challenge packet.
74	ARAP-Security-Data	Contains the actual security module challenge or response. It can be found in Access-Challenge and Access-Request packets.
75	Password-Retry	Indicates how many times a user may attempt authentication before being disconnected.

Table 72 **RADIUS IETF Attributes (continued)**

Number	IETF Attribute	Description
76	Prompt	Indicates to the NAS whether it should echo the user's response as it is entered or not echo it. (0=no echo, 1=echo)
77	Connect-Info	Provides additional call information for modem calls. This attribute is generated in start and stop accounting records.
78	Configuration-Token	Indicates a type of user profile to be used. This attribute should be used in large distributed authentication networks based on proxy. It is sent from a RADIUS Proxy Server to a RADIUS Proxy Client in an Access-Accept; it should not be sent to a NAS.
79	EAP-Message	Encapsulates Extended Access Protocol (EAP) packets that allow the NAS to authenticate dial-in users via EAP without having to understand the EAP protocol.
80	Message-Authenticator	Prevents spoofing Access-Requests using CHAP, ARAP, or EAP authentication methods.
81	Tunnel-Private-Group-ID	Indicates the group ID for a particular tunneled session.
82	Tunnel-Assignment-ID ¹	Indicates to the tunnel initiator the particular tunnel to which a session is assigned.
83	Tunnel-Preference	Indicates the relative preference assigned to each tunnel. This attribute should be included if more than one set of tunneling attributes is returned by the RADIUS server to the tunnel initiator.
84	ARAP-Challenge-Response	Contains the response to the challenge of the dial-in client.
85	Acct-Interim-Interval	Indicates the number of seconds between each interim update in seconds for this specific session. This value can only appear in the Access-Accept message.
86	Acct-Tunnel-Packets-Lost	Indicates the number of packets lost on a given link. This attribute should be included in Accounting-Request packets that contain an Acct-Status-Type attribute having the value Tunnel-Link-Stop.
87	NAS-Port-ID	Contains a text string which identifies the port of the NAS that is authenticating the user.
88	Framed-Pool	Contains the name of an assigned address pool that should be used to assign an address for the user. If a NAS does not support multiple address pools, the NAS should ignore this attribute.
90	Tunnel-Client-Auth-ID	Specifies the name used by the tunnel initiator (also known as the NAS) when authenticating tunnel setup with the tunnel terminator. Supports L2F and L2TP protocols.
91	Tunnel-Server-Auth-ID	Specifies the name used by the tunnel terminator (also known as the Home Gateway) when authenticating tunnel setup with the tunnel initiator. Supports L2F and L2TP protocols.
200	IETF-Token-Immediate	<p>Determines how RADIUS treats passwords received from login-users when their file entry specifies a hand-held security card server.</p> <p>The value for this attribute is indicated by a numeric value as follows:</p> <ul style="list-style-type: none"> • 0: No, meaning that the password is ignored. • 1: Yes, meaning that the password is used for authentication.

1. This RADIUS attribute complies with the following two IETF documents: RFC 2868, *RADIUS Attributes for Tunnel Protocol Support* and RFC 2867, *RADIUS Accounting Modifications for Tunnel Protocol Support*.



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



RADIUS Vendor-Proprietary Attributes

Feature History

Release	Modification
Cisco IOS	For information about feature support in Cisco IOS software, use Cisco Feature Navigator.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Although an IETF draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the network access server and the RADIUS server, some vendors have extended the RADIUS attribute set for specific applications.

This section contains the following sections:

- [Supported Vendor-Proprietary RADIUS Attributes](#)
- [Comprehensive List of Vendor-Proprietary RADIUS Attribute Descriptions](#)

Supported Vendor-Proprietary RADIUS Attributes

Table 73 lists Cisco-supported vendor-proprietary RADIUS attributes and the Cisco IOS release in which they are implemented. In cases where the attribute has a security server-specific format, the format is specified. Refer to Table 74 for a list of descriptions.



Note

Attributes implemented in special (AA) or early development (T) releases will be added to the next mainline image.

Table 73 Supported Vendor-Proprietary RADIUS Attributes

Number	Vendor-Proprietary Attribute	11.1	11.2	11.3	11.3AA	11.3T	12.0	12.1	12.2
17	Change-Password	no	no	yes	yes	yes	yes	yes	yes
21	Password-Expiration	no	no	yes	yes	yes	yes	yes	yes
68	Tunnel-ID	no	no	no	no	no	no	no	yes
108	My-Endpoint-Disc-Alias	no	no	no	no	no	no	no	no



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Table 73 **Supported Vendor-Proprietary RADIUS Attributes (continued)**

Number	Vendor-Proprietary Attribute	11.1	11.2	11.3	11.3AA	11.3T	12.0	12.1	12.2
109	My-Name-Alias	no	no	no	no	no	no	no	no
110	Remote-FW	no	no	no	no	no	no	no	no
111	Multicast-GLeave-Delay	no	no	no	no	no	no	no	no
112	CBCP-Enable	no	no	no	no	no	no	no	no
113	CBCP-Mode	no	no	no	no	no	no	no	no
114	CBCP-Delay	no	no	no	no	no	no	no	no
115	CBCP-Trunk-Group	no	no	no	no	no	no	no	no
116	Appletalk-Route	no	no	no	no	no	no	no	no
117	Appletalk-Peer-Mode	no	no	no	no	no	no	no	no
118	Route-Appletalk	no	no	no	no	no	no	no	no
119	FCP-Parameter	no	no	no	no	no	no	no	no
120	Modem-PortNo	no	no	no	no	no	no	no	no
121	Modem-SlotNo	no	no	no	no	no	no	no	no
122	Modem-ShelfNo	no	no	no	no	no	no	no	no
123	Call-Attempt-Limit	no	no	no	no	no	no	no	no
124	Call-Block-Duration	no	no	no	no	no	no	no	no
125	Maximum-Call-Duration	no	no	no	no	no	no	no	no
126	Router-Preference	no	no	no	no	no	no	no	no
127	Tunneling-Protocol	no	no	no	no	no	no	no	no
128	Shared-Profile-Enable	no	no	no	no	no	no	no	no
129	Primary-Home-Agent	no	no	no	no	no	no	no	no
130	Secondary-Home-Agent	no	no	no	no	no	no	no	no
131	Dialout-Allowed	no	no	no	no	no	no	no	no
133	BACP-Enable	no	no	no	no	no	no	no	no
134	DHCP-Maximum-Leases	no	no	no	no	no	no	no	no
135	Primary-DNS-Server	no	no	no	no	yes	yes	yes	yes
136	Secondary-DNS-Server	no	no	no	no	yes	yes	yes	yes
137	Client-Assign-DNS	no	no	no	no	no	no	no	no
138	User-Acct-Type	no	no	no	no	no	no	no	no
139	User-Acct-Host	no	no	no	no	no	no	no	no
140	User-Acct-Port	no	no	no	no	no	no	no	no
141	User-Acct-Key	no	no	no	no	no	no	no	no
142	User-Acct-Base	no	no	no	no	no	no	no	no
143	User-Acct-Time	no	no	no	no	no	no	no	no
144	Assign-IP-Client	no	no	no	no	no	no	no	no

Table 73 **Supported Vendor-Proprietary RADIUS Attributes (continued)**

Number	Vendor-Proprietary Attribute	11.1	11.2	11.3	11.3AA	11.3T	12.0	12.1	12.2
145	Assign-IP-Server	no	no	no	no	no	no	no	no
146	Assign-IP-Global-Pool	no	no	no	no	no	no	no	no
147	DHCP-Reply	no	no	no	no	no	no	no	no
148	DHCP-Pool-Number	no	no	no	no	no	no	no	no
149	Expect-Callback	no	no	no	no	no	no	no	no
150	Event-Type	no	no	no	no	no	no	no	no
151	Session-Svr-Key	no	no	no	yes	no	no	yes	yes
152	Multicast-Rate-Limit	no	no	no	yes	no	no	yes	yes
153	IF-Netmask	no	no	no	no	no	no	no	no
154	Remote-Addr	no	no	no	no	no	no	no	no
155	Multicast-Client	no	no	no	yes	no	no	yes	yes
156	FR-Circuit-Name	no	no	no	no	no	no	no	no
157	FR-LinkUp	no	no	no	no	no	no	no	no
158	FR-Nailed-Grp	no	no	no	no	no	no	no	no
159	FR-Type	no	no	no	no	no	no	no	no
160	FR-Link-Mgt	no	no	no	no	no	no	no	no
161	FR-N391	no	no	no	no	no	no	no	no
162	FR-DCE-N392	no	no	no	no	no	no	no	no
163	FR-DTE-N392	no	no	no	no	no	no	no	no
164	FR-DCE-N393	no	no	no	no	no	no	no	no
165	FR-DTE-N393	no	no	no	no	no	no	no	no
166	FR-T391	no	no	no	no	no	no	no	no
167	FR-T392	no	no	no	no	no	no	no	no
168	Bridge-Address	no	no	no	no	no	no	no	no
169	TS-Idle-Limit	no	no	no	no	no	no	no	no
170	TS-Idle-Mode	no	no	no	no	no	no	no	no
171	DBA-Monitor	no	no	no	no	no	no	no	no
172	Base-Channel-Count	no	no	no	no	no	no	no	no
173	Minimum-Channels	no	no	no	no	no	no	no	no
174	IPX-Route	no	no	no	no	no	no	no	no
175	FT1-Caller	no	no	no	no	no	no	no	no
176	Backup	no	no	no	no	no	no	no	no
177	Call-Type	no	no	no	no	no	no	no	no
178	Group	no	no	no	no	no	no	no	no
179	FR-DLCI	no	no	no	no	no	no	no	no

Table 73 **Supported Vendor-Proprietary RADIUS Attributes (continued)**

Number	Vendor-Proprietary Attribute	11.1	11.2	11.3	11.3AA	11.3T	12.0	12.1	12.2
180	FR-Profile-Name	no	no	no	no	no	no	no	no
181	Ara-PW	no	no	no	no	no	no	no	no
182	IPX-Node-Addr	no	no	no	no	no	no	no	no
183	Home-Agent-IP-Addr	no	no	no	no	no	no	no	no
184	Home-Agent-Password	no	no	no	no	no	no	no	no
185	Home-Network-Name	no	no	no	no	no	no	no	no
186	Home-Agent-UDP-Port	no	no	no	no	no	no	no	no
187	Multilink-ID	no	no	no	yes	yes	yes	yes	yes
188	Num-In-Multilink	no	no	no	yes	yes	yes	yes	yes
189	First-Dest	no	no	no	no	no	no	no	no
190	Pre-Input-Octets	no	no	no	yes	yes	yes	yes	yes
191	Pre-Output-Octets	no	no	no	yes	yes	yes	yes	yes
192	Pre-Input-Packets	no	no	no	yes	yes	yes	yes	yes
193	Pre-Output-Packets	no	no	no	yes	yes	yes	yes	yes
194	Maximum-Time	no	no	yes	yes	yes	yes	yes	yes
195	Disconnect-Cause	no	no	yes	yes	yes	yes	yes	yes
196	Connect-Progress	no	no	no	no	no	no	yes	yes
197	Data-Rate	no	no	no	no	yes	yes	yes	yes
198	PreSession-Time	no	no	no	yes	yes	yes	yes	yes
199	Token-Idle	no	no	no	no	no	no	no	no
201	Require-Auth	no	no	no	no	no	no	no	no
202	Number-Sessions	no	no	no	no	no	no	no	no
203	Authen-Alias	no	no	no	no	no	no	no	no
204	Token-Expiry	no	no	no	no	no	no	no	no
205	Menu-Selector	no	no	no	no	no	no	no	no
206	Menu-Item	no	no	no	no	no	no	no	no
207	PW-Warntime	no	no	no	no	no	no	no	no
208	PW-Lifetime	no	no	yes	yes	yes	yes	yes	yes
209	IP-Direct	no	no	no	no	yes	yes	yes	yes
210	PPP-VJ-Slot-Comp	no	no	yes	yes	yes	yes	yes	yes
211	PPP-VJ-1172	no	no	no	no	no	no	no	no
212	PPP-Async-Map	no	no	no	no	no	no	no	no
213	Third-Prompt	no	no	no	no	no	no	no	no
214	Send-Secret	no	no	no	no	no	no	yes	yes
215	Receive-Secret	no	no	no	no	no	no	no	no

Table 73 **Supported Vendor-Proprietary RADIUS Attributes (continued)**

Number	Vendor-Proprietary Attribute	11.1	11.2	11.3	11.3AA	11.3T	12.0	12.1	12.2
216	IPX-Peer-Mode	no	no	no	no	no	no	no	no
217	IP-Pool-Definition	no	no	yes	yes	yes	yes	yes	yes
218	Assign-IP-Pool	no	no	yes	yes	yes	yes	yes	yes
219	FR-Direct	no	no	no	no	no	no	no	no
220	FR-Direct-Profile	no	no	no	no	no	no	no	no
221	FR-Direct-DLCI	no	no	no	no	no	no	no	no
222	Handle-IPX	no	no	no	no	no	no	no	no
223	Netware-Timeout	no	no	no	no	no	no	no	no
224	IPX-Alias	no	no	no	no	no	no	no	no
225	Metric	no	no	no	no	no	no	no	no
226	PRI-Number-Type	no	no	no	no	no	no	no	no
227	Dial-Number	no	no	no	no	no	no	yes	yes
228	Route-IP	no	no	yes	yes	yes	yes	yes	yes
229	Route-IPX	no	no	no	no	no	no	no	no
230	Bridge	no	no	no	no	no	no	no	no
231	Send-Auth	no	no	no	no	no	no	yes	yes
232	Send-Passwd	no	no	no	no	no	no	no	no
233	Link-Compression	no	no	yes	yes	yes	yes	yes	yes
234	Target-Util	no	no	no	yes	no	yes	yes	yes
235	Maximum-Channels	no	no	yes	yes	yes	yes	yes	yes
236	Inc-Channel-Count	no	no	no	no	no	no	no	no
237	Dec-Channel-Count	no	no	no	no	no	no	no	no
238	Seconds-of-History	no	no	no	no	no	no	no	no
239	History-Weigh-Type	no	no	no	no	no	no	no	no
240	Add-Seconds	no	no	no	no	no	no	no	no
241	Remove-Seconds	no	no	no	no	no	no	no	no
242	Data-Filter	no	no	yes	yes	yes	yes	yes	yes
243	Call-Filter	no	no	no	no	no	no	no	no
244	Idle-Limit	no	no	yes	yes	yes	yes	yes	yes
245	Preempt-Limit	no	no	no	no	no	no	no	no
246	Callback	no	no	no	no	no	no	no	no
247	Data-Svc	no	no	no	no	no	no	yes	yes
248	Force-56	no	no	no	no	no	no	yes	yes
249	Billing Number	no	no	no	no	no	no	no	no
250	Call-By-Call	no	no	no	no	no	no	no	no

Table 73 **Supported Vendor-Proprietary RADIUS Attributes (continued)**

Number	Vendor-Proprietary Attribute	11.1	11.2	11.3	11.3AA	11.3T	12.0	12.1	12.2
251	Transit-Number	no	no	no	no	no	no	no	no
252	Host-Info	no	no	no	no	no	no	no	no
253	PPP-Address	no	no	no	no	no	no	no	no
254	MPP-Idle-Percent	no	no	no	no	no	no	no	no
255	Xmit-Rate	no	no	no	yes	yes	yes	yes	yes

Comprehensive List of Vendor-Proprietary RADIUS Attribute Descriptions

Table 74 lists and describes the known vendor-proprietary RADIUS attributes:

Table 74 **Vendor-Proprietary RADIUS Attributes**

Number	Vendor-Proprietary Attribute	Description
17	Change-Password	Specifies a request to change the password of a user.
21	Password-Expiration	Specifies an expiration date for a user's password in the user's file entry.
68	Tunnel-ID	(Ascend 5) Specifies the string assigned by RADIUS for each session using CLID or DNIS tunneling. When accounting is implemented, this value is used for accounting.
108	My-Endpoint-Disc-Alias	(Ascend 5) No description available.
109	My-Name-Alias	(Ascend 5) No description available.
110	Remote-FW	(Ascend 5) No description available.
111	Multicast-GLeave-Delay	(Ascend 5) No description available.
112	CBCP-Enable	(Ascend 5) No description available.
113	CBCP-Mode	(Ascend 5) No description available.
114	CBCP-Delay	(Ascend 5) No description available.
115	CBCP-Trunk-Group	(Ascend 5) No description available.
116	Appletalk-Route	(Ascend 5) No description available.
117	Appletalk-Peer-Mode	(Ascend 5) No description available.
118	Route-Appletalk	(Ascend 5) No description available.
119	FCP-Parameter	(Ascend 5) No description available.
120	Modem-PortNo	(Ascend 5) No description available.
121	Modem-SlotNo	(Ascend 5) No description available.
122	Modem-ShelfNo	(Ascend 5) No description available.
123	Call-Attempt-Limit	(Ascend 5) No description available.
124	Call-Block-Duration	(Ascend 5) No description available.
125	Maximum-Call-Duration	(Ascend 5) No description available.

Table 74 **Vendor-Proprietary RADIUS Attributes (continued)**

Number	Vendor-Proprietary Attribute	Description
126	Router-Preference	(Ascend 5) No description available.
127	Tunneling-Protocol	(Ascend 5) No description available.
128	Shared-Profile-Enable	(Ascend 5) No description available.
129	Primary-Home-Agent	(Ascend 5) No description available.
130	Secondary-Home-Agent	(Ascend 5) No description available.
131	Dialout-Allowed	(Ascend 5) No description available.
133	BACP-Enable	(Ascend 5) No description available.
134	DHCP-Maximum-Leases	(Ascend 5) No description available.
135	Primary-DNS-Server	Identifies a primary DNS server that can be requested by Microsoft PPP clients from the network access server during IPCP negotiation.
136	Secondary-DNS-Server	Identifies a secondary DNS server that can be requested by Microsoft PPP clients from the network access server during IPCP negotiation.
137	Client-Assign-DNS	No description available.
138	User-Acct-Type	No description available.
139	User-Acct-Host	No description available.
140	User-Acct-Port	No description available.
141	User-Acct-Key	No description available.
142	User-Acct-Base	No description available.
143	User-Acct-Time	No description available.
144	Assign-IP-Client	No description available.
145	Assign-IP-Server	No description available.
146	Assign-IP-Global-Pool	No description available.
147	DHCP-Reply	No description available.
148	DHCP-Pool-Number	No description available.
149	Expect-Callback	No description available.
150	Event-Type	No description available.
151	Session-Svr-Key	No description available.
152	Multicast-Rate-Limit	No description available.
153	IF-Netmask	No description available.
154	Remote-Addr	No description available.
155	Multicast-Client	No description available.
156	FR-Circuit-Name	No description available.
157	FR-LinkUp	No description available.
158	FR-Nailed-Grp	No description available.
159	FR-Type	No description available.

Table 74 **Vendor-Proprietary RADIUS Attributes (continued)**

Number	Vendor-Proprietary Attribute	Description
160	FR-Link-Mgt	No description available.
161	FR-N391	No description available.
162	FR-DCE-N392	No description available.
163	FR-DTE-N392	No description available.
164	FR-DCE-N393	No description available.
165	FR-DTE-N393	No description available.
166	FR-T391	No description available.
167	FR-T392	No description available.
168	Bridge-Address	No description available.
169	TS-Idle-Limit	No description available.
170	TS-Idle-Mode	No description available.
171	DBA-Monitor	No description available.
172	Base-Channel-Count	No description available.
173	Minimum-Channels	No description available.
174	IPX-Route	No description available.
175	FT1-Caller	No description available.
176	Backup	No description available.
177	Call-Type	No description available.
178	Group	No description available.
179	FR-DLCI	No description available.
180	FR-Profile-Name	No description available.
181	Ara-PW	No description available.
182	IPX-Node-Addr	No description available.
183	Home-Agent-IP-Addr	Indicates the home agent's IP address (in dotted decimal format) when using Ascend Tunnel Management Protocol (ATMP).
184	Home-Agent-Password	With ATMP, specifies the password that the foreign agent uses to authenticate itself.
185	Home-Network-Name	With ATMP, indicates the name of the connection profile to which the home agent sends all packets.
186	Home-Agent-UDP-Port	Indicates the UDP port number the foreign agent uses to send ATMP messages to the home agent.
187	Multilink-ID	Reports the identification number of the multilink bundle when the session closes. This attribute applies to sessions that are part of a multilink bundle. The Multilink-ID attribute is sent in authentication-response packets.

Table 74 **Vendor-Proprietary RADIUS Attributes (continued)**

Number	Vendor-Proprietary Attribute	Description
188	Num-In-Multilink	Reports the number of sessions remaining in a multilink bundle when the session reported in an accounting-stop packet closes. This attribute applies to sessions that are part of a multilink bundle. The Num-In-Multilink attribute is sent in authentication-response packets and in some accounting-request packets.
189	First-Dest	Records the destination IP address of the first packet received after authentication.
190	Pre-Input-Octets	Records the number of input octets before authentication. The Pre-Input-Octets attribute is sent in accounting-stop records.
191	Pre-Output-Octets	Records the number of output octets before authentication. The Pre-Output-Octets attribute is sent in accounting-stop records.
192	Pre-Input-Packets	Records the number of input packets before authentication. The Pre-Input-Packets attribute is sent in accounting-stop records.
193	Pre-Output-Packets	Records the number of output packets before authentication. The Pre-Output-Packets attribute is sent in accounting-stop records.
194	Maximum-Time	Specifies the maximum length of time (in seconds) allowed for any session. After the session reaches the time limit, its connection is dropped.
195	Disconnect-Cause	Specifies the reason a connection was taken offline. The Disconnect-Cause attribute is sent in accounting-stop records. This attribute also causes stop records to be generated without first generating start records if disconnection occurs before authentication is performed. For more information, refer to the table of Disconnect-Cause Attribute Values and their meanings.
196	Connect-Progress	Indicates the connection state before the connection is disconnected.
197	Data-Rate	Specifies the average number of bits per second over the course of the connection's lifetime. The Data-Rate attribute is sent in accounting-stop records.
198	PreSession-Time	Specifies the length of time, in seconds, from when a call first connects to when it completes authentication. The PreSession-Time attribute is sent in accounting-stop records.
199	Token-Idle	Indicates the maximum amount of time (in minutes) a cached token can remain alive between authentications.
201	Require-Auth	Defines whether additional authentication is required for class that has been CLID authenticated.
202	Number-Sessions	Specifies the number of active sessions (per class) reported to the RADIUS accounting server.

Table 74 **Vendor-Proprietary RADIUS Attributes (continued)**

Number	Vendor-Proprietary Attribute	Description
203	Authen-Alias	Defines the RADIUS server's login name during PPP authentication.
204	Token-Expiry	Defines the lifetime of a cached token.
205	Menu-Selector	Defines a string to be used to cue a user to input data.
206	Menu-Item	Specifies a single menu-item for a user-profile. Up to 20 menu items can be assigned per profile.
207	PW-Warntime	(Ascend 5) No description available.
208	PW-Lifetime	Enables you to specify on a per-user basis the number of days that a password is valid.
209	IP-Direct	<p>When you include this attribute in a user's file entry, a framed route is installed to the routing and bridging tables.</p> <p>Note Packet routing is dependent upon the entire table, not just this newly installed entry. The inclusion of this attribute does not guarantee that all packets should be sent to the specified IP address; thus, this attribute is not fully supported.</p> <p>These attribute limitations occur because the Cisco router cannot bypass all internal routing and bridging tables and send packets to a specified IP address.</p>
210	PPP-VJ-Slot-Comp	Instructs the Cisco router not to use slot compression when sending VJ-compressed packets over a PPP link.
211	PPP-VJ-1172	Instructs PPP to use the 0x0037 value for VJ compression.
212	PPP-Async-Map	Gives the Cisco router the asynchronous control character map for the PPP session. The specified control characters are passed through the PPP link as data and used by applications running over the link.
213	Third-Prompt	Defines a third prompt (after username and password) for additional user input.
214	Send-Secret	Enables an encrypted password to be used in place of a regular password in outdial profiles.
215	Receive-Secret	Enables an encrypted password to be verified by the RADIUS server.
216	IPX-Peer-Mode	(Ascend 5) No description available.
217	IP-Pool-Definition	Defines a pool of addresses using the following format: X a.b.c Z; where X is the pool index number, a.b.c is the pool's starting IP address, and Z is the number of IP addresses in the pool. For example, 3 10.0.0.1 5 allocates 10.0.0.1 through 10.0.0.5 for dynamic assignment.
218	Assign-IP-Pool	Tells the router to assign the user and IP address from the IP pool.
219	FR-Direct	Defines whether the connection profile operates in Frame Relay redirect mode.

Table 74 **Vendor-Proprietary RADIUS Attributes (continued)**

Number	Vendor-Proprietary Attribute	Description
220	FR-Direct-Profile	Defines the name of the Frame Relay profile carrying this connection to the Frame Relay switch.
221	FR-Direct-DLCI	Indicates the DLCI carrying this connection to the Frame Relay switch.
222	Handle-IPX	Indicates how NCP watchdog requests will be handled.
223	Netware-Timeout	Defines, in minutes, how long the RADIUS server responds to NCP watchdog packets.
224	IPX-Alias	Allows you to define an alias for IPX routers requiring numbered interfaces.
225	Metric	No description available.
226	PRI-Number-Type	No description available.
227	Dial-Number	Defines the number to dial.
228	Route-IP	Indicates whether IP routing is allowed for the user's file entry.
229	Route-IPX	Allows you to enable IPX routing.
230	Bridge	No description available.
231	Send-Auth	Defines the protocol to use (PAP or CHAP) for username-password authentication following CLID authentication.
232	Send-Passwd	Enables the RADIUS server to specify the password that is sent to the remote end of a connection on outgoing calls.
233	Link-Compression	<p>Defines whether to turn on or turn off "stac" compression over a PPP link.</p> <p>Link compression is defined as a numeric value as follows:</p> <ul style="list-style-type: none"> • 0: None • 1: Stac • 2: Stac-Draft-9 • 3: MS-Stac
234	Target-Util	Specifies the load-threshold percentage value for bringing up an additional channel when PPP multilink is defined.
235	Maximum-Channels	Specifies allowed/allocatable maximum number of channels.
236	Inc-Channel-Count	No description available.
237	Dec-Channel-Count	No description available.
238	Seconds-of-History	No description available.
239	History-Weigh-Type	No description available.
240	Add-Seconds	No description available.
241	Remove-Seconds	No description available.

Table 74 **Vendor-Proprietary RADIUS Attributes (continued)**

Number	Vendor-Proprietary Attribute	Description
242	Data-Filter	Defines per-user IP data filters. These filters are retrieved only when a call is placed using a RADIUS outgoing profile or answered using a RADIUS incoming profile. Filter entries are applied on a first-match basis; therefore, the order in which filter entries are entered is important.
243	Call-Filter	Defines per-user IP data filters. On a Cisco router, this attribute is identical to the Data-Filter attribute.
244	Idle-Limit	Specifies the maximum time (in seconds) that any session can be idle. When the session reaches the idle time limit, its connection is dropped.
245	Preempt-Limit	No description available.
246	Callback	Allows you to enable or disable callback.
247	Data-Svc	No description available.
248	Force-56	Determines whether the network access server uses only the 56 K portion of a channel, even when all 64 K appear to be available.
249	Billing Number	No description available.
250	Call-By-Call	No description available.
251	Transit-Number	No description available.
252	Host-Info	No description available.
253	PPP-Address	Indicates the IP address reported to the calling unit during PPP IPCP negotiations.
254	MPP-Idle-Percent	No description available.
255	Xmit-Rate	(Ascend 5) No description available.

For more information on vendor-proprietary RADIUS attributes, refer to the section “[Configuring Router for Vendor-Proprietary RADIUS Server Communication](#)” in the chapter “[Configuring RADIUS](#).”



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and

coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



RADIUS Vendor-Specific Attributes (VSA) and RADIUS Disconnect-Cause Attribute Values

First Published: September 23, 2005
Last Updated: December 17, 2007

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26). Attribute 26 encapsulates vendor specific attributes, thereby, allowing vendors to support their own extended attributes otherwise not suitable for general use.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for RADIUS Vendor-Specific Attributes \(VSA\) and RADIUS Disconnect-Cause Attribute Values”](#) section on page 14.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Information About RADIUS Vendor-Specific Attributes \(VSA\) and RADIUS Disconnect-Cause Attribute Values, page 2](#)
- [RADIUS Disconnect-Cause Attribute Values, page 8](#)
- [Additional References, page 12](#)
- [Feature Information for RADIUS Vendor-Specific Attributes \(VSA\) and RADIUS Disconnect-Cause Attribute Values, page 14](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2005, 2007 Cisco Systems, Inc. All rights reserved.

Information About RADIUS Vendor-Specific Attributes (VSA) and RADIUS Disconnect-Cause Attribute Values

The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option has vendor-type 1, which is named "cisco-avpair." The value is a string of the following format:

```
protocol : attribute sep value *
```

"Protocol" is a value of the Cisco "protocol" attribute for a particular type of authorization; protocols that can be used include IP, IPX, VPDN, VOIP, SHELL, RSVP, SIP, AIRNET, OUTBOUND. "Attribute" and "value" are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification, and "sep" is "=" for mandatory attributes and "*" for optional attributes. This allows the full set of features available for TACACS+ authorization to also be used for RADIUS.

For example, the following AV pair causes Cisco's "multiple named ip address pools" feature to be activated during IP authorization (during PPP's IPCP address assignment):

```
cisco-avpair= "ip:addr-pool=first"
```

If you insert an "*", the AV pair "ip:addr-pool=first" becomes optional. Note that any AV pair can be made optional.

```
cisco-avpair= "ip:addr-pool*first"
```

The following example shows how to cause a user logging in from a network access server to have immediate access to EXEC commands:

```
cisco-avpair= "shell:priv-lvl=15"
```

Attribute 26 contains the following three elements:

- Type
- Length
- String (also known as data)
 - Vendor-Id
 - Vendor-Type
 - Vendor-Length
 - Vendor-Data

Figure 1 shows the packet format for a VSA encapsulated "behind" attribute 26.

Figure 1 VSA Encapsulated Behind Attribute 26


Note

It is up to the vendor to specify the format of their VSA. The Attribute-Specific field (also known as Vendor-Data) is dependent on the vendor's definition of that attribute.

[Table 2](#) lists supported vendor-specific RADIUS attributes (IETF attribute 26). [Table 1](#) describes significant fields listed in the [Table 2](#).

Table 1 Vendor-Specific Attributes Table Field Descriptions

Field	Description
Number	All attributes listed in the following table are extensions of IETF attribute 26.
Vendor-Specific Command Codes	A defined code used to identify a particular vendor. Code 9 defines Cisco VSAs, 311 defines Microsoft VSAs, and 529 defines Ascend VSAs.
Sub-Type Number	The attribute ID number. This number is much like the ID numbers of IETF attributes, except it is a “second layer” ID number encapsulated behind attribute 26.
Attribute	The ASCII string name of the attribute.
Description	Description of the attribute.

Table 2 Vendor-Specific RADIUS IETF Attributes

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
MS-CHAP Attributes				
26	311	1	MSCHAP-Response	Contains the response value provided by a PPP MS-CHAP user in response to the challenge. It is only used in Access-Request packets. This attribute is identical to the PPP CHAP Identifier. (RFC 2548)
26	311	11	MSCHAP-Challenge	Contains the challenge sent by a network access server to an MS-CHAP user. It can be used in both Access-Request and Access-Challenge packets. (RFC 2548)
VPDN Attributes				
26	9	1	l2tp-cm-local-window-size	Specifies the maximum receive window size for L2TP control messages. This value is advertised to the peer during tunnel establishment.

Table 2 **Vendor-Specific RADIUS IETF Attributes (continued)**

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	1	l2tp-drop-out-of-order	Respects sequence numbers on data packets by dropping those that are received out of order. This does not ensure that sequence numbers will be sent on data packets, just how to handle them if they are received.
26	9	1	l2tp-hello-interval	Specifies the number of seconds for the hello keepalive interval. Hello packets are sent when no data has been sent on a tunnel for the number of seconds configured here.
26	9	1	l2tp-hidden-avp	When enabled, sensitive AVPs in L2TP control messages are scrambled or hidden.
26	9	1	l2tp-nosession-timeout	Specifies the number of seconds that a tunnel will stay active with no sessions before timing out and shutting down.
26	9	1	l2tp-tos-reflect	Copies the IP ToS field from the IP header of each payload packet to the IP header of the tunnel packet for packets entering the tunnel at the LNS.
26	9	1	l2tp-tunnel-authen	If this attribute is set, it performs L2TP tunnel authentication.
26	9	1	l2tp-tunnel-password	Shared secret used for L2TP tunnel authentication and AVP hiding.
26	9	1	l2tp-udp-checksum	This is an authorization attribute and defines whether L2TP should perform UDP checksums for data packets. Valid values are “yes” and “no.” The default is no.

Store and Forward Fax Attributes

26	9	3	Fax-Account-Id-Origin	Indicates the account ID origin as defined by system administrator for the mmoip aaa receive-id or the mmoip aaa send-id commands.
26	9	4	Fax-Msg-Id=	Indicates a unique fax message identification number assigned by Store and Forward Fax.
26	9	5	Fax-Pages	Indicates the number of pages transmitted or received during this fax session. This page count includes cover pages.
26	9	6	Fax-Coverpage-Flag	Indicates whether or not a cover page was generated by the off-ramp gateway for this fax session. True indicates that a cover page was generated; false means that a cover page was not generated.
26	9	7	Fax-Modem-Time	Indicates the amount of time in seconds the modem sent fax data (x) and the amount of time in seconds of the total fax session (y), which includes both fax-mail and PSTN time, in the form x/y. For example, 10/15 means that the transfer time took 10 seconds, and the total fax session took 15 seconds.

Table 2 Vendor-Specific RADIUS IETF Attributes (continued)

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	8	Fax-Connect-Speed	Indicates the modem speed at which this fax-mail was initially transmitted or received. Possible values are 1200, 4800, 9600, and 14400.
26	9	9	Fax-Recipient-Count	Indicates the number of recipients for this fax transmission. Until e-mail servers support Session mode, the number should be 1.
26	9	10	Fax-Process-Abort-Flag	Indicates that the fax session was aborted or successful. True means that the session was aborted; false means that the session was successful.
26	9	11	Fax-Dsn-Address	Indicates the address to which DSNs will be sent.
26	9	12	Fax-Dsn-Flag	Indicates whether or not DSN has been enabled. True indicates that DSN has been enabled; false means that DSN has not been enabled.
26	9	13	Fax-Mdn-Address	Indicates the address to which MDNs will be sent.
26	9	14	Fax-Mdn-Flag	Indicates whether or not message delivery notification (MDN) has been enabled. True indicates that MDN had been enabled; false means that MDN had not been enabled.
26	9	15	Fax-Auth-Status	Indicates whether or not authentication for this fax session was successful. Possible values for this field are success, failed, bypassed, or unknown.
26	9	16	Email-Server-Address	Indicates the IP address of the e-mail server handling the on-ramp fax-mail message.
26	9	17	Email-Server-Ack-Flag	Indicates that the on-ramp gateway has received a positive acknowledgment from the e-mail server accepting the fax-mail message.
26	9	18	Gateway-Id	Indicates the name of the gateway that processed the fax session. The name appears in the following format: hostname.domain-name.
26	9	19	Call-Type	Describes the type of fax activity: fax receive or fax send.
26	9	20	Port-Used	Indicates the slot/port number of the Cisco AS5300 used to either transmit or receive this fax-mail.
26	9	21	Abort-Cause	If the fax session aborts, indicates the system component that signaled the abort. Examples of system components that could trigger an abort are FAP (Fax Application Process), TIFF (the TIFF reader or the TIFF writer), fax-mail client, fax-mail server, ESMTP client, or ESMTP server.
H323 Attributes				
26	9	23	Remote-Gateway-ID (h323-remote-address)	Indicates the IP address of the remote gateway.

Table 2 *Vendor-Specific RADIUS IETF Attributes (continued)*

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	24	Connection-ID (h323-conf-id)	Identifies the conference ID.
26	9	25	Setup-Time (h323-setup-time)	Indicates the setup time for this connection in Coordinated Universal Time (UTC) formerly known as Greenwich Mean Time (GMT) and Zulu time.
26	9	26	Call-Origin (h323-call-origin)	Indicates the origin of the call relative to the gateway. Possible values are originating and terminating (answer).
26	9	27	Call-Type (h323-call-type)	Indicates call leg type. Possible values are telephony and VoIP .
26	9	28	Connect-Time (h323-connect-time)	Indicates the connection time for this call leg in UTC.
26	9	29	Disconnect-Time (h323-disconnect-time)	Indicates the time this call leg was disconnected in UTC.
26	9	30	Disconnect-Cause (h323-disconnect-cause)	Specifies the reason a connection was taken offline per Q.931 specification.
26	9	31	Voice-Quality (h323-voice-quality)	Specifies the impairment factor (ICPIF) affecting voice quality for a call.
26	9	33	Gateway-ID (h323-gw-id)	Indicates the name of the underlying gateway.

Large Scale Dialout Attributes

26	9	1	callback-dialstring	Defines a dialing string to be used for callback.
26	9	1	data-service	No description available.
26	9	1	dial-number	Defines the number to dial.
26	9	1	force-56	Determines whether the network access server uses only the 56 K portion of a channel, even when all 64 K appear to be available.
26	9	1	map-class	Allows the user profile to reference information configured in a map class of the same name on the network access server that dials out.
26	9	1	send-auth	Defines the protocol to use (PAP or CHAP) for username-password authentication following CLID authentication.

Table 2 Vendor-Specific RADIUS IETF Attributes (continued)

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	1	send-name	<p>PPP name authentication. To apply for PAP, do not configure the ppp pap sent-name password command on the interface. For PAP, “preauth:send-name” and “preauth:send-secret” will be used as the PAP username and PAP password for outbound authentication. For CHAP, “preauth:send-name” will be used not only for outbound authentication, but also for inbound authentication. For a CHAP inbound case, the NAS will use the name defined in “preauth:send-name” in the challenge packet to the caller box.</p> <p>Note The send-name attribute has changed over time: Initially, it performed the functions now provided by both the send-name and remote-name attributes. Because the remote-name attribute has been added, the send-name attribute is restricted to its current behavior.</p>
26	9	1	send-secret	<p>PPP password authentication. The vendor-specific attributes (VSAs) “preauth:send-name” and “preauth:send-secret” will be used as the PAP username and PAP password for outbound authentication. For a CHAP outbound case, both “preauth:send-name” and “preauth:send-secret” will be used in the response packet.</p>
26	9	1	remote-name	<p>Provides the name of the remote host for use in large-scale dial-out. Dialer checks that the large-scale dial-out remote name matches the authenticated name, to protect against accidental user RADIUS misconfiguration. (For example, dialing a valid phone number but connecting to the wrong router.)</p>
Miscellaneous Attributes				
26	9	2	Cisco-NAS-Port	<p>Specifies additional vendor specific attribute (VSA) information for NAS-Port accounting. To specify additional NAS-Port information in the form an Attribute-Value Pair (AVPair) string, use the radius-server vsa send global configuration command.</p> <p>Note This VSA is typically used in Accounting, but may also be used in Authentication (Access-Request) packets.</p>
26	9	1	min-links	<p>Sets the minimum number of links for MLP.</p>

Table 2 Vendor-Specific RADIUS IETF Attributes (continued)

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	1	proxyacl#<n>	Allows users to configure the downloadable user profiles (dynamic ACLs) by using the authentication proxy feature so that users can have the configured authorization to permit traffic going through the configured interfaces.
26	9	1	spi	Carries the authentication information needed by the home agent to authenticate a mobile node during registration. The information is in the same syntax as the ip mobile secure host <addr> configuration command. Basically it contains the rest of the configuration command that follows that string, verbatim. It provides the Security Parameter Index (SPI), key, authentication algorithm, authentication mode, and replay protection timestamp range.

For more information on configuring your NAS to recognize and use VSAs, refer to the section [“Configuring Router to Use Vendor-Specific RADIUS Attributes”](#) of the chapter [“Configuring RADIUS.”](#)

RADIUS Disconnect-Cause Attribute Values

Disconnect-cause attribute values specify the reason a connection was taken offline. The attribute values are sent in Accounting request packets. These values are sent at the end of a session, even if the session fails to be authenticated. If the session is not authenticated, the attribute can cause stop records to be generated without first generating start records.

[Table 3](#) lists the cause codes, values, and descriptions for the Disconnect-Cause (195) attribute.



Note

The Disconnect-Cause is incremented by 1000 when it is used in RADIUS AVPairs; for example, disc-cause 4 becomes 1004.

Table 3 Disconnect-Cause Attribute Values

Cause Code	Value	Description
0	No-Reason	No reason is given for the disconnect.
1	No-Disconnect	The event was not disconnected.
2	Unknown	Reason unknown.
3	Call-Disconnect	The call has been disconnected.
4	CLID-Authentication-Failure	Failure to authenticate number of the calling-party.
9	No-Modem-Available	A modem is not available to connect the call.

Table 3 *Disconnect-Cause Attribute Values (continued)*

Cause Code	Value	Description
10	No-Carrier	No carrier detected. Note Codes 10, 11, and 12 can be sent if there is a disconnection during initial modem connection.
11	Lost-Carrier	Loss of carrier.
12	No-Detected-Result-Codes	Failure to detect modem result codes.
20	User-Ends-Session	User terminates a session. Note Codes 20, 22, 23, 24, 25, 26, 27, and 28 apply to EXEC sessions.
21	Idle-Timeout	Timeout waiting for user input. Codes 21, 100, 101, 102, and 120 apply to all session types.
22	Exit-Telnet-Session	Disconnect due to exiting Telnet session.
23	No-Remote-IP-Addr	Could not switch to SLIP/PPP; the remote end has no IP address.
24	Exit-Raw-TCP	Disconnect due to exiting raw TCP.
25	Password-Fail	Bad passwords.
26	Raw-TCP-Disabled	Raw TCP disabled.
27	Control-C-Detected	Control-C detected.
28	EXEC-Process-Destroyed	EXEC process destroyed.
29	Close-Virtual-Connection	User closes a virtual connection.
30	End-Virtual-Connection	Virtual connected has ended.
31	Exit-Rlogin	User exists Rlogin.
32	Invalid-Rlogin-Option	Invalid Rlogin option selected.
33	Insufficient-Resources	Insufficient resources.
40	Timeout-PPP-LCP	PPP LCP negotiation timed out. Note Codes 40 through 49 apply to PPP sessions.
41	Failed-PPP-LCP-Negotiation	PPP LCP negotiation failed.
42	Failed-PPP-PAP-Auth-Fail	PPP PAP authentication failed.
43	Failed-PPP-CHAP-Auth	PPP CHAP authentication failed.
44	Failed-PPP-Remote-Auth	PPP remote authentication failed.
45	PPP-Remote-Terminate	PPP received a Terminate Request from remote end.
46	PPP-Closed-Event	Upper layer requested that the session be closed.
47	NCP-Closed-PPP	PPP session closed because there were no NCPs open.
48	MP-Error-PPP	PPP session closed because of an MP error.
49	PPP-Maximum-Channels	PPP session closed because maximum channels were reached.
50	Tables-Full	Disconnect due to full terminal server tables.
51	Resources-Full	Disconnect due to full internal resources.
52	Invalid-IP-Address	IP address is not valid for Telnet host.
53	Bad-Hostname	Hostname cannot be validated.

Table 3 *Disconnect-Cause Attribute Values (continued)*

Cause Code	Value	Description
54	Bad-Port	Port number is invalid or missing.
60	Reset-TCP	TCP connection has been reset. Note Codes 60 through 67 apply to Telnet or raw TCP sessions.
61	TCP-Connection-Refused	TCP connection has been refused by the host.
62	Timeout-TCP	TCP connection has timed out.
63	Foreign-Host-Close-TCP	TCP connection has been closed.
64	TCP-Network-Unreachable	TCP network is unreachable.
65	TCP-Host-Unreachable	TCP host is unreachable.
66	TCP-Network-Admin Unreachable	TCP network is unreachable for administrative reasons.
67	TCP-Port-Unreachable	TCP port is unreachable.
100	Session-Timeout	Session timed out.
101	Session-Failed-Security	Session failed for security reasons.
102	Session-End-Callback	Session terminated due to callback.
120	Invalid-Protocol	Call refused because the detected protocol is disabled.
150	RADIUS-Disconnect	Disconnected by RADIUS request.
151	Local-Admin-Disconnect	Administrative disconnect.
152	SNMP-Disconnect	Disconnected by SNMP request.
160	V110-Retries	Allowed V.110 retries have been exceeded.
170	PPP-Authentication-Timeout	PPP authentication timed out.
180	Local-Hangup	Disconnected by local hangup.
185	Remote-Hangup	Disconnected by remote end hangup.
190	T1-Quiesced	Disconnected because T1 line was quiesced.
195	Call-Duration	Disconnected because the maximum duration of the call was exceeded.
600	VPN-User-Disconnect	Call disconnected by client (through PPP). Code is sent if the LNS receives a PPP terminate request from the client.
601	VPN-Carrier-Loss	Loss of carrier. This can be the result of a physical line going dead. Code is sent when a client is unable to dial out using a dialer.
602	VPN-No-Resources	No resources available to handle the call. Code is sent when the client is unable to allocate memory (running low on memory).
603	VPN-Bad-Control-Packet	Bad L2TP or L2F control packets. This code is sent when an invalid control packet, such as missing mandatory Attribute-Value pairs (AVP), from the peer is received. When using L2TP, the code will be sent after six retransmits; when using L2F, the number of retransmits is user configurable. Note VPN-Tunnel-Shut will be sent if there are active sessions in the tunnel.

Table 3 **Disconnect-Cause Attribute Values (continued)**

Cause Code	Value	Description
604	VPN-Admin-Disconnect	Administrative disconnect. This can be the result of a VPN soft shutdown, which is when a client reaches maximum session limit or exceeds maximum hopcount. Code is sent when a tunnel is brought down by issuing the clear vpdn tunnel command.
605	VPN-Tunnel-Shut	Tunnel teardown or tunnel setup has failed. Code is sent when there are active sessions in a tunnel and the tunnel goes down. Note This code is <i>not</i> sent when tunnel authentication fails.
606	VPN-Local-Disconnect	Call is disconnected by LNS PPP module. Code is sent when the LNS sends a PPP terminate request to the client. It indicates a normal PPP disconnection initiated by the LNS.
607	VPN-Session-Limit	VPN soft shutdown is enabled. Code is sent when a call has been refused due to any of the soft shutdown restrictions previously mentioned.
608	VPN-Call-Redirect	VPN call redirect is enabled.

For Q.850 cause codes and descriptions, see the section “Internal Cause Codes for SIP and H.323” in the chapter “Cause Codes and Debug Values” of the *Cisco IOS Voice Troubleshooting and Monitoring*.

Additional References

The following sections provide references related to RADIUS Vendor-Specific Attributes (VSA) and RADIUS Disconnect-Cause Attribute Values.

Related Documents

Related Topic	Document Title
Security Features	Cisco IOS Security Configuration Guide, Release 12.4
Security Server Protocols	Part 2: Security Server Protocols in the Cisco IOS Security Configuration Guide, Release 12.4
RADIUS Configuration	Configuring RADIUS

Standards

Standard	Title
Internet Engineering Task Force (IETF) Internet Draft: Network Access Servers Requirements	Network Access Servers Requirements: Extended RADIUS Practices

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2865	Remote Authentication Dial In User Service (RADIUS)

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Feature Information for RADIUS Vendor-Specific Attributes (VSA) and RADIUS Disconnect-Cause Attribute Values

Table 4 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 4 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 4 Feature Information for RADIUS Vendor-Specific Attributes (VSA) and RADIUS Disconnect-Cause Attribute Values

Feature Name	Releases	Feature Information
RADIUS Vendor-Specific Attributes (VSA) and RADIUS Disconnect-Cause Attribute Values	12.0(30)S3s 12.3(11)YS1 12.2(33)SRC	This document discusses the Internet Engineering Task Force (IETF) draft standard, which specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26). Attribute 26 encapsulates vendor specific attributes, thereby, allowing vendors to support their own extended attributes otherwise not suitable for general use. This feature was introduced into Cisco IOS Release 12.0(30)S3s. This feature was integrated into Cisco IOS Release 12.3(11)YS1 This feature was integrated into Cisco IOS Release 12.2(33)SRC.
Accounting of VPDN Disconnect Cause	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.
Vendor-Specific RADIUS Attributes	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2005, 2007 Cisco Systems, Inc. All rights reserved.



Connect-Info RADIUS Attribute 77

First Published: September 22, 2002

Last Published: December 17, 2007

The Connect-Info RADIUS Attribute 77 feature enables the Network Access Server (NAS) to report Connect-Info (attribute 77) in RADIUS accounting “start” and “stop” records that are sent to the RADIUS client (dial-in modem). These records allow the transmit and receive connection speeds, modulation, and compression to be compared in order to analyze a user session over a dial-in modem where speeds are often different at the end of the connection (after negotiation).

When the network access server (NAS) sends attribute 77 in accounting “start” and “stop” records, the connect rates can be measured across the platform. The “transmit” speed (the speed at which the NAS modem sends information) and “receive” speed (the speed at which the NAS receives information) can be recorded to determine whether user modem connections renegotiate to lower speeds shortly into a session. If the transmit and receive speeds are different from each other, attribute 77 reports both speeds, which allows the modem connection speeds that each customer gets from their session.

Attribute 77 is also used to send the Class string for broadband connections such as PPPoX, physical connection speeds for dial access, and the VRF string for any sessions on router interfaces defined with **ip vrf forwarding** command.



Note

This feature requires no configuration.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Connect-Info RADIUS Attribute 77” section on page 5](#).

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Contents

- [Prerequisites for Connect-Info RADIUS Attribute 77, page 2](#)
- [How to Verify the Connect-Info RADIUS Attribute 77, page 2](#)
- [Configuration Example for Connect-Info RADIUS Attribute 77, page 3](#)
- [Additional References, page 3](#)
- [Command Reference, page 4](#)
- [Feature Information for Connect-Info RADIUS Attribute 77, page 5](#)

Prerequisites for Connect-Info RADIUS Attribute 77

Before the NAS can send attribute 77 in accounting “start” and “stop” records, you must perform the following tasks:

- Configure your NAS for authentication, authorization, and accounting (AAA) and to accept incoming modem calls.
- Enable AAA accounting by using the **aaa accounting network default start-stop group radius** command in global configuration mode.
- Change the modem poll timer by using the **modem link-info poll time** command in global configuration mode. (Changing the modem poll timer is required on all supported platforms *except* the Cisco AS5400).

How to Verify the Connect-Info RADIUS Attribute 77

To verify attribute 77 in your accounting “start” and “stop” records, use the **debug radius** privileged EXEC command. The following example shows that Connect-Info appears in the first and last accounting attributes:

Router# **debug radius**

```
RADIUS: code=Acct-Request id=04 len=0134
      authenticator=BE A2 F3 BD EE CE 89 C7 - 48 19 32 F5 79 84 94 D5
      T=Connect-Info[77]                      L=17 V="31200/33600 V34+/LAPM"
      T=Acct-Status-Type[40]                  L=06 V=Start                      [1]
      ...

RADIUS: code=Acct-Request id=07 len=0226
      authenticator=06 AC 03 10 4A 84 44 A4 - 6F D9 68 AA B3 90 44 CB
      ...
      T=Connect-Info[77]                      L=1F V="33600 V34+/LAPM (31200/336"
      T=Acct-Status-Type[40]                  L=06 V=Stop                          [2]
      ...
```



Note

If the modem negotiation speeds are different, the speeds are shown in a bracket format at the end of the call.

Configuration Example for Connect-Info RADIUS Attribute 77

This section provides the following configuration example:

- [Configure NAS for AAA and Incoming Modem Calls Example](#)

Configure NAS for AAA and Incoming Modem Calls Example

The following example is a sample NAS configuration for AAA and incoming modem calls:

```
interface Serial0:15
  no ip address
  isdn switch-type primary-net5
  isdn incoming-voice modem
!
interface Async1
  ip address 10.0.0.10 255.0.0.0
  encapsulation ppp
  async default routing
  async mode interactive
  no peer default ip address
  ppp authentication chap
!
line 1
  modem InOu
  transport preferred none
  transport input all
  autoselect ppp
!
```

Additional References

The following sections provide references related to the Connect-Info RADIUS Attribute 77 feature.

Related Documents

Related Topic	Document Title
IOS dial technologies	“Configuring and Managing Cisco Access Servers and Dial Shelves” chapter of the <i>Cisco IOS Dial Technologies Configuration Guide</i>
	Cisco IOS Dial Technologies Command Reference
RADIUS and security related information	Cisco IOS Security Command Reference

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2869	<i>RADIUS Extensions</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

No commands are introduced or modified in the feature documented in this module. For information about commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

Feature Information for Connect-Info RADIUS Attribute 77

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Connect-Info RADIUS Attribute 77

Feature Name	Releases	Feature Information
Connect-Info RADIUS Attribute 77	12.2(11)T 12.2(33)SRC Cisco IOS XE Release 2.1	<p>The Connect-Info RADIUS Attribute 77 feature enables the network access server (NAS) to report Connect-Info (attribute 77) in RADIUS accounting “start” and “stop” records that are sent to the RADIUS client (dial-in modem). These “start” and “stop” records allow the transmit and receive connection speeds, modulation, and compression to be compared in order to analyze a user session over a dial-in modem where speeds are often different at the end of the connection (after negotiation).</p> <p>This feature was introduced on Cisco IOS Release 12.2(11)T.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRC.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers</p> <p>This feature supports the following platforms:</p> <ul style="list-style-type: none"> • Cisco AS5300 series • Cisco AS5400 series • Cisco AS5800 series • Cisco AS5850 series

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2002, 2007 Cisco Systems, Inc. All rights reserved.



Encrypted Vendor-Specific Attributes

First Published: February 25, 2002

Last Updated: December 3, 2007

The Encrypted Vendor-Specific Attributes feature provides users with a way to centrally manage filters at a RADIUS server and supports the following types of string vendor-specific attributes (VSAs):

- **Tagged String VSA** (similar to Cisco VSA type 1 (Cisco:AVPair (1)) except that this new VSA is tagged)
- **Encrypted String VSA** (similar to Cisco VSA type 1 except that this new VSA is encrypted)
- **Tagged and Encrypted String VSA** (similar to Cisco VSA type 1 except that this new VSA is tagged and encrypted)

Cisco:AVPairs specify additional authentication and authorization information in the form an Attribute-Value Pair (AVPair) string. When Internet Engineering Task Force (IETF) RADIUS attribute 26 (Vendor-Specific) is transmitted with a vendor-Id number of “9” and a vendor-type value of “1” (which means that it is a Cisco AVPair), the RADIUS user profile format for a Cisco AVPair looks as follows: Cisco:AVPair = “protocol:attribute=value”.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Encrypted Vendor-Specific Attributes” section on page 7](#).

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2002, 2006, 2007 Cisco Systems, Inc. All rights reserved.

Contents

- [Prerequisites for Encrypted Vendor-Specific Attributes, page 2](#)
- [Information About Encrypted Vendor-Specific Attributes, page 2](#)
- [How to Verify Encrypted Vendor-Specific Attributes, page 4](#)
- [Configuration Examples for Encrypted Vendor-Specific Attributes, page 4](#)
- [Additional References, page 5](#)
- [Command Reference, page 6](#)
- [Feature Information for Encrypted Vendor-Specific Attributes, page 7](#)

Prerequisites for Encrypted Vendor-Specific Attributes

Before the RADIUS server can accept tagged and encrypted VSAs, you must configure your server for AAA authentication and authorization and to accept PPP calls.

For information on performing these tasks, refer to the chapter “PPP Configuration” in the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.4 and the chapters “Configuring Authentication” and “Configuring Authorization” in the *Cisco IOS Security Configuration Guide*, Release 12.4.

Information About Encrypted Vendor-Specific Attributes

The following sections describe packet encryption formats for the different VSAs:

- [Tagged String VSA](#)
- [Encrypted String VSA](#)
- [Tagged and Encrypted String VSA](#)

Tagged String VSA

Figure 1 displays the packet format for the Tagged String VSA:

Figure 1 Tagged String VSA Format

Tagged String VSA

Type (26)	Length	Vendor-ID (9)	
Vendor-ID (cont.)		Vendor-type (1)	Vendor-length
Tag	Attribute string		

62354

To retrieve the correct value, the Tag field must be parsed correctly. The value for this field can range only from 0x01 through 0x1F. If the value is not within the specified range, the RADIUS server ignores the value and considers the Tag field to be a part of the Attribute String field.

Encrypted String VSA

Figure 2 displays the packet format for the Encrypted String VSA:

Figure 2 *Encrypted String VSA Format*

Encrypted String VSA

Type (26)	Length	Vendor-ID (9)	
Vendor-ID (cont.)		Vendor-type (36)	Vendor-length
Salt	Salt (cont.)	Attribute string	

62355

The Salt field ensures the uniqueness of the encryption key that is used to encrypt each instance of the VSA. The first and most significant bit of the Salt field must be set to 1.



Note

Vendor-type (36) indicates that the attribute is an encrypted string VSA.

Tagged and Encrypted String VSA

Figure 3 displays the packet formats for each of the newly supported VSAs:

Figure 3 *Tagged and Encrypted String VSA Format*

Tagged and Encrypted String VSA

Type (26)	Length	Vendor-ID (9)	
Vendor-ID (cont.)		Vendor-type (36)	Vendor-length
*Tag	Salt	Salt (cont.)	Attribute string

62356

This VSA is similar to encrypted string VSAs *except* this VSA has an additional Tag field. If the Tag field is not within the valid range (0x01 through 0x1F), it is considered to be part of the Salt field.

How to Verify Encrypted Vendor-Specific Attributes

The Encrypted Vendor-Specific Attributes feature requires no configuration. To verify that RADIUS-tagged and encrypted VSAs are being sent from the RADIUS server, use the following command in privileged EXEC mode:

Command	Purpose
Router# debug radius	Displays information associated with RADIUS. The output of this command shows whether tagged and encrypted VSAs are being sent from the RADIUS server.

Configuration Examples for Encrypted Vendor-Specific Attributes

This section provides the following configuration examples:

- [NAS Configuration Example, page 4](#)
- [RADIUS User Profile with a Tagged and Encrypted VSA Example, page 4](#)

NAS Configuration Example

The following example shows how to configure a network access server (NAS) with a basic configuration using tagged and encrypted VSAs. (This example assumes that the configuration required to make PPP calls is already enabled.)

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
!
radius-server host 10.2.2.2 auth-port 1645 acct-port 1646
radius-server key cisco
```

RADIUS User Profile with a Tagged and Encrypted VSA Example

The following is an example of user profile on a RADIUS server that supports tagged and encrypted string VSAs:

```
mascot Password = "cisco"
Service-Type = NAS-Prompt,
Framed-Protocol = PPP,
Cisco:Cisco-Enc = "ip:route=10.0.0.0 255.0.0.0"
Cisco.attr Cisco-Enc 36 tag-encstr(*,*)
```

Additional References

The following sections provide references related to the Encrypted Vendor-Specific Attributes.

Related Documents

Related Topic	Document Title
RADIUS Attributes	<i>Cisco IOS Security Configuration Guide</i> , Release 12.4

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2865	Remote Authentication Dial In User Service (RADIUS)
RFC 2868	RADIUS Attributes for Tunnel Protocol Support

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Command Reference

No commands are introduced or modified in the feature documented in this module. For information about commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

Feature Information for Encrypted Vendor-Specific Attributes

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Encrypted Vendor-Specific Attributes

Feature Name	Releases	Feature Information
Encrypted Vendor-Specific Attributes	12.2(8)T 12.2(28)SB 12.2(33)SRC	<p>The Encrypted Vendor-Specific Attributes feature provides users with a way to centrally manage filters at a RADIUS server and supports the Tagged String, Encrypted String, and Tagged and Encrypted String vendor-specific attributes (VSAs).</p> <p>This feature was introduced in Cisco IOS Release 12.2(8)T.</p> <p>This feature was integrated into Cisco IOS Release 12.2(28)SB.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRC.</p>

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Local AAA Server

First Published: March 28, 2005

Last Updated: January 2 2008

The Local AAA Server feature allows you to configure your router so that user authentication and authorization attributes currently available on AAA servers are available locally on the router. The attributes can be added to existing framework, such as the local user database or subscriber profile. The local AAA server provides access to the complete dictionary of Cisco IOS supported attributes.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Local AAA Server” section on page 14](#).

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Local AAA Server, page 2](#)
- [Information About Local AAA Server, page 2](#)
- [How to Configure Local AAA Server, page 3](#)
- [Configuration Examples for Local AAA Server, page 10](#)
- [Additional References, page 12](#)
- [Command Reference, page 13](#)
- [“Feature Information for Local AAA Server” section on page 14](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2005-2008 Cisco Systems, Inc. All rights reserved.

Prerequisites for Local AAA Server

- Before using this feature, you must have the **aaa new-model** command enabled.

Information About Local AAA Server

To configure the Local AAA Server feature, you should understand the following concepts:

- [Local Authorization Attributes: Overview, page 2](#)
- [Local AAA Attribute Support, page 2](#)
- [AAA Attribute Lists, page 3](#)
- [Validation of Attributes, page 3](#)

Local Authorization Attributes: Overview

The AAA subsystem (authentication, authorization, and accounting) is responsible for managing all supported attributes that are available to the various services within the Cisco IOS software. As such, it maintains its own local dictionary of all supported attributes. However, prior to Cisco IOS Release 12.3(14)T, most of these authorization options were not available for local (on-box) authorizations.

Local AAA Attribute Support

Effective with Cisco IOS Release 12.3(14)T, you can configure your router so that AAA authentication and authorization attributes currently available on AAA servers are made available on existing Cisco IOS devices. The attributes can be added to existing framework, such as the local user database or subscriber profile. For example, an attribute list can now be added to an existing username, providing the ability for the local user database to act as a local AAA server. For situations in which the local username list is relatively small, this flexibility allows you to provide complete user authentication or authorization locally within the Cisco IOS software without having a AAA server. This ability can allow you to maintain your user database locally or provide a failover local mechanism without having to sacrifice policy options when defining local users.

A subscriber profile allows domain-based clients to have policy applied at the end-user service level. This flexibility allows common policy to be set for all users under a domain in one place and applied there whether or not user authorization is done locally. Effective with Cisco IOS Release 12.3(14)T, an attribute list can be added to the subscriber profile, allowing the profile to apply all attributes that can be applied to services using AAA servers. Attributes that are configured under the AAA attribute list are merged with the existing attributes that are generated with the existing subscriber profile and passed to the Subscriber Server Switch (SSS) framework for application.

**Note**

Accounting is still done on a AAA server and is not supported by this feature.

AAA Attribute Lists

AAA attribute lists define user profiles that are local to the router. Every attribute that is known to the AAA subsystem is made available for configuration.

The AAA attributes that are defined in the AAA attribute list are standard RADIUS or TACACS+ attributes. However, they are in the Cisco IOS internal format for that attribute. The attributes must be converted from the RADIUS format (for a RADIUS case) to the Cisco IOS AAA interface format. TACACS+ attributes are generally identical to the Cisco IOS AAA interface format.

Converting from RADIUS Format to Cisco IOS AAA Format

You can use the **show aaa attributes protocol radius** command to get the Cisco IOS AAA format of the Internet Engineering Task Force (IETF) RADIUS attribute. The **show** command output provides a complete list of all the AAA attributes that are supported.

**Note**

The conversion from RADIUS to internal AAA is done internally within the AAA framework. RADIUS vendor-specific attributes (VSAs) are usually accurately reflected during conversion. TACACS+ attributes are also usually identical to the local attributes and do not require the conversion process. However, IETF numbered attributes and some special VSAs often require the conversion process.

Validation of Attributes

Attributes are not validated at configuration. The AAA subsystem “knows” only the format that is expected by the services when the service defines a given attribute inside a definition file. However, it cannot validate the attribute information itself. This validation is done by a service when it first uses the attribute. This validation applies whether the AAA server is RADIUS or TACACS+. Thus, if you are not familiar with configuring a AAA server, it is advisable that you test your attribute list on a test device with the service that will be using the list before configuring and using it in a production environment.

How to Configure Local AAA Server

This section contains the following procedures:

- [Defining a AAA Attribute List, page 3](#) (required)
- [Defining a Subscriber Profile, page 6](#) (required)
- [Monitoring and Troubleshooting a Local AAA Server, page 7](#) (optional)

Defining a AAA Attribute List

To define an AAA attribute list, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **aaa attribute list** *list-name*
4. **attribute type** {*name*} {*value*} [**service** *service*] [**protocol** *protocol*]
5. **attribute type** {*name*} {*value*} [**service** *service*] [**protocol** *protocol*]
6. **attribute type** {*name*} {*value*} [**service** *service*] [**protocol** *protocol*]
7. **attribute type** {*name*} {*value*}
8. **attribute type** {*name*} {*value*}
9. **attribute type** {*name*} {*value*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa attribute list list-name Example: Router (config)# aaa attribute list TEST	Defines a AAA attribute list.
Step 4	attribute type {name} {value} [service service] [protocol protocol] Example: Router (config)# attribute type addr-pool "pool name" service ppp protocol ip	Defines an IP address pool to use.
Step 5	attribute type {name} {value} [service service] [protocol protocol] Example: Router (config)# attribute type ip-unnumbered "loopback number" service ppp protocol ip	Defines the loopback interface to use.
Step 6	attribute type {name} {value} [service service] [protocol protocol] Example: Router (config)# attribute type vrf-id "vrf name" service ppp protocol ip	Defines the virtual route forwarding (VRF) to use.
Step 7	attribute type {name} {value} Example: Router (config)# attribute type ppp-authen-list "aaa list name"	Defines the AAA authentication list to use.
Step 8	attribute type {name} {value} Example: Router (config)# attribute type ppp-author-list "aaa list name"	Defines the AAA authorization list to use.
Step 9	attribute type {name} {value} Example: Router (config)# attribute type ppp-acct-list "aaa list name"	Defines the AAA accounting list to use.

Defining a Subscriber Profile

To define a subscriber profile, perform the following steps.

**Note**

RADIUS users should use the **show aaa attributes** command to map the RADIUS version of the particular attribute to the Cisco IOS AAA version of the string attribute. See the example “[Mapping from the RADIUS Version of a Particular Attribute to the Cisco IOS AAA Version: Example, page 11.](#)”

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber authorization enable**
4. **subscriber profile** *domain-name*
5. **service local**
6. **exit**
7. **aaa attribute list** *list-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	subscriber authorization enable Example: Router (config)# subscriber authorization enable	Enables subscriber authorization.
Step 4	subscriber profile domain-name Example: Router (config)# subscriber profile cisco1.com	Specifies the username domain that has to be matched and enters subscriber profile configuration mode.
Step 5	service local Example: Router (subscriber-profile)# service local	Specifies that local subscriber authorization should be performed.
Step 6	exit Example: Router (subscriber-profile)# exit	Exits subscriber profile configuration mode.
Step 7	aaa attribute list list-name Example: Router (config)# aaa attribute list TEST	Defines the AAA attribute list from which RADIUS attributes are retrieved.

Monitoring and Troubleshooting a Local AAA Server

The following debug commands may be helpful in monitoring and troubleshooting, especially to ensure that domain-based service authorization is being triggered and that location authorization is being called on the local AAA server, which triggers the service.

SUMMARY STEPS

1. enable
2. debug aaa authentication
3. debug aaa authorization
4. debug aaa per-user

5. **debug ppp authentication**
6. **debug ppp error**
7. **debug ppp forward**
8. **debug ppp negotiation**
9. **debug radius**
10. **debug sss error**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	debug aaa authentication Example: Router# debug aaa authentication	Displays the methods of authentication being used and the results of these methods.
Step 3	debug aaa authorization Example: Router# debug aaa authorization	Displays the methods of authorization being used and the results of these methods.
Step 4	debug aaa per-user Example: Router# debug aaa per-user	Displays information about PPP session per-user activities.
Step 5	debug ppp authentication Example: Router# debug ppp authentication	Indicates whether a client is passing authentication.
Step 6	debug ppp error Example: Router (config)# debug ppp error	Displays protocol errors and error statistics that are associated with PPP connection negotiation and operation.
Step 7	debug ppp forward Example: Router# debug ppp forward	Displays who is taking control of a session.
Step 8	debug ppp negotiation Example: Router# debug ppp negotiation	Displays PPP packets sent during PPP startup, where PPP options are negotiated.
Step 9	debug radius Example: Router# debug radius	Displays information about the RADIUS server.
Step 10	debug sss error Example: Router# debug sss error	Displays diagnostic information about errors that may occur during SSS call setup.

Configuration Examples for Local AAA Server

This section contains the following configuration examples:

- [Local AAA Server: Example, page 10](#)
- [Mapping from the RADIUS Version of a Particular Attribute to the Cisco IOS AAA Version: Example, page 11](#)

Local AAA Server: Example

The following example shows a Point to Point over Ethernet (PPPoE) group named “bba-group” that is configured for subscriber profile cisco.com (thus, any user with the domain name cisco.com will execute the subscriber profile cisco.com authorization policy). The cisco.com subscriber profile is configured to attach the AAA attribute list “TEST,” which has both “ip vrf forwarding” and “ip unnumbered” configured for PPP service under Link Control Protocol (LCP) negotiation. This configuration will essentially cause the named attributes to be applied on the session with the cisco.com domain under the bba-group “pppoe grp1.”

```
aaa authentication ppp template1 local
aaa authorization network template1 local
!
aaa attribute list TEST
  attribute type interface-config "ip unnumbered FastEthernet0" service ppp protocol lcp
  attribute type interface-config "ip vrf forwarding blue" service ppp protocol lcp
!
ip vrf blue
  description vrf blue template1
  rd 1:1
  route-target export 1:1
  route-target import 1:1
!
subscriber authorization enable
!
subscriber profile cisco.com
  service local
  aaa attribute list TEST
!
bba-group pppoe grp1
  virtual-template 1
  service profile cisco.com
!
interface Virtual-Template1
  no ip address
  no snmp trap link-status
  no peer default ip address
  no keepalive
  ppp authentication pap template1
  ppp authorization template1
!
```



Note

In some versions of Cisco IOS software, it is better to use the explicit attribute instead of interface-config because it provides better scalability (full VAccess interfaces are not required, and sub interfaces could be used to provide the service). In such a case, you might configure “attribute type ip-unnumbered ‘FastEthernet0’ service ppp protocol ip” instead of “attribute type interface-config ‘ip unnumbered FastEthernet0’ service ppp protocol lcp.”

Mapping from the RADIUS Version of a Particular Attribute to the Cisco IOS AAA Version: Example

The following output example of the **show aaa attributes** command lists RADIUS attributes, which can be used when configuring this feature.

```
Router# show aaa attributes protocol radius
```

IETF defined attributes:

Type=4	Name=acl	Format=Ulong
Protocol:RADIUS		
Unknown	Type=11	Name=Filter-Id
		Format=Binary

Converts attribute 11 (Filter-Id) of type Binary into an internal attribute named "acl" of type Ulong. As such, one can configure this attributes locally by using the attribute type "acl."

Cisco VSA attributes:

Type=157	Name=interface-config	Format=String
----------	-----------------------	---------------

Simply expects a string for the attribute of type "interface-config."

**Note**

The **aaa attribute list** command requires the Cisco IOS AAA version of an attribute, which is defined in the "Name" field above.

Additional References

The following sections provide references related to Local AAA Server.

Related Document

Related Topic	Document Title
AAA, AAA attribute lists, AAA method lists, and subscriber profiles	The chapter “ Configuring Local AAA Server, User Database—Domain to VRF ” in <i>Cisco 10000 Series Broadband Aggregation and Leased-Line Configuration Guide</i>
Cisco IOS security commands	Cisco IOS Security Command Reference

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or a Cisco IOS master commands list.

- **aaa attribute list**
- **attribute type**

Feature Information for Local AAA Server

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

[Table 1](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Local AAA Server

Feature Name	Releases	Feature Information
Local AAA Server	12.3(14)T 12.2(28)SB 12.2(33)SRC Cisco IOS XE Release 2.1	The Local AAA Server feature allows you to configure your router so that user authentication and authorization attributes currently available on AAA servers are available locally on the router. The attributes can be added to existing framework, such as the local user database or subscriber profile. The local AAA server provides access to the complete dictionary of Cisco IOS supported attributes. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2000-2008 Cisco Systems, Inc. All rights reserved.



Per-User QoS via AAA Policy Name

First Published: March 31, 2000

Last Updated: January 2, 2008

The Per-User QoS via AAA Policy Name feature provides the ability to download a policy name that describes quality of service (QoS) parameters for a user session from a RADIUS server and apply them for the particular session.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Command Reference](#)” section on page 6.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Per-User QoS via AAA Policy Name, page 2](#)
- [Information About Per-User QoS via AAA Policy Name, page 2](#)
- [How to Configure Per-User QoS via AAA Policy Name, page 2](#)
- [Configuration Examples for Per-User QoS via AAA Policy Name, page 3](#)
- [Additional References, page 5](#)
- [Command Reference, page 6](#)
- [Feature Information for Per-User QoS via AAA Policy Name, page 6](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2000–2008 Cisco Systems, Inc. All rights reserved.

Prerequisites for Per-User QoS via AAA Policy Name

Before you configure the Per-User QoS via AAA Policy Name feature, you must locally define on your router the policy whose name is received from the RADIUS server.

Information About Per-User QoS via AAA Policy Name

Effective with Cisco IOS Release 12.2(15)T, separate Cisco vendor-specific attributes (VSAs) are added for the service map.

To configure the Per-User QoS via AAA Policy Name feature, you must understand the following concept:

VSAs Added for Per-User QoS via AAA Policy Name

Two new VSAs have been added for the service map, and the VSAs will bypass the parser while applying the policy for a particular user or session. The new VSAs are as follows:

- vendor-id=9 (Cisco) Vendor type 37 for upstream traffic to input policy name
- vendor-id+9 (Cisco) Vendor type 38 for downstream traffic to output policy name

How to Configure Per-User QoS via AAA Policy Name

This section contains the following procedure:

- [Monitoring and Maintaining Per-User QoS via AAA Policy Name, page 2](#)

To configure per-user QoS, use the authentication, authorization, and accounting (AAA) policy name that you have received from the RADIUS server. To configure QoS policy, refer to the documents listed in the section [Related Documents](#).

Monitoring and Maintaining Per-User QoS via AAA Policy Name

To monitor and maintain per-user QoS using the AAA policy name, use the following **debug** commands:

SUMMARY STEPS

1. **enable**
2. **debug aaa authorization**
3. **debug aaa per-user**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	debug aaa authorization Example: Router# debug aaa authorization	Displays information about AAA/TACACS+ authorization.
Step 3	debug aaa per-user Example: Router# debug aaa per-user	Displays information about per-user QoS parameters.

Configuration Examples for Per-User QoS via AAA Policy Name

This section provides the following configuration example:

- [Per-User QoS Using the AAA Policy Name, page 3](#)

Per-User QoS Using the AAA Policy Name

The following example shows that per-user QoS is being configured using the AAA policy name “policy_class_1_2”:

```
class-map match-all class1
  match access-group 101
class-map match-all class2
  match qos-group 4
  match access-group 101

policy-map policy_class_1_2
  class class1
    bandwidth 3000
    queue-limit 30
  class class2
    bandwidth 2000
  class class-default
    bandwidth 500

peruser_qos_1    Password = "lab"
  Service-Type = Framed,
  Framed-Protocol = PPP,
  Cisco:Cisco-avpair = "ip:sub-policy-In=ssspolicy"
!ssspolicy in the above line is the name of the policy.

peruser_qos_2    Password = "lab"
  Service-Type = Framed,
```



```
Framed-Protocol = PPP,  
Cisco:Cisco-avpair = "ip:sub-policy-Out=ssspolicy"
```

Additional References

For additional information related to the Per-User QoS via AAA Policy Name feature, refer to the following references:

Related Documents

Related Topic	Document Title
<ul style="list-style-type: none">AAA per-user and QoS configurations and information about the policy-map command	<ul style="list-style-type: none">Configuring Per-User ConfigurationCisco IOS Security Command Reference, Release 12.2 T

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

This feature uses no new or modified commands. To see the command pages for the commands used with this feature, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or a Cisco IOS master commands list.

Feature Information for Per-User QoS via AAA Policy Name

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Per-User QoS via AAA Policy Name

Feature Name	Releases	Feature Information
Per-User QoS via AAA Policy Name	12.2(15)B 12.2(15)T 12.2(33)SRC	You can use the Per-User QoS via AAA Policy Name feature to download a policy name that describes QoS parameters for a user session from a RADIUS server and apply them for a particular session.

Glossary

RADIUS—Remote Authentication Dial-In User Service. RADIUS is a database for authenticating modem and ISDN connections and for tracking connection time.

VSA—vendor-specific attribute. A VSA is an attribute that has been implemented by a particular vendor. It uses the attribute Vendor-Specific to encapsulate the resulting AV pair: essentially, Vendor-Specific = protocol:attribute = value.

**Note**

Refer to the [Internetworking Terms and Acronyms](#) for terms not included in this glossary.



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2000–2007 Cisco Systems, Inc. All rights reserved



RADIUS Attribute 5 (NAS-Port) Format Specified on a Per-Server Group Level

The RADIUS Attribute 5 (NAS-Port) Format Specified on a Per-Server Group Level feature allows you to customize configurations for different RADIUS server groups. This flexibility allows customized network access server- (NAS-) port formats to be used instead of global formats.

Feature History for RADIUS Attribute 5 (NAS-Port) Format Specified on a Per-Server Group Level

Release	Modification
12.3(14)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for RADIUS Attribute 5 \(NAS-Port\) Format Specified on a Per-Server Group Level, page 2](#)
- [Information About RADIUS Attribute 5 \(NAS-Port\) Format Specified on a Per-Server Group Level, page 2](#)
- [How to Configure RADIUS Attribute 5 \(NAS-Port\) Format Specified on a Per-Server Group Level, page 2](#)
- [Configuration Examples for RADIUS Attribute 5 \(NAS-Port\) Format Specified on a Per-Server Group Level, page 5](#)
- [Additional References, page 5](#)
- [Command Reference, page 6](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for RADIUS Attribute 5 (NAS-Port) Format Specified on a Per-Server Group Level

- You must be running a Cisco IOS image that contains the authentication, authorization, and accounting (AAA) component.

Information About RADIUS Attribute 5 (NAS-Port) Format Specified on a Per-Server Group Level

To configure the RADIUS Attribute 5 (NAS-Port) Format Specified on a Per-Server Group Level feature, you should understand the following concept:

- [RADIUS Attribute 5 Format Customization, page 2](#)

RADIUS Attribute 5 Format Customization

Prior to Cisco IOS Release 12.3(14)T, Cisco IOS software allowed RADIUS attributes that were sent in access requests or accounting requests to be customized on a global basis. You could customize how each configurable attribute should function when communicating with a RADIUS server. Since the implementation of server groups, global attribute configurations were not flexible enough to address the different customizations that were required to support the various RADIUS servers with which a router might be interacting. For example, if you configured the **global radius-server attribute nas-port format command** option, every service on the router that interacted with a RADIUS server was used in the same way.

Effective with Cisco IOS Release 12.3(14)T, you can configure your router to support override flexibility for per-server groups. You can configure services to use specific named methods for different service types on a RADIUS server. The service types can be set to use their own respective service groups. This flexibility allows customized NAS-port formats to be used instead of the global formats.

How to Configure RADIUS Attribute 5 (NAS-Port) Format Specified on a Per-Server Group Level

This section contains the following procedures:

- [Configuring the RADIUS Attribute 5 Format on a Per-Server Group Level, page 2](#)
- [Monitoring and Maintaining RADIUS Attribute 5 Format on a Per-Server Group Level, page 4](#)

Configuring the RADIUS Attribute 5 Format on a Per-Server Group Level

To configure your router to support the RADIUS Attribute 5 format on a per-server group level, perform the following steps.

**Note**

To use this per-server group capability, you must actively use a named method list within your services. You can configure one client to use a specific named method while other clients use the default format.

Prerequisites

Before performing these steps, you should first configure method lists for AAA as is applicable for your situation.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *group-name*
4. **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
5. **attribute nas-port format** *format-type* [*string*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa group server radius group-name Example: Router (config)# aaa group server radius radius1	Groups different RADIUS server hosts into distinct lists and distinct methods and enters server-group configuration mode.
Step 4	server ip-address [auth-port port-number] [acct-port port-number] Example: Router (server-group)# server 172.101.159.172 auth-port 1645 acct-port 1646	Configures the IP address of the RADIUS server for the group server.
Step 5	attribute nas-port format format-type [string] Example: Router (server-group)# attribute nas-port format d	Configures a service to use specific named methods for different service types. <ul style="list-style-type: none"> The service types can be set to use their own respective server groups.

Monitoring and Maintaining RADIUS Attribute 5 Format on a Per-Server Group Level

To monitor and maintain RADIUS Attribute 5 Format on a Per-Server Group Level, perform the following steps (the **debug** commands may be used separately):

SUMMARY STEPS

1. **enable**
2. **debug aaa sg-server selection**
3. **debug radius**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	debug aaa sg-server selection Example: Router# debug aaa sg-server selection	Displays information about why the RADIUS and TACACS+ server group system in a router is choosing a particular server.
Step 3	debug radius Example: Router# debug radius	Displays information showing that a server group has been selected for a particular request.

Configuration Examples for RADIUS Attribute 5 (NAS-Port) Format Specified on a Per-Server Group Level

- This section provides the following configuration example:
- [RADIUS Attribute 5 Format Specified on a Per-Server Level: Example, page 5](#)

RADIUS Attribute 5 Format Specified on a Per-Server Level: Example

The following configuration example shows a leased-line PPP client that has chosen to send no RADIUS Attribute 5 while the default is to use format d:

```
interface Serial2/0
no ip address
encapsulation ppp
ppp accounting SerialAccounting
ppp authentication pap

aaa accounting network default start-stop group radius
aaa accounting network SerialAccounting start-stop group group1

aaa group server radius group1
server 10.101.159.172 auth-port 1645 acct-port 1646
attribute nas-port none

radius-server host 10.101.159.172 auth-port 1645 acct-port 1646
radius-server attribute nas-port format d
```

Additional References

The following sections provide references related to RADIUS Attribute 5 (NAS-Port) Format Specified on a Per-Server Group Level.

Related Documents

Related Topic	Document Title
Cisco IOS commands	<i>Cisco IOS Security Command Reference</i> , Release 12.3T
Configuring AAA and AAA method lists	“ Authentication, Authorization, and Accounting (AAA) ” section of <i>Cisco IOS Security Configuration Guide, Release 12.3</i> .

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following new command is pertinent to this feature.

- **attribute nas-port format**

For information about these commands, see the Cisco IOS Security Command Reference at

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at

<http://tools.cisco.com/Support/CLILookup> or the Master Command List.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

© 2007 Cisco Systems, Inc. All rights reserved.



RADIUS Attribute 8 (Framed-IP-Address) in Access Requests

First Published: August 12, 2002

Last Updated: January 10, 2008

The RADIUS Attribute 8 (Framed-IP-Address) in Access Requests feature makes it possible for a network access server (NAS) to provide the RADIUS server with a hint of the user IP address in advance of user authentication. An application can be run on the RADIUS server to use this hint and build a table (map) of user names and addresses. Using the mapping information, service applications can begin preparing user login information to have available upon successful user authentication.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for RADIUS Attribute 8 \(Framed-IP-Address\) in Access Requests”](#) section on page 7.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for RADIUS Attribute 8 \(Framed-IP-Address\) in Access Requests, page 2](#)
- [Information About RADIUS Attribute 8 \(Framed-IP-Address\) in Access Requests, page 2](#)
- [How to Configure RADIUS Attribute 8 \(Framed-IP-Address\) in Access Requests, page 3](#)
- [Configuration Examples for RADIUS Attribute 8 \(Framed-IP-Address\) in Access Requests, page 4](#)
- [Additional References, page 5](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2002–2008 Cisco Systems, Inc. All rights reserved.

- [Command Reference, page 6](#)
- [Feature Information for RADIUS Attribute 8 \(Framed-IP-Address\) in Access Requests, page 7](#)

Prerequisites for RADIUS Attribute 8 (Framed-IP-Address) in Access Requests

Sending RADIUS attribute 8 in the RADIUS access requests assumes that the login host has been configured to request its IP address from the NAS server. It also assumes that the login host has been configured to accept an IP address from the NAS.

The NAS must be configured with a pool of network addresses on the interface supporting the login hosts.

Information About RADIUS Attribute 8 (Framed-IP-Address) in Access Requests

How This Feature Works

When a network device dials in to a NAS that is configured for RADIUS authentication, the NAS begins the process of contacting the RADIUS server in preparation for user authentication. Typically, the IP address of the dial-in host is not communicated to the RADIUS server until after successful user authentication. Communicating the device IP address to the server in the RADIUS access request allows other applications to begin to take advantage of that information.

As the NAS is setting up communication with the RADIUS server, the NAS assigns an IP address to the dial-in host from a pool of IP addresses configured at the specific interface. The NAS sends the IP address of the dial-in host to the RADIUS server as attribute 8. At that time, the NAS sends other user information, such as the user name, to the RADIUS server.

After the RADIUS server receives the user information from the NAS, it has two options:

- If the user profile on the RADIUS server already includes attribute 8, the RADIUS server can override the IP address sent by the NAS with the IP address defined as attribute 8 in the user profile. The address defined in the user profile is returned to the NAS.
- If the user profile does not include attribute 8, the RADIUS server can accept attribute 8 from the NAS, and the same address is returned to the NAS.

The address returned by the RADIUS server is saved in memory on the NAS for the life of the session. If the NAS is configured for RADIUS accounting, the accounting start packet sent to the RADIUS server includes the same IP address as in attribute 8. All subsequent accounting packets, updates (if configured), and stop packets will also include the same IP address provided in attribute 8.

Benefits

The RADIUS Attribute 8 (Framed-IP-Address) in Access Requests feature makes it possible to run applications on the RADIUS server that builds mapping tables of users and IP addresses. The server can then use the mapping table information in other applications, such as preparing customized user login pages in advance of a successful user authentication with the RADIUS server.

How to Configure RADIUS Attribute 8 (Framed-IP-Address) in Access Requests

This section contains the following procedures:

- [Configuring RADIUS Attribute 8 in Access Requests, page 3](#) (required)
- [Verifying RADIUS Attribute 8 in Access Requests, page 4](#)

Configuring RADIUS Attribute 8 in Access Requests

To send RADIUS attribute 8 in the access request, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute 8 include-in-access-req**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	radius-server attribute 8 include-in-access-req Example: Router(config)# radius-server attribute 8 include-in-access-req	Sends RADIUS attribute 8 in access-request packets.

Verifying RADIUS Attribute 8 in Access Requests

To verify that RADIUS attribute 8 is being sent in access requests, perform the following steps. Attribute 8 should be present in all PPP access requests.

SUMMARY STEPS

- 1. `enable`
- 2. `more system:running-config`
- 3. `debug radius`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	<code>more system:running-config</code> Example: Router# more system:running-config	Displays the contents of the current running configuration file. (Note that the <code>more system:running-config</code> command has replaced the <code>show running-config</code> command.)
Step 3	<code>debug radius</code> Example: Router# debug radius	Displays information associated with RADIUS. The output of this command shows whether attribute 8 is being sent in access requests.

Configuration Examples for RADIUS Attribute 8 (Framed-IP-Address) in Access Requests

This section provides the following configuration example:

- [NAS Configuration That Sends the IP Address of the Dial-in Host to the RADIUS Server in the RADIUS Access Request](#)

NAS Configuration That Sends the IP Address of the Dial-in Host to the RADIUS Server in the RADIUS Access Request

The following example shows a NAS configuration that sends the IP address of the dial-in host to the RADIUS server in the RADIUS access request. The NAS is configured for RADIUS authentication, authorization, and accounting (AAA). A pool of IP addresses (async1-pool) has been configured and applied at interface Async1.

```
aaa new-model
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authorization network default group radius
```

```

aaa accounting network default start-stop group radius
!
ip address-pool local
!
interface Async1
 peer default ip address pool async1-pool
!
ip local pool async1-pool 209.165.200.225 209.165.200.229
!
radius-server host 172.31.71.146 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute 8 include-in-access-req
radius-server key radhost<xxx>: Example

```

Additional References

The following sections provide references related to the RADIUS Attribute 8 (Framed-IP-Address) in Access Requests feature.

Related Documents

Related Topic	Document Title
Configuring authentication and configuring RADIUS	“ Configuring Authentication ” and “ Configuring RADIUS ” chapters, <i>Cisco Security Configuration Guide</i>
RFC 2138 (RADIUS)	RFC 2138 , <i>Remote Authentication Dial In User Service (RADIUS)</i>

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Cisco IOS Master Commands list.

- **radius-server attribute 8 include-in-access-req**

Feature Information for RADIUS Attribute 8 (Framed-IP-Address) in Access Requests

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for RADIUS Attribute 8 (Framed-IP-Address) in Access Requests


Feature Name	Releases	Feature Information
RADIUS Attribute 8 (Framed-IP-Address) in Access Requests	12.2(11)T 12.2(28)SB 12.2(33)SRC	<p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Information About RADIUS Attribute 8 (Framed-IP-Address) in Access Requests, page 2 • How to Configure RADIUS Attribute 8 (Framed-IP-Address) in Access Requests, page 3 • Configuration Examples for RADIUS Attribute 8 (Framed-IP-Address) in Access Requests, page 4 <p>The following commands were introduced or modified: radius-server attribute 8 include-in-access-req.</p>
Sticky IP	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2002–2008 Cisco Systems, Inc. All rights reserved.



RADIUS Attribute 82: Tunnel Assignment ID

Feature History

Release	Modification
12.2(4)T	This feature was introduced.
12.2(4)T3	Support for the Cisco 7500 series routers was added.
12.2(11)T	This feature was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco 1760, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800 and Cisco AS5850 platforms.
12.2(27)SB	This feature was integrated into Cisco IOS Release 12.2(27)SB.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Feature Overview, page 2](#)
- [Supported Platforms, page 2](#)
- [Supported Standards, MIBs, and RFCs, page 3](#)
- [Prerequisites, page 3](#)
- [Configuration Tasks, page 3](#)
- [Configuration Examples, page 5](#)
- [Command Reference, page 6](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Feature Overview

The RADIUS Attribute 82: Tunnel Assignment ID feature allows the Layer 2 Transport Protocol access concentrator (LAC) to group users from different per-user or domain RADIUS profiles into the same active tunnel. Previously, Cisco IOS software assigned a separate virtual private dialup network (VPDN) tunnel for each per-user or domain RADIUS profile, even if tunnels with identical endpoints already existed. The RADIUS Attribute 82: Tunnel Assignment ID feature defines a new avpair, Tunnel-Assignment-ID, which allows the LAC to group users from different RADIUS profiles into the same tunnel if the chosen endpoint, tunnel type, and Tunnel-Assignment-ID are identical. This feature introduces new software functionality. No new commands are introduced with this feature.

Benefits

The RADIUS Attribute 82: Tunnel Assignment ID feature improves LAC and L2TP network server (LNS) performance by reducing memory usage, because fewer tunnel data structures must be maintained. This feature allows the LAC and LNS to handle a higher volume of users without negatively impacting router performance.

Restrictions

This feature is designed only for VPDN dial-in applications. It does not support VPDN dial-out.

Related Documents

- *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2
- *Cisco IOS Dial Technologies Command Reference*, Release 12.2
- *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.2
- *Cisco IOS Wide-Area Networking Command Reference*, Release 12.2

Supported Platforms

- Catalyst 4000 Gateway
- Cisco 806
- Cisco 1400 series
- Cisco 1600 series
- Cisco 1700 series
- Cisco 2600 series
- Cisco 3600 series
- Cisco 3700 series
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7500 series

- Cisco AS5300
- Cisco AS5400
- Cisco AS5800
- Cisco IGX 8400 URM
- Cisco MGX 8850
- Cisco ubr7200

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

You must be using a Cisco platform that supports VPDN to use this feature.

Configuration Tasks

None

Verifying RADIUS Attribute 82

To verify that RADIUS attribute 82 is being used by the LAC during tunnel authorization, use the following privileged EXEC command:

Command	Purpose
Router# debug radius	Displays information associated with RADIUS. The output of this command shows whether attribute 82 is being sent in access requests.

Configuration Examples

This section provides the following configuration examples:

- [LAC Configuration Example](#)
- [LNS Configuration Example](#)
- [RADIUS Configuration Example](#)

LAC Configuration Example

The following example configures VPDN on the LAC:

```
hostname lac
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius

vpdn enable
vpdn authen-before-forward

interface Serial2/0:23
no ip address
encapsulation ppp
dialer-group 1
isdn switch-type primary-5ess
no fair-queue

dialer-list 1 protocol ip permit

radius-server host lac-radiusd auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key rad123
```

LNS Configuration Example

The following example configures VPDN on the LNS:

```
hostname lns
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius

vpdn enable

vpdn-group 1
accept-dialin
protocol any
virtual-template 1

interface Loopback0
ip address 10.1.1.3 255.255.255.0

interface Virtual-Template1
ip unnumbered Loopback0
no keepalive
peer default ip address pool mypool
ppp authentication chap
```

```
ip local pool mypool 10.1.1.10 10.1.1.50

radius-server host lns-radiusd auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
```

RADIUS Configuration Example

The following examples configure the RADIUS server to group sessions in a tunnel:

Per-User Configuration

```
user@router.com Password = "cisco" Service-Type = Outbound,
    Tunnel-Type = :1:L2TP,
    Tunnel-Server-Endpoint = :1:"10.14.10.54",
    Tunnel-Assignment-Id = :1:"router"

client@router.com Password = "cisco" Service-Type = Outbound,
    Tunnel-Type = :1:L2TP,
    Tunnel-Server-Endpoint = :1:"10.14.10.54",
    Tunnel-Assignment-Id = :1:"router"
```

Domain Configuration

```
eng.router.com Password = "cisco" Service-Type = Outbound,
    Tunnel-Type = :1:L2TP,
    Tunnel-Server-Endpoint = :1:"10.14.10.54",
    Tunnel-Assignment-Id = :1:"router"

sales.router.com Password = "cisco" Service-Type = Outbound,
    Tunnel-Type = :1:L2TP,
    Tunnel-Server-Endpoint = :1:"10.14.10.54",
    Tunnel-Assignment-Id = :1:"router"
```

Command Reference

This feature uses no new or modified commands. To see the command pages for the commands used with this feature, see the Cisco IOS Security Command Reference at

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at

<http://tools.cisco.com/Support/CLILookup> or the Master Command List. .



© 2007 Cisco Systems, Inc. All rights reserved.



RADIUS Attribute 104

First Published: March 1, 2004

Last Updated: February 28, 2006

The RADIUS Attribute 104 feature allows you to specify private routes (attribute 104) in your RADIUS authorization profile. The private routes affect only packets that are received on an individual interface. The routes are stored apart from the global routing table and are not injected into any routing protocols for redistribution.

History for the RADIUS Attribute 104 Feature

Release	Modification
12.3(7)T	This feature was introduced.
12.3(14)T	This feature was integrated into Cisco IOS release 12.3(14)T.
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for RADIUS Attribute 104, page 2](#)
- [Restrictions for RADIUS Attribute 104, page 2](#)
- [Information About RADIUS Attribute 104, page 2](#)
- [How to Apply RADIUS Attribute 104, page 3](#)
- [Configuration Examples for RADIUS Attribute 104, page 6](#)
- [Additional References, page 7](#)
- [Command Reference, page 9](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for RADIUS Attribute 104

- You must be using a Cisco RADIUS server.
- You should be familiar with configuring RADIUS.
- You should be familiar with policy-based routing (PBR) and private routes.
- You should be familiar with configuring access control lists (ACLs).
- Before using the RADIUS Attribute 104 feature, you must configure RADIUS AAA authorization and RADIUS route download.
- The following memory bytes are required:
 - One route map—50 bytes.
 - One match-set clause—600 bytes.
 - One extended ACL—366 bytes.
 - For N number of attribute 104s, the memory requirement is $(600+366)*N+50=1000*N$ (approximate) per user.

Restrictions for RADIUS Attribute 104

- If you already have PBR locally (statically) configured under the interface, and you specify attribute 104, the locally configured PBR will be disabled.
- If a pseudo next-hop address is involved, there must be a route available in the routing table for the next-hop address. If a route is not available, the packet will not be policy routed.
- Policy routing does not order the match-set clauses and relies on the first match, so you should specify the attributes in the order in which you want them to be matched.
- Metric numbers cannot be used in the attribute.

Information About RADIUS Attribute 104

Before using the RADIUS Attribute 104 feature, you should understand the following concepts:

- [Policy-Based Routing: Background, page 2](#)
- [Attribute 104 and the Policy-Based Route Map, page 3](#)

Policy-Based Routing: Background

PBR provides a mechanism for the forwarding, or routing of, data packets on the basis of defined policies. The policies are not wholly dependent on the destination address but rather on other factors, such as type of service, source address, precedence, port numbers, or protocol type.

Policy-based routing is applied to incoming packets. All packets that are received on an interface that has policy-based routing enabled are considered for policy-based routing. The router passes the packets through enhanced packet filters called route maps. On the basis of the criteria that are defined in the route maps, the packets are forwarded to the appropriate next hop.

Each entry in a route map statement contains a combination of match clauses and set clauses or commands. The match clauses define the criteria for whether appropriate packets meet the particular policy (that is, whether the conditions are met). The set clauses provide instruction for how the packets should be routed after they have met the match criteria. The match clause specifies which set of filters a packet must match for the corresponding set clause to be applied.

Attribute 104 and the Policy-Based Route Map

This section discusses the attribute 104 feature and how it works with policy-based route maps.

RADIUS Attribute 104 Overview

Using the RADIUS Attribute 104 feature, you can specify private routes in your RADIUS authorization profile. The private routes you specify will affect only packets that are received on an individual interface. The routes are stored apart from the global routing table and are not injected into any routing protocols for redistribution.

Permit Route Map

Route map statements can be marked as “permit” or “deny.” If the statement is marked “permit,” the set clause is applied to the packets that match the match criteria. For attribute 104, when you are configuring the route map, you need to mark the route map as “permit,” as follows. (To configure a route map, see the chapter “[Configuring Policy-Based Routing](#)” in the *Cisco IOS Quality of Service Solutions Configuration Guide*.)

```
route-map map-tag permit sequence-number
```

Default Private Route

The policy routing process proceeds through the route map until a match is found. If no match is found in the route map, the global routing table is consulted. If you have specified a default route in your user profile, any further routes beyond the default route are effectively ignored.

Route Map Order

You need to specify route maps on the server in the order that you want them to be applied.

How to Apply RADIUS Attribute 104

This section contains the following procedures:

- [Applying RADIUS Attribute 104 to Your User Profile, page 4](#)
- [Verifying Route Maps, page 4](#)
- [Troubleshooting the RADIUS Profile, page 5](#)

Applying RADIUS Attribute 104 to Your User Profile

You can apply RADIUS attribute 104 to your user profile by adding the following to the RADIUS server database.

SUMMARY STEPS

1. Apply RADIUS attribute 104 to your user profile.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Apply RADIUS attribute 104 to your user profile.	<p>Ascend-Private-Route="dest_addr/netmask next_hop"</p> <p>The destination network address of the router is "dest_addr/netmask", and the address of the next-hop router is "next_hop."</p>

Examples

The following is a sample user profile that creates three private routes that are associated with the caller:

```
username Password="ascend"; User-Service=Framed-User
```

```
Framed-Protocol=PPP,
Framed-Address=10.1.1.1,
Framed-Netmask=255.0.0.0,
Ascend-Private-Route="172.16.1.1/16 10.10.10.1"
Ascend-Private-Route="192.168.1.1/32 10.10.10.2"
Ascend-Private-Route="10.20.0.0/1 10.10.10.3"
Ascend-Private-Route="10.0.0.0/0 10.10.10.4"
```

Using the above profile, the private routing table for the connection contains the following routes, including a default route:

Destination/Mask	Gateway
172.16.1.1/16	10.10.10.1
192.168.1.1/32	10.10.10.2
10.20.20.20/1	10.10.10.3
10.0.0.0/0	10.10.10.4

Verifying Route Maps

You can use the following **show** commands to verify the route maps that have been configured.

SUMMARY STEPS

1. **enable**
2. **show ip policy**
3. **show route-map** [*map-name* | **dynamic** [*dynamic-map-name* | **application** [*application-name*]] | **all**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show ip policy Example: Router# show ip policy	Displays the route map that is used for policy routing.
Step 3	show route-map [<i>map-name</i> dynamic [<i>dynamic-map-name</i> application [<i>application-name</i>]] all] Example: Router# show route-map	Displays all route maps that are configured or only the one that is specified.

Troubleshooting the RADIUS Profile

If your private route configuration is not working properly, you may want to reread the section “[Policy-Based Routing: Background](#).” This section may help you determine what is happening to the packets. In addition, the following **debug** commands can be used to troubleshoot your RADIUS profile.

SUMMARY STEPS

1. **enable**
2. **debug radius**
3. **debug aaa per-user**
4. **debug ip policy**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	debug radius Example: Router# debug radius	Displays information associated with RADIUS.
Step 3	debug aaa per-user Example: Router# debug aaa per-user	Displays the attributes that are applied to each user as the user authenticates.
Step 4	debug ip policy Example: Router# debug ip policy	Displays IP routing packet activity.

Configuration Examples for RADIUS Attribute 104

This section includes the following configuration example:

- [Route-Map Configuration in Which Attribute 104 Has Been Applied: Example, page 6](#)

Route-Map Configuration in Which Attribute 104 Has Been Applied: Example

The following output is a typical route-map configuration to which attribute 104 has been applied:

```
Router# show route-map dynamic
```

```
route-map AAA-01/08/04-14:13:59.542-1-AppSpec, permit, sequence 0, identifier 1639994476
  Match clauses:
    ip address (access-lists): PBR#1 PBR#2
  Set clauses:
    Policy routing matches: 0 packets, 0 bytes
route-map AAA-01/08/04-14:13:59.542-1-AppSpec, permit, sequence 1, identifier 1640264784
  Match clauses:
    ip address (access-lists): PBR#3 PBR#4
  Set clauses:
    Policy routing matches: 0 packets, 0 bytes
route-map AAA-01/08/04-14:13:59.542-1-AppSpec, permit, sequence 2, identifier 1645563704
  Match clauses:
    ip address (access-lists): PBR#5 PBR#6
    length 10 100
  Set clauses:
    ip next-hop 10.1.1.1
    ip gateway 10.1.1.1
  Policy routing matches: 0 packets, 0 bytes
Current active dynamic routemaps = 1
```

Additional References

The following sections provide references related to RADIUS Attribute 104.

Related Documents

Related Topic	Document Title
Configuring RADIUS	“Configuring RADIUS” chapter in the “Security Server Protocols” section of the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4
Configuring policy-based routing	“Configuring Policy-Based Routing” chapter in the “Classification” section of the <i>Cisco IOS Quality of Service Configuration Guide</i> , Release 12.4
Configuring access control lists	<ul style="list-style-type: none"> The “Access Control Lists: Overview and Guidelines” chapter of the “Traffic Filtering and Firewalls” section of the <i>Cisco IOS Security Configuration Guide</i>, 12.4 <i>IP Access List Entry Sequence Numbering</i>, Release 12.3(2)T
Configuring RADIUS AAA authorization and RADIUS route download	“RADIUS Route Download” chapter in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.2(8)T
Security commands	<i>Cisco IOS Security Command Reference</i> , Release 12.4
Quality of Service (QoS) commands (for policy-based routing commands)	<i>Cisco IOS Quality of Service Solutions Command Reference</i> , Release 12.3 T

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features

- **show ip policy**
- **show route-map**

For information about these commands, see the Cisco IOS Security Command Reference at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



RADIUS Progress Codes

First Published: August 12, 2002

Last Updated: December 17, 2007

The RADIUS Progress Codes feature adds additional progress codes that are defined in [Table 1](#) to RADIUS attribute 196 (Ascend-Connect-Progress), which indicates a connection state before a call is disconnected through progress codes.

Attribute 196 is sent in network, exec, and resource accounting “start” and “stop” records. This attribute can facilitate call failure debugging because each progress code identifies accounting information relevant to the connection state of a call. The attribute is activated by default; when an accounting “start” or “stop” accounting record is requested, authentication, authorization, and accounting (AAA) adds attribute 196 into the record as part of the standard attribute list. Attribute 196 is valuable because the progress codes, which are sent in accounting “start” and “stop” records, facilitate the debugging of call failures.



Note

In accounting “start” records, attribute 196 does not have a value.

Table 1 *Newly Supported Progress Codes for Attribute 196*

Code	Description
10	Modem allocation and negotiation is complete; the call is up.
30	The modem is up.
33	The modem is waiting for result codes.
41	The max TNT is establishing the TCP connection by setting up a TCP clear call.
60	Link control protocol (LCP) is the open state with PPP and IP Control Protocol (IPCP) negotiation; the LAN session is up.
65	PPP negotiation occurs and, initially, the LCP negotiation occurs; LCP is in the open state.
67	After PPP negotiation with LCP in the open state occurs, IPCP negotiation begins.



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2002, 2006, 2007 Cisco Systems, Inc. All rights reserved.

**Note**

Progress codes 33, 30, and 67 are generated and seen through debugs on the NAS; all other codes are generated and seen through debugs and the accounting record on the RADIUS server.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for RADIUS Progress Codes](#)” section on page 6.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for RADIUS Progress Codes, page 2](#)
- [How to Configure RADIUS Progress Codes, page 2](#)
- [How to Verify Attribute 196, page 3](#)
- [Debug Output Example for RADIUS Progress Codes, page 3](#)
- [Additional References, page 4](#)
- [Command Reference, page 5](#)
- [Feature Information for RADIUS Progress Codes, page 6](#)
- [Glossary, page 7](#)

Prerequisites for RADIUS Progress Codes

Before attribute 196 (Ascend-Connect-Progress) can be sent in accounting “start” and “stop” records, you must perform the following tasks:

- Enable AAA.
- Enable exec, network, or resource accounting.

For information on completing these tasks, refer to the AAA sections of the *Cisco IOS Security Configuration Guide*, Release 12.4.

When these tasks are completed, attribute 196 is active by default.

How to Configure RADIUS Progress Codes

No configuration is required to configure RADIUS Progress Codes.

How to Verify Attribute 196

To verify attribute 196 in accounting “start” and “stop” records, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **debug aaa accounting**
3. **show radius statistics**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	debug aaa accounting Example: Router# debug aaa accounting	Displays information on accountable events as they occur.
Step 3	show radius statistics Example: Router# debug aaa authorization	Displays the RADIUS statistics for accounting and authentication packets.

Debug Output Example for RADIUS Progress Codes

The following example is a sample debug output from the **debug ppp negotiation** command. This debug output is used to verify that accounting “stop” records have been generated and that attribute 196 (Ascend-Connect-Progress) has a value of 65.

```
Tue Aug 7 06:21:03 2001
  NAS-IP-Address = 10.0.58.62
  NAS-Port = 20018
  Vendor-Specific = ""
  NAS-Port-Type = ISDN
  User-Name = "peer_16a"
  Called-Station-Id = "5213124"
  Calling-Station-Id = "5212175"
  Acct-Status-Type = Stop
  Acct-Authentic = RADIUS
  Service-Type = Framed-User
  Acct-Session-Id = "00000014"
  Framed-Protocol = PPP
  Framed-IP-Address = 172.16.0.2
  Acct-Input-Octets = 3180
  Acct-Output-Octets = 3186
  Acct-Input-Packets = 40
  Acct-Output-Packets = 40
```

```

Ascend-Connect-Pr = 65
Acct-Session-Time = 49
Acct-Delay-Time = 0
Timestamp = 997190463
Request-Authenticator = Unverified

```

Additional References

The following sections provide references related to RADIUS Progress Codes.

Related Documents

Related Topic	Document Title
Cisco IOS Security commands	Cisco IOS Security Command Reference
Configuring Accounting	“ Configuring Accounting ” chapter in the <i>Cisco IOS Security Configuration Guide</i>
Radius Attributes	“ RADIUS Attributes ” chapter in the <i>Cisco IOS Security Configuration Guide</i>

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Command Reference

No commands are introduced or modified in the feature documented in this module. For information about commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

Feature Information for RADIUS Progress Codes

Table 2 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 2 Feature Information for RADIUS Progress Codes

Feature Name	Releases	Feature Information
RADIUS Progress Codes	12.2(11)T 12.2(28)SB 12.2(33)SRC Cisco IOS XE Release 2.1	<p>The RADIUS Progress Codes feature adds additional progress codes that are defined in Table 1 to RADIUS attribute 196 (Ascend-Connect-Progress), which indicates a connection state before a call is disconnected through progress codes.</p> <p>This feature was introduced in Cisco IOS Release 12.2(11)T.</p> <p>This feature was integrated into Cisco IOS Release 12.2(28)SB.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRC.</p> <p>In Cisco IOS Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers</p>

Glossary

AAA—authentication, authorization, and accounting. Suite of network security services that provide the primary framework through which access control can be set up on your Cisco router or access server.

attribute—RADIUS Internet Engineering Task Force (IETF) attributes are the original set of 255 standard attributes that are used to communicate AAA information between a client and a server. Because IETF attributes are standard, the attribute data is predefined and well known; thus all clients and servers who exchange AAA information through IETF attributes must agree on attribute data such as the exact meaning of the attributes and the general bounds of the values for each attribute.

EXEC accounting—Provides information about user EXEC terminal sessions of the network access server.

IPCP—IP Control Protocol. A protocol that establishes and configures IP over PPP.

LCP—link control protocol. A protocol that establishes, configures, and tests data-link connections for use by PPP.

network accounting—Provides information for all PPP, Serial Line Internet Protocol (SLIP), or AppleTalk Remote Access Protocol (ARAP) sessions, including packet and byte counts.

PPP—Point-to-Point Protocol. Successor to SLIP that provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. Whereas SLIP was designed to work with IP, PPP was designed to work with several network layer protocols, such as IP, IPX, and ARA. PPP also has built-in security mechanisms, such as CHAP and PAP. PPP relies on two protocols: LCP and NCP.

RADIUS—Remote Authentication Dial-In User Service. RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

resource accounting—Provides “start” and “stop” records for calls that have passed user authentication, and provides “stop” records for calls that fail to authenticate.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



RADIUS Timeout Set During Pre-Authentication

First Published: March 17, 2003
Last Updated: December 17, 2007

Some call sessions for Internet Service Provider (ISP) subscribers are billed through authentication, authorization, and accounting (AAA) messages in a prepaid time model. When these subscribers are preauthenticated, a RADIUS server checks for any remaining credit in the prepaid time model and sets a session timeout based on the credit available. The RADIUS Timeout Set During Pre-Authentication feature is useful in situations where the PPP authentication that follows the preauthentication phase of these call sessions does not return the Session-Timeout value (RADIUS attribute 27), and therefore allows the ISP to add call setup time to the subscriber's bill.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for RADIUS Timeout Set During Pre-Authentication” section on page 5](#).

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for the RADIUS Timeout Set During Pre-Authentication Feature, page 2](#)
- [Information About the RADIUS Timeout Set During Pre-Authentication Feature, page 2](#)
- [How to Configure the RADIUS Timeout Set During Pre-Authentication Feature, page 2](#)
- [Additional References, page 3](#)
- [Command Reference, page 4](#)
- [Feature Information for RADIUS Timeout Set During Pre-Authentication, page 5](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2003–2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for the RADIUS Timeout Set During Pre-Authentication Feature

- This feature is specific to RADIUS. Basic AAA authentication and preauthentication must be configured.
- Preauthentication and normal PPP authentication are required for legacy functionality.

Information About the RADIUS Timeout Set During Pre-Authentication Feature

You need to understand the following concept about the RADIUS Timeout Set During Pre-Authentication feature:

- [RADIUS Attribute 27 and the PPP Authentication Phase, page 2](#)

RADIUS Attribute 27 and the PPP Authentication Phase

The RADIUS Timeout Set During Pre-Authentication feature was developed for ISPs that want to bill dial-in subscribers for call setup time and the entire duration of the call session. These subscribers are billed through AAA messages in a prepaid time model. When the subscribers are preauthenticated, a RADIUS server checks for any remaining credit in the prepaid time model and sets a session timeout (in minutes or seconds) based on the credit available. This time can range from a few seconds for ISDN users, to much longer for asynchronous dial-up subscribers.

Until the RADIUS Timeout Set During Pre-Authentication feature was developed, the value of RADIUS attribute 27, which is returned during the preauthentication phase of a call, was either ignored or overwritten during the PPP authentication phase. Even when the PPP authentication phase did not return a value for attribute 27, the old value obtained during the preauthentication phase was being ignored.

With the RADIUS Timeout Set During Pre-Authentication feature introduced for Cisco IOS Release 12.2(15)T, if the PPP authentication phase does not return a value for attribute 27, the old value that was returned during the preauthentication phase is saved and used to time out the session; attribute 27 is saved in a preauthentication database for future use. However, if the PPP authentication user profile has a session timeout configured and PPP authentication succeeds, the new value downloaded during PPP authentication overwrites the old attribute 27 value. By setting the session timeout value in the preauthentication phase itself, the service provider can bill the subscriber for the call setup time and the call duration.

How to Configure the RADIUS Timeout Set During Pre-Authentication Feature

No new configuration is required. The RADIUS Timeout Set During Pre-Authentication feature is included in all Cisco platforms that support preauthentication, and that have RADIUS attribute 27, Session-Timeout, specified in a preauthentication user profile.

Additional References

- The following sections provide references related to the RADIUS Timeout Set During Pre-Authentication feature.

Related Documents

Related Topic	Document Title
RADIUS attributes and user profiles	<i>Cisco IOS Security Configuration Guide</i> , Release 12.2. Refer to “RADIUS Attributes” in the Appendixes.

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Command Reference

This feature uses no new and modified commands.

No new or modified commands are introduced or modified in the feature documented in this module. For information about commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

Feature Information for RADIUS Timeout Set During Pre-Authentication

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for RADIUS Timeout Set During Pre-Authentication

Feature Name	Releases	Feature Information
RADIUS Timeout Set During Pre-Authentication	12.2(15)T 12.2(28)SB	<p>The RADIUS Timeout Set During Pre-Authentication feature is useful in situations where the PPP authentication that follows the preauthentication phase of these call sessions does not return the Session-Timeout value (RADIUS attribute 27), and therefore allows the ISP to add call setup time to the subscriber's bill.</p> <p>This feature was introduced in Cisco IOS Release 12.2(15)T.</p> <p>This feature was integrated into Cisco IOS Release 12.2(28)SB.</p>

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2003–2007 Cisco Systems, Inc. All rights reserved.



RADIUS Tunnel Attribute Extensions

Feature History

Release	Modification
12.1(5)T	This feature was introduced.
12.2(4)B3	This feature was integrated into Cisco IOS Release 12.2(4)B3.
12.2(13)T	This feature was integrated into Cisco IOS Release 12.2(13)T.
Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

This feature module describes the RADIUS Tunnel Attribute Extensions feature. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 3](#)
- [Supported Standards, MIBs, and RFCs, page 4](#)
- [Prerequisites, page 4](#)
- [Configuration Tasks, page 4](#)
- [Configuration Examples, page 5](#)
- [Command Reference, page 6](#)
- [Glossary, page 7](#)

Feature Overview

The RADIUS Tunnel Attribute Extensions feature introduces RADIUS attribute 90 (Tunnel-Client-Auth-ID) and RADIUS attribute 91 (Tunnel-Server-Auth-ID). Both attributes help support the provision of compulsory tunneling in virtual private networks (VPNs) by allowing the user to specify authentication names for the network access server (NAS) and the RADIUS server.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

How It Works

Once a NAS has set up communication with a RADIUS server, you can enable a tunneling protocol. Some applications of tunneling protocols are voluntary, but others involve compulsory tunneling; that is, a tunnel is created without any action from the user and without allowing the user any choice in the matter. In those cases, new RADIUS attributes are needed to carry the tunneling information from the NAS to the RADIUS server to establish authentication. These new RADIUS attributes are listed in [Table 79](#).


Note

In compulsory tunneling, any security measures in place apply only to traffic between the tunnel endpoints. Encryption or integrity protection of tunneled traffic must not be considered as a replacement for end-to-end security.

Table 79 **RADIUS Tunnel Attributes**

Number	IETF RADIUS Tunnel Attribute	Equivalent TACACS+ Attribute	Supported Protocols	Description
90	Tunnel-Client-Auth-ID	tunnel-id	<ul style="list-style-type: none"> Layer 2 Forwarding (L2F) Layer 2 Tunneling Protocol (L2TP) 	Specifies the name used by the tunnel initiator (also known as the NAS ¹) when authenticating tunnel setup with the tunnel terminator.
91	Tunnel-Server-Auth-ID	gw-name	<ul style="list-style-type: none"> Layer 2 Forwarding (L2F) Layer 2 Tunneling Protocol (L2TP) 	Specifies the name used by the tunnel terminator (also known as the Home Gateway ²) when authenticating tunnel setup with the tunnel initiator.

1. When L2TP is used, the NAS is referred to as an L2TP access concentrator (LAC).
2. When L2TP is used, the Home Gateway is referred to as an L2TP network server (LNS).

RADIUS attribute 90 and RADIUS attribute 91 are included in the following situations:

- If the RADIUS server accepts the request and the desired authentication name is different from the default, they must be included it.
- If an accounting request contains Acct-Status-Type attributes with values of either start or stop and pertains to a tunneled session, they should be included in.

Benefits

The RADIUS Tunnel Attribute Extensions feature allows you to specify a name (other than the default) of the tunnel initiator and the tunnel terminator. Thus, you can establish a higher level of security when setting up VPN tunneling.

Restrictions

Your RADIUS server must support tagged attributes to use RADIUS tunnel attributes 90 and 91.

Related Documents

The following documents provide information related to the RADIUS Tunnel Attribute Extensions feature:

- The chapters “Configuring Authentication” and “Configuring RADIUS” in the *Cisco IOS Security Configuration Guide*, Release 12.2
- The appendix “RADIUS Attributes” in the *Cisco IOS Security Configuration Guide*, Release 12.2
- The chapter “Configuring Virtual Private Networks” in the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2
- RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*

Supported Platforms

Cisco IOS Release 12.1(5)T Only

- AS5300
- AS5800

Cisco IOS Releases 12.2(4)B3 and 12.2(13)T Only

Cisco 6400-NRP-1

Cisco 6400-NRP-2

Cisco 6400-NRP-2SV

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

- RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*

Prerequisites

To use RADIUS attributes 90 and 91, you must complete the following tasks:

- Configure your NAS to support AAA.
- Configure your NAS to support RADIUS.
- Configure your NAS to support VPN.

Configuration Tasks

None

Verifying RADIUS Attribute 90 and RADIUS Attribute 91

To verify that RADIUS attribute 90 and RADIUS attribute 91 are being sent in access accepts and accounting requests, use the following command in privileged EXEC mode:

Command	Purpose
Router# debug radius	Displays information associated with RADIUS. The output of this command shows whether attribute 90 and attribute 91 are being sent in access accepts and accounting requests.

Configuration Examples

This section provides the following configuration examples:

- [L2TP Network Server \(LNS\) Configuration Example](#)
- [RADIUS User Profile with RADIUS Tunneling Attributes 90 and 91 Example](#)

L2TP Network Server (LNS) Configuration Example

The following example shows how to configure the LNS with a basic L2F and L2TP configuration using RADIUS tunneling attributes 90 and 91:

```
aaa new-model
aaa authentication login default none
aaa authentication login console none
aaa authentication ppp default local group radius
aaa authorization network default group radius if-authenticated
!
username l2f-cli-auth-id password 0 l2f-cli-pass
username l2f-svr-auth-id password 0 l2f-svr-pass
username l2tp-svr-auth-id password 0 l2tp-tnl-pass
!
vpdn enable
vpdn search-order domain
!
vpdn-group 1
accept-dialin
protocol l2f
virtual-template 1
terminate-from hostname l2f-cli-auth-id
local name l2f-svr-auth-id
!
vpdn-group 2
accept-dialin
protocol l2tp
virtual-template 2
terminate-from hostname l2tp-cli-auth-id
local name l2tp-svr-auth-id
!
interface Ethernet1/0
ip address 10.0.0.3 255.255.255.0
no ip route-cache
no ip mroute-cache
```

```

!
interface Virtual-Template1
ip unnumbered Ethernet1/0
ppp authentication pap
!
interface Virtual-Template2
ip unnumbered Ethernet1/0
ppp authentication pap
!
radius-server host 1.1.1.1 auth-port 1645 acct-port 1646
radius-server key <deleted>
!

```

RADIUS User Profile with RADIUS Tunneling Attributes 90 and 91 Example

The following is an example of a RADIUS user profile that includes RADIUS tunneling attributes 90 and 91. This entry supports two tunnels, one for L2F and the other for L2TP. The tag entries with :1 support L2F tunnels, and the tag entries with :2 support L2TP tunnels.

```

cisco.com Password = "cisco", Service-Type = Outbound
  Service-Type = Outbound,
  Tunnel-Type = :1:L2F,
  Tunnel-Medium-Type = :1:IP,
  Tunnel-Client-Endpoint = :1:"10.0.0.2",
  Tunnel-Server-Endpoint = :1:"10.0.0.3",
  Tunnel-Client-Auth-Id = :1:"l2f-cli-auth-id",
  Tunnel-Server-Auth-Id = :1:"l2f-svr-auth-id",
  Tunnel-Assignment-Id = :1:"l2f-assignment-id",
  Cisco-Avpair = "vpdn:nas-password=l2f-cli-pass",
  Cisco-Avpair = "vpdn:gw-password=l2f-svr-pass",
  Tunnel-Preference = :1:1,
  Tunnel-Type = :2:L2TP,
  Tunnel-Medium-Type = :2:IP,
  Tunnel-Client-Endpoint = :2:"10.0.0.2",
  Tunnel-Server-Endpoint = :2:"10.0.0.3",
  Tunnel-Client-Auth-Id = :2:"l2tp-cli-auth-id",
  Tunnel-Server-Auth-Id = :2:"l2tp-svr-auth-id",
  Tunnel-Assignment-Id = :2:"l2tp-assignment-id",
  Cisco-Avpair = "vpdn:l2tp-tunnel-password=l2tp-tnl-pass",
  Tunnel-Preference = :2:2

```

Command Reference

This feature uses no new or modified commands. To see the command pages for the commands used with this feature, see the Cisco IOS Security Command Reference at

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at

<http://tools.cisco.com/Support/CLILookup> or the Master Command List.

Glossary

Layer 2 Forwarding (L2F)—A Layer 2 tunneling protocol that enables an ISP or other access service to create a virtual tunnel to link customer remote sites or remote users with corporate home networks. In particular, a network access server (NAS) at the ISP point of presence (POP) exchanges PPP messages with the remote users and communicates by L2F or L2TP requests and responses with the customer tunnel server to set up tunnels.

Layer 2 Tunnel Protocol (L2TP)—A Layer 2 tunneling protocol that enables an ISP or other access service to create a virtual tunnel to link customer remote sites or remote users with corporate home networks. In particular, a network access server (NAS) at the ISP point of presence (POP) exchanges PPP messages with the remote users and communicates by L2F or L2TP requests and responses with the customer tunnel server to set up tunnels.

L2TP access concentrator (LAC)—A network access server (NAS) to which the client directly connects and through which PPP frames are tunneled to the L2TP network server (LNS). The LAC need only implement the media over which L2TP is to operate to pass traffic to one or more LNSs. The LAC may tunnel any protocol carried within PPP. The LAC initiates incoming calls and receives outgoing calls. A LAC is analogous to an L2F network access server.

L2TP network server (LNS)—A termination point for L2TP tunnels, and an access point where PPP frames are processed and passed to higher-layer protocols. An LNS can operate on any platform that terminates PPP. The LNS handles the server side of the L2TP protocol. L2TP relies only on the single medium over which L2TP tunnels arrive. The LNS initiates outgoing calls and receives incoming calls. An LNS is analogous to a home gateway in L2F technology.

network access server (NAS)—A Cisco platform, or collection of platforms, such as an AccessPath system, that interfaces between the packet world (such as the Internet) and the circuit-switched world (such as the PSTN).

tunnel—A virtual pipe between the L2TP access concentrator (LAC) and L2TP network server (LNS) that can carry multiple PPP sessions.

virtual private network (VPN)—A system that permits dial-in networks to exist remotely to home networks, while giving the appearance of being directly connected. VPNs use L2TP and L2F to terminate the Layer 2 and higher parts of the network connection at the L2TP network server (LNS) instead of the L2TP access concentrator (LAC).





V.92 Reporting Using RADIUS Attribute v.92-info

The V.92 Reporting Using RADIUS Attribute v.92-info feature provides the ability to track V.92 call information, such as V.92 features that are supported, the Quick Connect feature set that was attempted, the duration for which the original call was put on hold, and how many times Modem On Hold was initiated. The vendor-specific attribute (VSA) v.92-info is included in accounting “start” and “stop” records when modems negotiate a V.92 connection.

Feature Specifications for the V.92 Reporting Using RADIUS Attribute v.92-info Feature

Feature History

Release	Modification
12.3(1)	This feature was introduced.

Supported Platforms

Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco AS5850

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for V.92 Reporting Using RADIUS Attribute v.92-info, page 2](#)
- [Restrictions for V.92 Reporting Using RADIUS Attribute v.92-info, page 2](#)
- [Information About V.92 Reporting Using RADIUS Attribute v.92-info, page 2](#)
- [Monitoring V.92 Call Information, page 3](#)
- [Verifying V.92 Call Information, page 11](#)
- [Additional References, page 15](#)
- [Command Reference, page 16](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for V.92 Reporting Using RADIUS Attribute v.92-info

Before the network access server (NAS) can send attribute v.92-info information in accounting “start” and “stop” records, you must perform the following tasks:

- Configure your NAS for authentication, authorization, and accounting (AAA) and to accept incoming modem calls.
- Enable AAA accounting by using the **aaa accounting network default start-stop group radius** command in global configuration mode.
- Familiarize yourself with the V.92 Quick Connect feature. Refer to the following document:
 - *V.92 Quick Connect for Cisco AS5300 and Cisco AS5800 Universal Access Servers*
- Familiarize yourself with the V.92 Modem on Hold feature. Refer to the following document:
 - *V.92 Modem on Hold for Cisco AS5300 and Cisco AS5800 Universal Access Servers*

Restrictions for V.92 Reporting Using RADIUS Attribute v.92-info

- If V.92 is not negotiated on your server, V.92 information will not be included in the accounting record.
- Because the attribute v.92-info information is sent as a Cisco VSA, if you configure your RADIUS server as nonstandard (using a non-Cisco server), the V.92 call information will not be sent by default. However, you can still get the V.92 call information by first configuring the **radius-server vsa send** command with the **accounting** keyword (that is, **radius-server vsa send accounting**).

Information About V.92 Reporting Using RADIUS Attribute v.92-info

Before you use the V.92 Reporting Using RADIUS Attribute v.92-info feature, you must understand the following concepts:

- [V.92 Standard Overview, page 2](#)
- [VSA v.92-info, page 3](#)

V.92 Standard Overview

The International Telecommunication Union Telecommunication Standardization Sector (ITU-T) V.92 standard encompasses a number of specifications, including Quick Connect (QC), which dramatically improves how quickly users can connect with their Internet service provider (ISP), and Modem on Hold (MoH), which enables users to suspend and reactivate their dial-up connection to either receive or initiate a telephone call. V.92 also includes pulse code modulation (PCM) upstream, which boosts the upstream data rates from the user to the ISP to reduce transfer times for large files and e-mail attachments sent by the user.

VSA v.92-info

The VSA v.92-info information in RADIUS accounting “start” and “stop” records can help you track V.92 feature set information. The VSA is enabled by default for all sessions that reside over a modem call that is connected using V.92 model modulation.

The VSA information is displayed in the “start” and “stop” records as follows:

```
v92-info=<V.92 features supported>/<QC Exchange>/<Total MOH time>/<MOH count>
```

The VSA v92-info has the following four subfields:

- V.92 features supported—All features that are available for the V.92 modem user who is dialing in. These features include QC, MoH, and PCM Upstream.
- QC Exchange—If QC was initiated, this subfield states what feature set (within QC) was attempted.
- Total MOH time—If MoH was initiated, this subfield indicates the duration for which the original call was put on hold.
- MOH count—If MOH was initiated, this field indicates how many times the MOH was initiated.

The following is an example of VSA v92-info information displayed in an accounting record:

```
v92-info=V.92 QC MOH/QC Requested/60/1
```

How to Monitor and Verify V.92 Call Information

The following sections include tasks to help you monitor and verify V.92 call information:

- [Monitoring V.92 Call Information, page 3](#)
- [Verifying V.92 Call Information, page 11](#)

Monitoring V.92 Call Information

To monitor the V.92 information in the accounting “start” and “stop” records, you can perform the following task using some or all of the debug commands that are listed:

SUMMARY

1. **enable**
2. **debug aaa accounting**
3. **debug aaa authentication**
4. **debug aaa authorization**
5. **debug isdn event**
6. **debug modem csm** [*slot/port* | **group** *group-number*]
7. **debug ppp** {*negotiation* | *authentication*}
8. **debug radius**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	debug aaa accounting Example: Router# debug aaa accounting	Displays information about accountable events as they occur.
Step 3	debug aaa authentication Example: Router# debug aaa authentication	Displays information about AAA authentication.
Step 4	debug aaa authorization Example: Router# debug aaa authorization	Displays information about AAA and TACACS+ authorization.
Step 5	debug isdn event Example: Router# debug isdn event	Displays ISDN events occurring on the user side (on the router) of the ISDN interface.
Step 6	debug modem csm [<i>slot/port</i> group <i>group-number</i>] Example: Router# debug modem csm 1/0 group 1	Displays call switching module (CSM) modem call information.
Step 7	debug ppp { negotiation authentication } Example: Router# debug ppp authentication	Displays information on traffic and exchanges in an internetwork that is implementing the PPP.
Step 8	debug radius Example: Router# debug radius	Displays information associated with RADIUS.

Examples

The following sample debug outputs display information about a V.92 reporting situation:

Debug Output 1

```
01:39:19: ISDN Se7/6:23: RX <-  SETUP pd = 8  callref = 0x42A0
01:39:19:          Bearer Capability i = 0x9090A2
01:39:19:          Channel ID i = 0xA18396
01:39:19:          Progress Ind i = 0x8183 - Origination address is non-ISDN
01:39:19:          Calling Party Number i = 0xA1, '60112', Plan:ISDN, Type:National
```

```
01:39:19:      Called Party Number i = 0xA1, '50138', Plan:ISDN, Type:National
01:39:19:      Locking Shift to Codeset 6
01:39:19:      Codeset 6 IE 0x28 i = 'ANALOG,savitha'
01:39:19: ISDN Se7/6:23: Incoming call id = 0x0038, dsl 0
01:39:19: ISDN Se7/6:23: NegotiateBchan: bchan 22 intid 0 serv_st 0 chan_st 0 callid
0x0000 ev 0x90 n/w? 0
01:39:19: Negotiated int_id 0 bchan 0 cr=0xC2A0 callid=0x0038 lo_chan 22 final
int_id/bchan 0/22 cause 0x0
01:39:19: ISDN Se7/6:23: LIF_EVENT: ces/callid 1/0x38 CALL_INCOMING
01:39:19: ISDN Se7/6:23: CALL_INCOMING dsl 0 bchan 21
01:39:19: voice_parse_intf_name: Using the old NAS_PORT string
01:39:19: AAA/ACCT/EVENT/(00000007): CALL START
01:39:19: AAA/ACCT(00000000): add node, session 9
01:39:19: AAA/ACCT/NET(00000007): add, count 1
01:39:19: AAA/ACCT/EVENT/(00000007): ATTR REPLACE
01:39:19: ISDN Se7/6:23: CALL_INCOMING: call type is VOICE ULAW, bchan = 21
01:39:19: ISDN Se7/6:23: Event: Received a VOICE call from 60112 on B21 at 64 Kb/s Tone
Value 0
01:39:19: AAA/ACCT/DS0: channel=21, dsl=6, t3=0, slot=7, ds0=117465109
01:39:19: AAA/ACCT/DS0: channel=21, dsl=6, t3=0, slot=7, ds0=117465109
01:39:19: VDEV_ALLOCATE: 1/5 is allocated
01:39:19: ISDN Se7/6:23: RM returned call_type 1 resource type 0 response 2
01:39:19: EVENT_FROM_ISDN: dchan_idb=0x63B3D334, call_id=0x38, ces=0x0
bchan=0x15, event=0x1, cause=0x0
01:39:19: dev in call to isdn : set dnis_collected & fap_notify
01:39:19: EVENT_FROM_ISDN:(0038): DEV_INCALL at slot 1 and port 5
01:39:19: EVENT_FROM_ISDN: decode:calling oct3 0xA1, called oct3 0xA1, oct3a 0x0,mask 0x3D
01:39:19: EVENT_FROM_ISDN: csm_call_info:calling oct3 0xA1, called oct3 0xA1, oct3a
0x0,mask 0x3D
01:39:19: CSM_PROC_IDLE: CSM_EVENT_ISDN_CALL at slot 1, port 5
01:39:19: CSM DSPLIB(1/5/csm_flags=0x12): np_dsplib_prepare_modem
01:39:19: CSM_connect_pri_vdev: TS allocated at bp_stream 0, bp_Ch 5, vdev_common
0x62EAD8F4 1/5
01:39:19: ISDN Se7/6:23: EVENT to CSM:DEV_INCALL: calltype=VOICE, bchan=21
01:39:19: ISDN Se7/6:23: TX -> CALL_PROC pd = 8 callref = 0xC2A0
01:39:19:      Channel ID i = 0xA98396
01:39:19: ISDN Se7/6:23: TX -> ALERTING pd = 8 callref = 0xC2A0
01:39:19: CSM DSPLIB(1/5):DSPLIB_MODEM_INIT: Modem session transition to IDLE
01:39:19: CSM DSPLIB(1/5): Modem went offhook
01:39:19: CSM_PROC_IC2_RING: CSM_EVENT_MODEM_OFFHOOK at slot 1, port 5
01:39:19: ISDN Se7/6:23: VOICE_ANS Event: call id 0x38, bchan 21, ces 0
01:39:19: ISDN Se7/6:23: isdn_send_connect(): msg 74, call id 0x38, ces 0 bchan 21, call
type VOICE
01:39:19: ISDN Se7/6:23: TX -> CONNECT pd = 8 callref = 0xC2A0
01:39:19: ISDN Se7/6:23: RX <- CONNECT_ACK pd = 8 callref = 0x42A0
01:39:19: ISDN Se7/6:23: LIF_EVENT: ces/callid 1/0x38 CALL_PROGRESS
01:39:19: ISDN Se7/6:23: event CALL_PROGRESS dsl 0
01:39:19: ISDN Se7/6:23: CALL_PROGRESS: CALL_CONNECTED call id 0x38, bchan 21, dsl 0
01:39:19: EVENT_FROM_ISDN: dchan_idb=0x63B3D334, call_id=0x38, ces=0x0
bchan=0x15, event=0x4, cause=0x0
01:39:19: EVENT_FROM_ISDN:(0038): DEV_CONNECTED at slot 1 and port 5
01:39:19: CSM_PROC_IC6_WAIT_FOR_CONNECT: CSM_EVENT_ISDN_CONNECTED at slot 1, port 5
01:39:19: CSM DSPLIB(1/5): np_dsplib_call_accept
01:39:19: ISDN Se7/6:23: EVENT to CSM:DEV_CONNECTED: calltype=VOICE, bchan=21
01:39:19: CSM DSPLIB(1/5):DSPLIB_MODEM_WAIT_ACTIVE: Modem session transition to ACTIVE
01:39:19: CSM DSPLIB(1/5): Modem state changed to (CONNECT_STATE)
01:39:22: CSM DSPLIB(1/5): Modem state changed to (V8BIS_EXCHANGE_STATE)
01:39:24: CSM DSPLIB(1/5): Modem state changed to (LINK_STATE)
01:39:28: CSM DSPLIB(1/5): Modem state changed to (RANGING_STATE)
01:39:30: CSM DSPLIB(1/5): Modem state changed to (HALF_DUPLEX_TRAIN_STATE)
01:39:45: CSM DSPLIB(1/5): Modem state changed to (TRAINUP_STATE)
01:39:45: CSM DSPLIB(1/5): Modem state changed to (EC_NEGOTIATING_STATE)
01:39:46: CSM DSPLIB(1/5): Modem state changed to (STEADY_STATE)
01:39:46: TTY1/05: DSR came up
```

```

01:39:46: tty1/05: Modem: IDLE->(unknown)
01:39:46: TTY1/05: EXEC creation
01:39:46: CHAT1/05: Attempting line activation script
01:39:46: CHAT1/05: Asserting DTR
01:39:50: voice_parse_intf_name: Using the old NAS_PORT string
01:39:50: voice_parse_intf_name: Using the old NAS_PORT string
01:39:50: AAA/AUTHEN/LOGIN (00000007): Pick method list 'default'
01:39:50: RADIUS/ENCODE(00000007): ask "Username: "
01:39:50: RADIUS/ENCODE(00000007): send packet; GET_USER
01:39:50: TTY1/05: set timer type 10, 30 seconds
01:39:50: TTY1/05: Autoselect(2) sample 7E
01:39:50: TTY1/05: Autoselect(2) sample 7EFF
01:39:50: TTY1/05: Autoselect(2) sample 7EFF7D
01:39:50: TTY1/05: Autoselect(2) sample 7EFF7D23
01:39:50: TTY1/05 Autoselect cmd: ppp negotiate
01:39:50: TTY1/05: EXEC creation
01:39:50: CHAT1/05: Attempting line activation script
01:39:50: CHAT1/05: Asserting DTR
01:39:54: voice_parse_intf_name: Using the old NAS_PORT string
01:39:54: voice_parse_intf_name: Using the old NAS_PORT string
01:39:54: TTY1/05: no timer type 1 to destroy
01:39:54: TTY1/05: no timer type 0 to destroy
01:39:54: As1/05 LCP: I CONFREQ [Closed] id 0 len 50
01:39:54: As1/05 LCP:   ACCM 0x00000000 (0x020600000000)
01:39:54: As1/05 LCP:   MagicNumber 0x00002EB8 (0x050600002EB8)
01:39:54: As1/05 LCP:   PFC (0x0702)
01:39:54: As1/05 LCP:   ACFC (0x0802)
01:39:54: As1/05 LCP:   Callback 6 (0x0D0306)
01:39:54: As1/05 LCP:   MRRU 1614 (0x1104064E)
01:39:54: As1/05 LCP:   EndpointDisc 1 Local
01:39:54: As1/05 LCP:   (0x131701CC7F60A0E7A211D6B549000102)
01:39:54: As1/05 LCP:   (0x2BC4390000000000)
01:39:54: As1/05 LCP: Lower layer not up, Fast Starting
01:39:54: voice_parse_intf_name: Using the old NAS_PORT string
01:39:54: voice_parse_intf_name: Using the old NAS_PORT string
01:39:54: As1/05 PPP: Treating connection as a callin
01:39:54: As1/05 PPP: Phase is ESTABLISHING, Passive Open
01:39:54: As1/05 LCP: State is Listen
01:39:54: As1/05 PPP: Authorization required
01:39:54: As1/05 LCP: O CONFREQ [Listen] id 1 len 25
01:39:54: As1/05 LCP:   ACCM 0x000A0000 (0x0206000A0000)
01:39:54: As1/05 LCP:   AuthProto CHAP (0x0305C22305)
01:39:54: As1/05 LCP:   MagicNumber 0x099EBCBA (0x0506099EBCBA)
01:39:54: As1/05 LCP:   PFC (0x0702)
01:39:54: As1/05 LCP:   ACFC (0x0802)
01:39:54: As1/05 LCP: O CONFREQ [Listen] id 0 len 11
01:39:54: As1/05 LCP:   Callback 6 (0x0D0306)
01:39:54: As1/05 LCP:   MRRU 1614 (0x1104064E)
01:39:54: As1/05 LCP: I CONFACK [REQsent] id 1 len 25
01:39:54: As1/05 LCP:   ACCM 0x000A0000 (0x0206000A0000)
01:39:54: As1/05 LCP:   AuthProto CHAP (0x0305C22305)
01:39:54: As1/05 LCP:   MagicNumber 0x099EBCBA (0x0506099EBCBA)
01:39:54: As1/05 LCP:   PFC (0x0702)
01:39:54: As1/05 LCP:   ACFC (0x0802)
01:39:54: As1/05 LCP: I CONFREQ [ACKrcvd] id 1 len 43
01:39:54: As1/05 LCP:   ACCM 0x00000000 (0x020600000000)
01:39:54: As1/05 LCP:   MagicNumber 0x00002EB8 (0x050600002EB8)
01:39:54: As1/05 LCP:   PFC (0x0702)
01:39:54: As1/05 LCP:   ACFC (0x0802)
01:39:54: As1/05 LCP:   EndpointDisc 1 Local
01:39:54: As1/05 LCP:   (0x131701CC7F60A0E7A211D6B549000102)
01:39:54: As1/05 LCP:   (0x2BC4390000000000)
01:39:54: As1/05 LCP: O CONFACK [ACKrcvd] id 1 len 43
01:39:54: As1/05 LCP:   ACCM 0x00000000 (0x020600000000)

```

```

01:39:54: As1/05 LCP: MagicNumber 0x00002EB8 (0x050600002EB8)
01:39:54: As1/05 LCP: PFC (0x0702)
01:39:54: As1/05 LCP: ACFC (0x0802)
01:39:54: As1/05 LCP: EndpointDisc 1 Local
01:39:54: As1/05 LCP: (0x131701CC7F60A0E7A211D6B549000102)
01:39:54: As1/05 LCP: (0x2BC43900000000)
01:39:54: As1/05 LCP: State is Open
01:39:54: As1/05 PPP: Phase is AUTHENTICATING, by this end
01:39:54: As1/05 CHAP: O CHALLENGE id 1 len 26 from "s5400"
01:39:54: As1/05 LCP: I IDENTIFY [Open] id 2 len 18 magic 0x00002EB8 MSRASV4.00
01:39:54: As1/05 LCP: I IDENTIFY [Open] id 3 len 23 magic 0x00002EB8 MSRAS-1-PTE-PC1
01:39:54: As1/05 CHAP: I RESPONSE id 1 len 34 from "Administrator"
01:39:54: As1/05 PPP: Phase is FORWARDING, Attempting Forward
01:39:54: As1/05 PPP: Phase is AUTHENTICATING, Unauthenticated User
01:39:54: AAA/AUTHEN/PPP (00000007): Pick method list 'default'
01:39:54: As1/05 PPP: Sent CHAP LOGIN Request
01:39:54: RADIUS/ENCODE(00000007): Unsupported AAA attribute parent-interface
01:39:54: RADIUS/ENCODE(00000007): Unsupported AAA attribute parent-interface-type
01:39:54: RADIUS/ENCODE(00000007): acct_session_id: 9
01:39:54: RADIUS(00000007): sending
01:39:54: RADIUS: Send to unknown id 2 10.107.164.120:1645, Access-Request, len 128
01:39:54: RADIUS: authenticator 13 E4 F2 9F BC 3E CE 52 - CC 93 0C E0 01 0C 73 7B
01:39:54: RADIUS: Framed-Protocol [7] 6 PPP [1]
01:39:54: RADIUS: User-Name [1] 15 "Administrator"
01:39:54: RADIUS: CHAP-Password [3] 19 *
01:39:54: RADIUS: Called-Station-Id [30] 7 "50138"
01:39:54: RADIUS: Calling-Station-Id [31] 7 "60112"
01:39:54: RADIUS: Vendor, Cisco [26] 30
01:39:54: RADIUS: cisco-nas-port [2] 24 "Async1/05*Serial7/6:21"
01:39:54: RADIUS: NAS-Port [5] 6 221
01:39:54: RADIUS: NAS-Port-Type [61] 6 Async [0]
01:39:54: RADIUS: Service-Type [6] 6 Framed [2]
01:39:54: RADIUS: NAS-IP-Address [4] 6 10.0.58.107
01:39:54: RADIUS: Received from id 2 10.107.164.120:1645, Access-Accept, len 62
01:39:54: RADIUS: authenticator EF 45 A3 D4 A7 EE D0 65 - 03 50 B4 3E 07 87 2E 2F
01:39:54: RADIUS: Vendor, Cisco [26] 30
01:39:54: RADIUS: cisco-nas-port [2] 24 "Async1/05*Serial7/6:21"
01:39:54: RADIUS: Service-Type [6] 6 Framed [2]
01:39:54: RADIUS: Framed-Protocol [7] 6 PPP [1]
01:39:54: RADIUS: Received from id 7
01:39:54: As1/05 PPP: Received LOGIN Response PASS
01:39:54: As1/05 PPP/AAA: Check Attr: interface
01:39:54: As1/05 PPP/AAA: Check Attr: service-type
01:39:54: As1/05 PPP/AAA: Check Attr: Framed-Protocol
01:39:54: As1/05 PPP: Phase is FORWARDING, Attempting Forward
01:39:54: As1/05 PPP: Phase is AUTHENTICATING, Authenticated User
01:39:54: As1/05 AAA/AUTHOR/LCP: Process Author
01:39:54: As1/05 AAA/AUTHOR/LCP: Process Attr: service-type
01:39:54: As1/05 CHAP: O SUCCESS id 1 len 4
01:39:54: AAA/ACCT/NET(00000007): Pick method list 'default'
01:39:54: AAA/ACCT/SETMLIST(00000007): Handle FFFFFFFF, mlist 630B11E4, Name default
01:39:54: AAA/ACCT/EVENT/(00000007): NET UP
01:39:54: AAA/ACCT/NET(00000007): Queueing record is START
01:39:54: As1/05 PPP: Phase is UP
01:39:54: As1/05 AAA/AUTHOR/PCP: FSM authorization not needed
01:39:54: As1/05 AAA/AUTHOR/FSM: We can start PCP
01:39:54: As1/05 IPCP: O CONFREQ [Closed] id 1 len 10
01:39:54: As1/05 IPCP: Address 10.1.1.2 (0x030646010102)
01:39:54: AAA/ACCT(00000007): Accounting method=radius (radius)
01:39:54: RADIUS/ENCODE(00000007): Unsupported AAA attribute timezone
01:39:54: RADIUS/ENCODE(00000007): Unsupported AAA attribute parent-interface
01:39:54: RADIUS/ENCODE(00000007): Unsupported AAA attribute parent-interface-type
01:39:54: RADIUS(00000007): sending
01:39:54: RADIUS: Send to unknown id 8 10.107.164.120:1646, Accounting-Request, len 243

```

8

```

01:39:54: As1/05 AAA/AUTHOR/PCP: no author-info for primary dns
01:39:54: As1/05 AAA/AUTHOR/PCP: no author-info for primary wins
01:39:54: As1/05 AAA/AUTHOR/PCP: no author-info for seconday dns
01:39:54: As1/05 AAA/AUTHOR/PCP: no author-info for seconday wins
01:39:54: As1/05 PCP: O CONFREQ [REQsent] id 5 len 28
01:39:54: As1/05 PCP: PrimaryDNS 0.0.0.0 (0x810600000000)
01:39:54: As1/05 PCP: PrimaryWINS 0.0.0.0 (0x820600000000)
01:39:54: As1/05 PCP: SecondaryDNS 0.0.0.0 (0x830600000000)
01:39:54: As1/05 PCP: SecondaryWINS 0.0.0.0 (0x840600000000)
01:39:54: As1/05 PCP: I CONFACK [REQsent] id 1 len 10
01:39:54: As1/05 PCP: Address 70.1.1.2 (0x030646010102)
01:39:54: As1/05 PCP: I CONFREQ [ACKrcvd] id 6 len 10
01:39:54: As1/05 PCP: Address 0.0.0.0 (0x030600000000)
01:39:54: As1/05 PCP: O CONFNAK [ACKrcvd] id 6 len 10
01:39:54: As1/05 PCP: Address 70.2.2.6 (0x030646020206)
01:39:55: As1/05 PCP: I CONFREQ [ACKrcvd] id 7 len 10
01:39:55: As1/05 PCP: Address 70.2.2.6 (0x030646020206)
01:39:55: As1/05 PCP: O CONFACK [ACKrcvd] id 7 len 10
01:39:55: As1/05 PCP: Address 70.2.2.6 (0x030646020206)
01:39:55: As1/05 PCP: State is Open
01:39:55: AAA/ACCT/EVENT/(00000007): PCP_PASS
01:39:55: As1/05 PCP: Install route to 10.2.2.6
01:39:55: As1/05 PCP: Add link info for cef entry 10.2.2.6

```

Debug Output 2

```

01:40:50: ISDN Se7/6:23: RX <- DISCONNECT pd = 8 callref = 0x42A0
01:40:50: Cause i = 0x8190 - Normal call clearing
01:40:50: ISDN Se7/6:23: LIF_EVENT: ces/callid 1/0x38 CALL_DISC
01:40:50: EVENT_FROM_ISDN: dchan_idb=0x63B3D334, call_id=0x38, ces=0x0
    bchan=0x15, event=0x0, cause=0x10
01:40:50: EVENT_FROM_ISDN:(0038): DEV_IDLE at slot 1 and port 5
01:40:50: CSM_PROC_IC7_OC6_CONNECTED: CSM_EVENT_ISDN_DISCONNECTED at slot 1, port 5
01:40:50: CSM DSPLIB(1/5): np_dsplib_call_hangup reason 14
01:40:50: CSM(1/5): Enter csm_enter_disconnecting_state
01:40:50: VDEV_DEALLOCATE: slot 1 and port 5 is deallocated

01:40:50: ISDN Se7/6:23: EVENT to CSM:DEV_IDLE: calltype=VOICE, bchan=21
01:40:50: ISDN Se7/6:23: process_disc_ack(): call id 0x38, ces 0, call type VOICE cause
0x10
01:40:50: ISDN Se7/6:23: TX -> RELEASE pd = 8 callref = 0xC2A0
01:40:50: AAA/ACCT/EVENT/(00000007): CALL STOP
01:40:50: AAA/ACCT/CALL STOP(00000007): Sending stop requests
01:40:50: AAA/ACCT(00000007): Send all stops
01:40:50: AAA/ACCT/NET(00000007): STOP
01:40:50: AAA/ACCT/NET(00000007): Queueing record is STOP osr 1
01:40:50: AAA/ACCT(00000007): Accounting method=radius (radius)
01:40:50: RADIUS/ENCODE(00000007): Unsupported AAA attribute timezone
01:40:50: RADIUS/ENCODE(00000007): Unsupported AAA attribute parent-interface
01:40:50: RADIUS/ENCODE(00000007): Unsupported AAA attribute parent-interface-type
01:40:50: RADIUS(00000007): sending
01:40:50: RADIUS: Send to unknown id 9 10.107.164.120:1646, Accounting-Request, len 315
01:40:50: RADIUS: authenticator 2E 6A 04 D0 04 9A D3 D5 - F7 DD 99 E0 C3 99 27 60
01:40:50: RADIUS: Acct-Session-Id [44] 10 "00000009"
01:40:50: RADIUS: Framed-Protocol [7] 6 PPP [1]
01:40:50: RADIUS: Framed-IP-Address [8] 6 70.2.2.6
01:40:50: RADIUS: Acct-Terminate-Cause[49] 6 lost-carrier [2]
01:40:50: RADIUS: Vendor, Cisco [26] 33
01:40:50: RADIUS: Cisco AVpair [1] 27 "disc-cause-ext=No Carrier"
01:40:50: RADIUS: Vendor, Cisco [26] 35
01:40:50: RADIUS: Cisco AVpair [1] 29 "connect-progress=LAN Ses Up"
01:40:50: RADIUS: Acct-Session-Time [46] 6 56
01:40:50: RADIUS: Connect-Info [77] 26 "52000/28800 V90/V44/LAPM"
01:40:50: RADIUS: Vendor, Cisco [26] 48

```

How to Monitor and Verify V.92 Call Information

```

01:40:50: RADIUS: Cisco AVpair [1] 42 "v92-info=V.92 QC MOH/No QC
Requested/0/0"
01:40:50: RADIUS: Acct-Input-Octets [42] 6 285
01:40:50: RADIUS: Acct-Output-Octets [43] 6 295
01:40:50: RADIUS: Acct-Input-Packets [47] 6 5
01:40:50: RADIUS: Acct-Output-Packets [48] 6 5
01:40:50: RADIUS: User-Name [1] 15 "Administrator"
01:40:50: RADIUS: Acct-Status-Type [40] 6 Stop [2]
01:40:50: RADIUS: Called-Station-Id [30] 7 "50138"
01:40:50: RADIUS: Calling-Station-Id [31] 7 "60112"
01:40:50: RADIUS: Vendor, Cisco [26] 30
01:40:50: RADIUS: cisco-nas-port [2] 24 "Async1/05*Serial7/6:21"
01:40:50: RADIUS: NAS-Port [5] 6 221
01:40:50: RADIUS: NAS-Port-Type [61] 6 Async [0]
01:40:50: RADIUS: Service-Type [6] 6 Framed [2]
01:40:50: RADIUS: NAS-IP-Address [4] 6 10.0.58.107
01:40:50: RADIUS: Acct-Delay-Time [41] 6 0
01:40:50: RADIUS: Received from id 9 10.107.164.120:1646, Accounting-response, len 20
01:40:50: RADIUS: authenticator D0 3F 32 D7 7C 8C 5E 22 - 9A 69 EF 17 AC 32 81 21
01:40:50: AAA/ACCT/NET(00000007): STOP protocol reply PASS
01:40:50: AAA/ACCT/NET(00000007): Cleaning up from Callback osr 0
01:40:50: AAA/ACCT(00000007): del node, session 9
01:40:50: AAA/ACCT/NET(00000007): free_rec, count 0
01:40:50: AAA/ACCT/NET(00000007) recnt 0, csr TRUE, osr 0
01:40:50: AAA/ACCT/NET(00000007): Last rec in db, intf not enqueued
01:40:50: ISDN Se7/6:23: RX <- RELEASE_COMP pd = 8 callref = 0x42A0
01:40:50: ISDN Se7/6:23: CCPRI_ReleaseCall(): bchan 22, call id 0x38, call type VOICE
01:40:50: CCPRI_ReleaseChan released b_dsl 0 B_Chan 22
01:40:50: ISDN Se7/6:23: LIF_EVENT: ces/callid 1/0x38 CALL_CLEARED
01:40:50: ISDN Se7/6:23: received CALL_CLEARED call_id 0x38
01:40:50: no resend setup, no redial
01:40:50: no resend setup, no redial
01:40:50: AAA/ACCT/DS0: channel=21, ds1=6, t3=0, slot=7, ds0=117465109
01:40:50: EVENT_FROM_ISDN: dchan_idb=0x63B3D334, call_id=0x38, ces=0x1
bchan=0x15, event=0x0, cause=0x0
01:40:50: ISDN Se7/6:23: EVENT to CSM:DEV_IDLE: calltype=VOICE, bchan=21
01:40:51: CSM DSPLIB(1/5): Modem state changed to (TERMINATING_STATE)
01:40:51: CSM DSPLIB(1/5): Modem went onhook
01:40:51: CSM_PROC_IC8_OC8_DISCONNECTING: CSM_EVENT_MODEM_ONHOOK at slot 1, port 5
01:40:51: CSM(1/5): Enter csm_enter_idle_state
01:40:51: CSM DSPLIB(1/5):DSPLIB_IDLE: Modem session transition to FLUSHING
01:40:51: CSM DSPLIB(1/5):DSPLIB_IDLE: Modem session transition to IDLE
01:40:51: TTY1/05: DSR was dropped
01:40:51: tty1/05: Modem: READY->(unknown)
01:40:52: TTY1/05: dropping DTR, hanging up
01:40:52: DSPLIB(1/5): np_dsplib_process_dtr_notify()
01:40:52: CSM DSPLIB(1/5): Modem went onhook
01:40:52: CSM_PROC_IDLE: CSM_EVENT_MODEM_ONHOOK at slot 1, port 5
01:40:52: TTY1/05: Async Int reset: Dropping DTR
01:40:52: tty1/05: Modem: HANGUP->(unknown)
01:40:52: AAA/ACCT/EVENT/(00000007): NET DOWN
01:40:52: As1/05 IPCP: Remove link info for cef entry 70.2.2.6
01:40:52: As1/05 IPCP: State is Closed
01:40:52: As1/05 PPP: Phase is TERMINATING
01:40:52: As1/05 LCP: State is Closed
01:40:52: As1/05 PPP: Phase is DOWN
01:40:52: As1/05 IPCP: Remove route to 70.2.2.6
01:40:52: As1/05 LCP: State is Closed
01:40:53: TTY1/05: cleanup pending. Delaying DTR
01:40:54: TTY1/05: cleanup pending. Delaying DTR
01:40:55: TTY1/05: cleanup pending. Delaying DTR
01:40:56: TTY1/05: cleanup pending. Delaying DTR
01:40:57: TTY1/05: no timer type 0 to destroy
01:40:57: TTY1/05: no timer type 1 to destroy

```

```

01:40:57: TTY1/05: no timer type 3 to destroy
01:40:57: TTY1/05: no timer type 4 to destroy
01:40:57: TTY1/05: no timer type 2 to destroy
01:40:57: Async1/05: allowing modem_process to continue hangup
01:40:57: TTY1/05: restoring DTR
01:40:57: TTY1/05: autoconfigure probe started
01:40:57: As1/05 LCP: State is Closed

```

Verifying V.92 Call Information

To verify that the V.92 call was correctly established, use the following **show** commands:

SUMMARY

- **show modem** [*slot/port* | *group number*]
- **show port modem log** [*reverse slot/port*] [*slot* | *slot/port*]
- **show users** [*all*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	show modem [<i>slot/port</i> <i>group number</i>] Example: Router# show modem 1/0 group 1	Displays a high-level performance report for all the modems or a single modem inside Cisco access servers.
Step 2	show port modem log [<i>reverse slot/port</i>] [<i>slot</i> <i>slot/port</i>] Example: Router# show port modem log	Displays the events generated by the modem sessions.
Step 3	show users [<i>all</i>] Example: Router# show users	Displays information about the active lines on the router.

Examples

The following V.92 reporting outputs are from the **show port modem log** and **show users** commands:

Show Output 1

```
Router# show port modem log 1/05
```

```

Port 1/05 Events Log
 01:46:19: Service Type: DATA_FAX_MODEM
 01:46:19: Service Mode: DATA_FAX_MODEM
 01:46:19: Session State: IDLE
 01:46:19: incoming caller number: 60112
 01:46:19: incoming called number: 50138
 01:46:19: Service Type: DATA_FAX_MODEM
 01:46:19: Service Mode: DATA_FAX_MODEM

```



```

01:46:19: Session State: IDLE
01:46:19: Service Type: DATA_FAX_MODEM
01:46:19: Service Mode: DATA_FAX_MODEM
01:46:19: Session State: ACTIVE
01:46:19: Modem State event:
      State: Connect
01:46:20: Modem State event:
      State: V.8bis Exchange
01:46:20: Modem State event:
      State: Link
01:46:20: Modem State event:
      State: Ranging
01:46:20: Modem State event:
      State: Half Duplex Train
01:46:20: Modem State event:
      State: Train Up
01:46:20: Modem State event:
      State: EC Negotiating
01:46:20: Modem State event:
      State: Steady
01:46:20: Modem Static event:
      Connect Protocol           : LAP-M
      Compression                : V.44
      Connected Standard         : V.90
      TX,RX Symbol Rate          : 8000, 3200
      TX,RX Carrier Frequency    : 0, 1829
      TX,RX Trellis Coding       : 16/No trellis
      Frequency Offset           : 0 Hz
      Round Trip Delay           : 0 msecs
      TX,RX Bit Rate             : 52000, 28800
      Robbed Bit Signalling (RBS) pattern : 255
      Digital Pad                : 6 dB
      Digital Pad Compensation   : Enabled
      MNP10EC                   : Off-None
      QC Exchange               : No QC Requested
      TX,RX Negotiated String Length : 255, 255
      DC TX,RX Negotiated Codewords : 1024, 1024
      DC TX,RX Negotiated History Size : 4096, 5120
01:46:21: ISDN Se7/6:23: RX <- SERVICE pd = 3 callref = 0x0000
01:46:21: Change Status i = 0xC0 - in-service
01:46:21: Channel ID i = 0xA98381
01:46:21: ISDN Se7/6:23: Incoming call id = 0x003A, dsl 0
01:46:21: ISDN Se7/6:23: LIF_EVENT: ces/callid 1/0x0 CHAN_STATUS
01:46:21: ISDN Se7/6:23: CHAN_STATUS B-chan=1, action=2; Maintenance.
01:46:21: ISDN Se7/6:23: TX -> SERVICE ACKNOWLEDGE pd = 3 callref = 0x8000
01:46:21: Change Status i = 0xC0 - in-service
01:46:21: Channel ID i = 1
s5400#sh port modem log 1/05
Port 1/05 Events Log
01:46:30: Service Type: DATA_FAX_MODEM
01:46:30: Service Mode: DATA_FAX_MODEM
01:46:30: Session State: IDLE
01:46:30: incoming caller number: 60112
01:46:30: incoming called number: 50138
01:46:30: Service Type: DATA_FAX_MODEM
01:46:30: Service Mode: DATA_FAX_MODEM
01:46:30: Session State: IDLE
01:46:30: Service Type: DATA_FAX_MODEM
01:46:30: Service Mode: DATA_FAX_MODEM
01:46:30: Session State: ACTIVE
01:46:30: Modem State event:
      State: Connect
01:46:30: Modem State event:
      State: V.8bis Exchange

```

```

01:46:30: Modem State event:
        State: Link
01:46:30: Modem State event:
        State: Ranging
01:46:30: Modem State event:
        State: Half Duplex Train
01:46:30: Modem State event:
        State: Train Up
01:46:31: Modem State event:
        State: EC Negotiating
01:46:31: Modem State event:
        State: Steady
01:46:31: Modem Static event:
        Connect Protocol           : LAP-M
        Compression                : V.44
        Connected Standard         : V.90
        TX,RX Symbol Rate          : 8000, 3200
        TX,RX Carrier Frequency    : 0, 1829
        TX,RX Trellis Coding       : 16/No trellis
        Frequency Offset           : 0 Hz
        Round Trip Delay           : 0 msecs
        TX,RX Bit Rate             : 52000, 28800
        Robbed Bit Signalling (RBS) pattern : 255
        Digital Pad                : 6 dB
        Digital Pad Compensation   : Enabled
        MNP10EC                   : Off-None
        QC Exchange                : No QC Requested
        TX,RX Negotiated String Length : 255, 255
        DC TX,RX Negotiated Codewords : 1024, 1024
        DC TX,RX Negotiated History Size : 4096, 5120
        Diagnostic Code            : 00 00 00 00 00 00 00 00
        V.92 Status                : V.92 QC MOH
01:46:32: Modem Dynamic event:
        Sq Value                   : 6
        Signal Noise Ratio         : 38 dB
        Receive Level              : -11 dBm
        Phase Jitter Frequency     : 0 Hz
        Phase Jitter Level        : 0 degrees
        Far End Echo Level         : 0 dBm
        Phase Roll                 : 0 degrees
        Total Retrans              : 0
        EC Retransmission Count    : 0
        Characters transmitted, received : 0, 0
        Characters received BAD    : 0
        PPP/SLIP packets transmitted, received : 0, 0
        PPP/SLIP packets received (BAD/ABORTED) : 0
        EC packets transmitted, received OK : 0, 0
        EC packets (Received BAD/ABORTED) : 0
        Total Speedshifts         : 0
        Total MOH Time             : 0 secs
        Current MOH Time          : 0 secs
        MOH Status                 : Modem is Not on Hold
        MOH Count                  : 0
        MOH Request Count         : 0
        Retrans due to Call Waiting : 0
        DC Encoder,Decoder State   : compressed/compressed
        DC TX,RX Compression Ratio : not calculated/not calculated
        DC TX,RX Dictionary Reset Count : 0, 0
        Diagnostic Code            : 00 00 00 00 00 00 00 00
01:46:35: Modem State event:
        State: Terminate
01:46:35: Service Type: DATA_FAX_MODEM
01:46:35: Service Mode: DATA_FAX_MODEM
01:46:35: Session State: FLUSHING

```

```

01:46:35: Service Type: DATA_FAX_MODEM
01:46:35: Service Mode: DATA_FAX_MODEM
01:46:35: Session State: IDLE
01:46:35: Modem End Connect event:
  Call Timer                               :    65  secs
  Disconnect Reason Info                   :    0x220
    Type (=0 ): <unknown>
    Class (=2 ): EC condition - locally detected
    Reason (=32 ): received DISC frame -- normal LAPM termination
  Total Retransmits                        :    0
  EC Retransmission Count                  :    0
  Characters transmitted, received         :   677, 817
  Characters received BAD                   :    0
  PPP/SLIP packets transmitted, received   :   10, 10
  PPP/SLIP packets received (BAD/ABORTED) :    0
  EC packets transmitted, received OK       :   10, 21
  EC packets (Received BAD/ABORTED)        :    0
  TX,RX Bit Rate                          :  52000, 28800
  Total Speedshifts                       :    0
  Total MOH Time                          :    0  secs
  Current MOH Time                        :    0  secs
  MOH Status                              :  Modem is Not on Hold
  MOH Count                               :    0
  MOH Request Count                       :    0
  Retransmits due to Call Waiting          :    0
  DC Encoder,Decoder State                 :  compressed/compressed
  DC TX,RX Compression Ratio               :   1.67:1/1.65:1
  DC TX,RX Dictionary Reset Count          :    0, 1
  Diagnostic Code                          :   00 00 00 00 00 00 00 00
01:46:37:Modem Link Rate event:

```

Show Output 2

Router# **show users**

Line	User	Host(s)	Idle	Location
* 0 con 0		idle	00:00:00	
tty 1/05	Administra	Async interface	00:00:29	PPP: 70.2.2.6

Interface	User	Mode	Idle	Peer Address
-----------	------	------	------	--------------

Troubleshooting Tips

If you see that V.92 call information is not being reported by AAA, ensure that the call is a V.92 call by using the **show modem** command or by looking at the modem logs by using the **show modem log** command.

Additional References

For additional information related to the V.92 Reporting Using RADIUS Attribute v.92-info feature, refer to the following references:

Related Documents

Related Topic	Document Title
AAA accounting	<i>The chapters “AAA Overview” and “Configuring Accounting” in the “Authentication, Authorization, and Accounting” section of the Cisco IOS Security Configuration Guide, Release 12.3.</i>
AAA accounting commands	<i>The Cisco IOS Security Command Reference, Release 12.3.</i>
V.92 Quick Connect feature	<i>V.92 Quick Connect for Cisco AS5300 and Cisco AS5800 Universal Access Servers</i>
V.92 Modem on Hold feature	<i>V.92 Modem on Hold for Cisco AS5300 and Cisco AS5800 Universal Access Servers</i>

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This feature uses no new or modified commands. To see the command pages for the commands used with this feature, see the Cisco IOS Security Command Reference at

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at

<http://tools.cisco.com/Support/CLILookup> or the Master Command List.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



TACACS+ Attribute-Value Pairs

Terminal Access Controller Access Control System Plus (TACACS+) attribute-value (AV) pairs are used to define specific authentication, authorization, and accounting elements in a user profile that is stored on the TACACS+ daemon. This appendix lists the TACACS+ AV pairs currently supported.

How to Use This Appendix

This appendix is divided into two sections:

-
-

and it specifies the Cisco IOS release in which they are implemented. The second section lists and describes the supported TACACS+ accounting AV pairs, and it specifies the Cisco IOS release in which they are implemented.

TACACS+ Authentication and Authorization AV Pairs

Table 80 lists and describes the supported TACACS+ authentication and authorization AV pairs and specifies the Cisco IOS release in which they are implemented.

Table 80 Supported TACACS+ Authentication and Authorization AV Pairs

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
acl=x	ASCII number representing a connection access list. Used only when service=shell.	yes	yes	yes	yes	yes	yes	yes
addr=x	A network address. Used with service=slip, service=ppp, and protocol=ip. Contains the IP address that the remote host should use when connecting via SLIP or PPP/IP. For example, addr=10.2.3.4.	yes	yes	yes	yes	yes	yes	yes



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Supported TACACS+ Authentication and Authorization AV Pairs (continued)

		yes	yes	yes	yes	yes	yes	yes
	<p>Note that addr-pool works in conjunction with local pooling. It specifies the name of a local pool (which must be preconfigured on the network access server). Use the ip-local pool</p> <pre>ip address-pool local ip local pool boo 10.0.0.1 10.0.0.10 ip local pool moo 10.0.0.1 10.0.0.20</pre> <p>You can then use TACACS+ to return <code>addr-pool=boo</code> or <code>addr-pool=moo</code> to indicate the address pool from which you want to get this remote node's address.</p>							
autocmd=x	Specifies an autocommand to be executed at EXEC startup (for example, <code>autocmd=telnet example.com</code>). Used only with <code>service=shell</code> .	yes	yes	yes	yes	yes	yes	yes
callback-dialstring	Sets the telephone number for a callback (for example: <code>callback-dialstring=408-555-1212</code>). Value is NULL, or a dial-string. A NULL value indicates that the service might choose to get the dial string through other means. Used with <code>service=arap</code> , <code>service=slip</code> , <code>service=ppp</code> , <code>service=shell</code> . Not valid for ISDN.	no	yes	yes	yes	yes	yes	yes
callback-line	The number of a TTY line to use for callback (for example: <code>callback-line=4</code>). Used with <code>service=arap</code> , <code>service=slip</code> , <code>service=ppp</code> , <code>service=shell</code> . Not valid for ISDN.	no	yes	yes	yes	yes	yes	yes
callback-rotary	The number of a rotary group (between 0 and 100 inclusive) to use for callback (for example: <code>callback-rotary=34</code>). Used with <code>service=arap</code> , <code>service=slip</code> , <code>service=ppp</code> , <code>service=shell</code> . Not valid for ISDN.	no	yes	yes	yes	yes	yes	yes
cmd-arg=x	<p>An argument to a shell (EXEC) command. This indicates an argument for the shell command that is to be run. Multiple <code>cmd-arg</code> attributes can be specified, and they are order dependent.</p> <p>Note</p> <p>with RADIUS attribute 26.</p>	yes	yes	yes	yes	yes	yes	yes

		yes	yes	yes	yes	yes	yes	yes
	<p>equals “shell.” A NULL value indicates that the shell itself is being referred to.</p> <p>This TACACS+ AV pair cannot be used with RADIUS attribute 26.</p>							
data-service	Used with the service=outbound and protocol=ip.	no	no	no	no	no	yes	yes
dial-number	Defines the number to dial. Used with the service=outbound and protocol=ip.	no	no	no	no	no	yes	yes
dns-servers=	Identifies a DNS server (primary or secondary) that can be requested by Microsoft PPP clients from the network access server during IPCP negotiation. To be used with service=ppp and protocol=ip. The IP address identifying each DNS server is entered in dotted decimal format.	no	no	no	yes	yes	yes	yes
force-56	Determines whether the network access server uses only the 56 K portion of a channel, even when all 64 K appear to be available. To turn on this attribute, use the “true” value (force-56=true). Any other value is treated as false. Used with the service=outbound and protocol=ip.	no	no	no	no	no	yes	yes
gw-password	Specifies the password for the home gateway during the L2F tunnel authentication. Used with service=ppp and protocol=vpdn.	no	no	yes	yes	yes	yes	yes
idletime=x	Sets a value, in minutes, after which an idle session is terminated. A value of zero indicates no timeout.	no	yes	yes	yes	yes	yes	yes
inac1#<n>	ASCII access list identifier for an input access list to be installed and applied to an interface for the duration of the current connection. Used with service=ppp and protocol=ip, and service service=ppp and protocol=ipx. Per-user access lists do not currently work with ISDN interfaces.	no	no	no	yes	yes	yes	yes
inac1=x	ASCII identifier for an interface input access list. Used with service=ppp and protocol=ip. Per-user access lists do not currently work with ISDN interfaces.	yes	yes	yes	yes	yes	yes	yes

interface-config# <n>	Specifies user-specific AAA interface configuration information with Virtual Profiles. The information that follows the equal sign (=) can be any Cisco IOS interface configuration command. Multiple instances of the attributes are allowed, but each instance must have a unique number. Used with service=ppp and protocol=lcp. This attribute replaces the “interface-config=” attribute.	no	no	no	yes	yes	yes	yes
ip-addresses	Space-separated list of possible IP addresses that can be used for the end-point of a tunnel. Used with service=ppp and protocol=vpdn.	no	no	yes	yes	yes	yes	yes
l2tp-busy-disconnect	If a vpdn-group on an LNS uses a virtual-template that is configured to be pre-cloned, this attribute will control the disposition of a new L2TP session that finds no pre-cloned interface to which to connect. If the attribute is true (the default), the session will be disconnected by the LNS. Otherwise, a new interface will be cloned from the virtual-template. Used with service=ppp and protocol=vpdn.	no	no	no	no	no	yes	yes
l2tp-cm-local-window-size	Specifies the maximum receive window size for L2TP control messages. This value is advertised to the peer during tunnel establishment. Used with service=ppp and protocol=vpdn.	no	no	no	no	no	yes	yes
l2tp-drop-out-of-order	Respects sequence numbers on data packets by dropping those that are received out of order. This does not ensure that sequence numbers will be sent on data packets, just how to handle them if they are received. Used with service=ppp and protocol=vpdn.	no	no	no	no	no	yes	yes
l2tp-hello-interval	Specifies the number of seconds for the hello keepalive interval. Hello packets are sent when no data has been sent on a tunnel for the number of seconds configured here. Used with service=ppp and protocol=vpdn.	no	no	no	no	no	yes	yes
l2tp-hidden-avp	When enabled, sensitive AVPs in L2TP control messages are scrambled or hidden. Used with service=ppp and protocol=vpdn.	no	no	no	no	no	yes	yes
l2tp-nosession-timeout	Specifies the number of seconds that a tunnel will stay active with no sessions before timing out and shutting down. Used with service=ppp and protocol=vpdn.	no	no	no	no	no	yes	yes

l2tp-tos-reflect	Copies the IP ToS field from the IP header of each payload packet to the IP header of the tunnel packet for packets entering the tunnel at the LNS. Used with service=ppp and protocol=vpdn.	no	no	no	no	no	yes	yes
l2tp-tunnel-authen	If this attribute is set, it performs L2TP tunnel authentication. Used with service=ppp and protocol=vpdn.	no	no	no	no	no	yes	yes
l2tp-tunnel-password	Shared secret used for L2TP tunnel authentication and AVP hiding. Used with service=ppp and protocol=vpdn.	no	no	no	no	no	yes	yes
l2tp-udp-checksum	This is an authorization attribute and defines whether L2TP should perform UDP checksums for data packets. Valid values are “yes” and “no.” The default is no. Used with service=ppp and protocol=vpdn.	no	no	no	no	no	yes	yes
link-compression=	Defines whether to turn on or turn off “stac” compression over a PPP link. Used with service=ppp. Link compression is defined as a numeric value as follows: 0: None 1: Stac 2: Stac-Draft-9 3: MS-Stac	no	no	no	yes	yes	yes	yes
load-threshold=<n>	Sets the load threshold for the caller at which additional links are either added to or deleted from the multilink bundle. If the load goes above the specified value, additional links are added. If the load goes below the specified value, links are deleted. Used with service=ppp and protocol=multilink. The range for <n> is from 1 to 255.	no	no	no	yes	yes	yes	yes
map-class	Allows the user profile to reference information configured in a map class of the same name on the network access server that dials out. Used with the service=outbound and protocol=ip.	no	no	no	no	no	yes	yes
max-links=<n>	Restricts the number of links that a user can have in a multilink bundle. Used with service=ppp and protocol=multilink. The range for <n> is from 1 to 255.	no	no	no	yes	yes	yes	yes
min-links	Sets the minimum number of links for MLP. Used with service=ppp and protocol=multilink, protocol=vpdn.	no	no	no	no	no	yes	yes

	compression when sending VJ-compressed packets over a PPP link.	no	no	no	yes	yes	yes	yes
priv-lvl=x	Privilege level to be assigned for the EXEC. Used with service=shell. Privilege levels range from 0 to 15, with 15 being the highest.	yes	yes	yes	yes	yes	yes	yes
protocol=x	A protocol that is a subset of a service. An example would be any PPP NCP. Currently known values are ipx atalk vines lat xremote tn3270 telnet rlogin pad vpdn osicp deccp ccp cdp bridging xns nbf bap multilink unknown							

	<div>route="<i>dst_address mask</i> [<i>gateway</i>]"</div> <div><i>dst_address mask</i> <i>gateway</i></div> <div><i>gateway</i></div>							

	system							
	vpdn outgoing							
		no	no	no	no	no	yes	yes
	ip mobile secure host <addr> configuration command. Basically it contains the rest of the configuration command that follows that string, verbatim. It provides the Security Parameter Index (SPI), key, authentication algorithm, authentication mode, and replay protection timestamp range. Used with the service=mobileip and protocol=ip.							
timeout=x	The number of minutes before an EXEC or ARA session disconnects (for example, timeout=60). A value of zero indicates no timeout. Used with service=arap.	yes	yes	yes	yes	yes	yes	yes
tunnel-id	Specifies the username that will be used to authenticate the tunnel over which the individual user MID will be projected. This is analogous to the <i>remote name</i>							

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2

TACACS+ Accounting AV Pairs

Table 81 *Supported TACACS+ Accounting AV Pairs*

			11.1	11.2	11.3	12.0	12.1	12.2
bytes_in	The number of input bytes transferred during this connection.	yes	yes	yes	yes	yes	yes	yes
bytes_out	The number of output bytes transferred during this connection.	yes	yes	yes	yes	yes	yes	yes
Call-Type	Describes the type of fax activity: fax receive or fax send.	no	no	no	no	no	yes	yes
cmd	The command the user executed.	yes	yes	yes	yes	yes	yes	yes
data-rate	This AV pair has been renamed. See nas-rx-speed.							
disc-cause	Specifies the reason a connection was taken off-line. The Disconnect-Cause attribute is sent in accounting-stop records. This attribute also causes stop records to be generated without first generating start records if disconnection occurs before authentication is performed. Refer to Table 82 for a list of Disconnect-Cause values and their meanings.	no	no	no	yes	yes	yes	yes

disc-cause-ext	Extends the disc-cause attribute to support vendor-specific reasons why a connection was taken off-line.	no	no	no	yes	yes	yes	yes
elapsed_time	The elapsed time in seconds for the action. Useful when the device does not keep real time.	yes	yes	yes	yes	yes	yes	yes
Email-Server-Address	Indicates the IP address of the e-mail server handling the on-ramp fax-mail message.	no	no	no	no	no	yes	yes
Email-Server-Ack-Flag	Indicates that the on-ramp gateway has received a positive acknowledgment from the e-mail server accepting the fax-mail message.	no	no	no	no	no	yes	yes
event	Information included in the accounting packet that describes a state change in the router. Events described are accounting starting and accounting stopping.	yes	yes	yes	yes	yes	yes	yes
Fax-Account-Id-Origin	Indicates the account ID origin as defined by system administrator for the command.	no	no	no	no	no	yes	yes
Fax-Auth-Status	Indicates whether or not authentication for this fax session was successful. Possible values for this field are success, failed, bypassed, or unknown.	no	no	no	no	no	yes	yes
Fax-Connect-Speed	Indicates the modem speed at which this fax-mail was initially transmitted or received. Possible values are 1200, 4800, 9600, and 14400.	no	no	no	no	no	yes	yes
Fax-Coverpage-Flag	Indicates whether or not a cover page was generated by the off-ramp gateway for this fax session. True indicates that a cover page was generated; false means that a cover page was not generated.	no	no	no	no	no	yes	yes
Fax-Dsn-Address	Indicates the address to which DSNs will be sent.	no	no	no	no	no	yes	yes
Fax-Dsn-Flag	Indicates whether or not DSN has been enabled. True indicates that DSN has been enabled; false means that DSN has not been enabled.	no	no	no	no	no	yes	yes
Fax-Mdn-Address	Indicates the address to which MDNs will be sent.	no	no	no	no	no	yes	yes
Fax-Mdn-Flag	Indicates whether or not message delivery notification (MDN) has been enabled. True indicates that MDN had been enabled; false means that MDN had not been enabled.	no	no	no	no	no	yes	yes
Fax-Modem-Time	Indicates the amount of time in seconds the modem sent fax data (x) and the amount of time in seconds of the total fax session (y), which includes both fax-mail and PSTN time, in the form x/y. For example, 10/15 means that the transfer time took 10 seconds, and the total fax session took 15 seconds.	no	no	no	no	no	yes	yes

Fax-Msg-Id=	Indicates a unique fax message identification number assigned by Store and Forward Fax.	no	no	no	no	no	yes	yes
Fax-Pages	Indicates the number of pages transmitted or received during this fax session. This page count includes cover pages.	no	no	no	no	no	yes	yes
Fax-Process-Abort-Flag	Indicates that the fax session was aborted or successful. True means that the session was aborted; false means that the session was successful.	no	no	no	no	no	yes	yes
Fax-Recipient-Count	Indicates the number of recipients for this fax transmission. Until e-mail servers support Session mode, the number should be 1.	no	no	no	no	no	yes	yes
Gateway-Id	Indicates the name of the gateway that processed the fax session. The name appears in the following format: hostname.domain-name	no	no	no	no	no	yes	yes
mlp-links-max	Gives the count of links which are known to have been in a given multilink session at the time the accounting record is generated.	no	no	no	yes	yes	yes	yes
mlp-sess-id	Reports the identification number of the multilink bundle when the session closes. This attribute applies to sessions that are part of a multilink bundle. This attribute is sent in authentication-response packets.	no	no	no	yes	yes	yes	yes
nas-rx-speed	Specifies the average number of bits per second over the course of the connection's lifetime. This attribute is sent in accounting-stop records.	no	no	no	yes	yes	yes	yes
nas-tx-speed	Reports the transmit speed negotiated by the two modems.	no	no	no	yes	yes	yes	yes
paks_in	The number of input packets transferred during this connection.	yes	yes	yes	yes	yes	yes	yes
paks_out	The number of output packets transferred during this connection.	yes	yes	yes	yes	yes	yes	yes
port	The port the user was logged in to.	yes	yes	yes	yes	yes	yes	yes
Port-Used	Indicates the slot/port number of the Cisco AS5300 used to either transmit or receive this fax-mail.	no	no	no	no	no	yes	yes
pre-bytes-in	Records the number of input bytes before authentication. This attribute is sent in accounting-stop records.	no	no	no	yes	yes	yes	yes
pre-bytes-out	Records the number of output bytes before authentication. This attribute is sent in accounting-stop records.	no	no	no	yes	yes	yes	yes
pre-paks-in	Records the number of input packets before authentication. This attribute is sent in accounting-stop records.	no	no	no	yes	yes	yes	yes

Table 81 **Supported TACACS+ Accounting AV Pairs (continued)**

	epoch, 12:00 a.m. Jan 1 1970). The clock must be configured to receive this information.	yes	yes	yes	yes	yes	yes	yes
stop_time	The time the action stopped (in seconds since the epoch.) The clock must be configured to receive this information.	yes	yes	yes	yes	yes	yes	yes
task_id	Start and stop records for the same event must have matching (unique) task_id numbers.	yes	yes	yes	yes	yes	yes	yes
timezone	The time zone abbreviation for all timestamps included in this packet.	yes	yes	yes	yes	yes	yes	yes
xmit-rate	This AV pair has been renamed. See nas-tx-speed.							

Table 82 lists the cause codes and descriptions for the Disconnect Cause Extended (disc-cause-ext) attribute.

Table 82 **Disconnect Cause Extensions**

Cause Codes	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
1000 – No Reason	No reason for the disconnect.	no	no	no	no	yes	yes	yes	yes
1001 – No Disconnect	The event was not a disconnect.	no	no	no	no	yes	yes	yes	yes
1002 – Unknown	The reason for the disconnect is unknown. This code can appear when the remote connection goes down.	no	no	no	no	yes	yes	yes	yes
1003 – Call Disconnect	The call has disconnected.	no	no	no	no	yes	yes	yes	yes
1004 – CLID Auth Fail	Calling line ID (CLID) authentication has failed.	no	no	no	no	yes	yes	yes	yes

Cause Codes	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
1009 – No Modem Available	The modem is not available.	no	no	no	no	yes	yes	yes	yes
1010 – No Carrier	The modem never detected data carrier detect (DCD). This code can appear if a disconnect occurs during the initial modem connection.	no	no	no	no	yes	yes	yes	yes
1011 – Lost Carrier	The modem detected DCD but became inactive. This code can appear if a disconnect occurs during the initial modem connection.	no	no	no	no	yes	yes	yes	yes
1012 – No Modem Results	The result codes could not be parsed. This code can appear if a disconnect occurs during the initial modem connection.	no	no	no	no	yes	yes	yes	yes
1020 – TS User Exit	The user exited normally from the terminal server. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	no	no	no	no	yes	yes	yes	yes
1021 – Idle Timeout	The user exited from the terminal server because the idle timer expired. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	no	no	no	no	yes	yes	yes	yes
1022 – TS Exit Telnet	The user exited normally from a Telnet session. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	no	no	no	no	yes	yes	yes	yes
1023 – TS No IP Addr	The user could not switch to Serial Line Internet Protocol (SLIP) or PPP because the remote host had no IP address or because the dynamic pool could not assign one. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	no	no	no	no	yes	yes	yes	yes
1024 – TS TCP Raw Exit	The user exited normally from a raw TCP session. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	no	no	no	no	yes	yes	yes	yes
1025 – TS Bad Password	The login process ended because the user failed to enter a correct password after three attempts. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	no	no	no	no	yes	yes	yes	yes
1026 – TS No TCP Raw	The raw TCP option is not enabled. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	no	no	no	no	yes	yes	yes	yes
1027 – TS CNTL-C	The login process ended because the user typed Ctrl-C. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	no	no	no	no	yes	yes	yes	yes
1028 – TS Session End	The terminal server session has ended. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	no	no	no	no	yes	yes	yes	yes

Cause Codes	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
1029 – TS Close Vconn	The user closed the virtual connection. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	no	no	no	no	yes	yes	yes	yes
1030 – TS End Vconn	The virtual connection has ended. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	no	no	no	no	yes	yes	yes	yes
1031 – TS Rlogin Exit	The user exited normally from an Rlogin session. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	no	no	no	no	yes	yes	yes	yes
1032 – TS Rlogin Opt Invalid	The user selected an invalid Rlogin option. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	no	no	no	no	yes	yes	yes	yes
1033 – TS Insuff Resources	The access server has insufficient resources for the terminal server session. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.	no	no	no	no	yes	yes	yes	yes
1040 – PPP LCP Timeout	PPP link control protocol (LCP) negotiation timed out while waiting for a response from a peer. This code concerns PPP connections.	no	no	no	no	yes	yes	yes	yes
1041 – PPP LCP Fail	There was a failure to converge on PPP LCP negotiations. This code concerns PPP connections.	no	no	no	no	yes	yes	yes	yes
1042 – PPP Pap Fail	PPP Password Authentication Protocol (PAP) authentication failed. This code concerns PPP connections.	no	no	no	no	yes	yes	yes	yes
1043 – PPP CHAP Fail	PPP Challenge Handshake Authentication Protocol (CHAP) authentication failed. This code concerns PPP connections.	no	no	no	no	yes	yes	yes	yes
1044 – PPP Remote Fail	Authentication failed from the remote server. This code concerns PPP sessions.	no	no	no	no	yes	yes	yes	yes
1045 – PPP Receive Term	The peer sent a PPP termination request. This code concerns PPP connections.	no	no	no	no	yes	yes	yes	yes
PPP LCP Close (1046)	LCP got a close request from the upper layer while LCP was in an open state. This code concerns PPP connections.	no	no	no	no	yes	yes	yes	yes
1047 – PPP No NCP	LCP closed because no NCPs were open. This code concerns PPP connections.	no	no	no	no	yes	yes	yes	yes
1048 – PPP MP Error	LCP closed because it could not determine to which Multilink PPP bundle that it should add the user. This code concerns PPP connections.	no	no	no	no	yes	yes	yes	yes
1049 – PPP Max Channels	LCP closed because the access server could not add any more channels to an MP session. This code concerns PPP connections.	no	no	no	no	yes	yes	yes	yes

Cause Codes	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
1050 – TS Tables Full	The raw TCP or Telnet internal session tables are full. This code relates to immediate Telnet and raw TCP disconnects and contains more specific information than the Telnet and TCP codes listed earlier in this table.	no	no	no	no	yes	yes	yes	yes
1051 – TS Resource Full	Internal resources are full. This code relates to immediate Telnet and raw TCP disconnects and contains more specific information than the Telnet and TCP codes listed earlier in this table.	no	no	no	no	yes	yes	yes	yes
1052 – TS Invalid IP Addr	The IP address for the Telnet host is invalid. This code relates to immediate Telnet and raw TCP disconnects and contains more specific information than the Telnet and TCP codes listed earlier in this table.	no	no	no	no	yes	yes	yes	yes
1053 – TS Bad Hostname	The access server could not resolve the host name. This code relates to immediate Telnet and raw TCP disconnects and contains more specific information than the Telnet and TCP codes listed earlier in this table.	no	no	no	no	yes	yes	yes	yes
1054 – TS Bad Port	The access server detected a bad or missing port number. This code relates to immediate Telnet and raw TCP disconnects and contains more specific information than the Telnet and TCP codes listed earlier in this table.	no	no	no	no	yes	yes	yes	yes
1060 – TCP Reset	The host reset the TCP connection. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.	no	no	no	no	yes	yes	yes	yes
1061 – TCP Connection Refused	The host refused the TCP connection. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.	no	no	no	no	yes	yes	yes	yes
1062 – TCP Timeout	The TCP connection timed out. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.	no	no	no	no	yes	yes	yes	yes
1063 – TCP Foreign Host Close	A foreign host closed the TCP connection. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.	no	no	no	no	yes	yes	yes	yes
1064 – TCP Net Unreachable	The TCP network was unreachable. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.	no	no	no	no	yes	yes	yes	yes
1065 – TCP Host Unreachable	The TCP host was unreachable. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.	no	no	no	no	yes	yes	yes	yes
1066 – TCP Net Admin Unreachable	The TCP network was administratively unreachable. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.	no	no	no	no	yes	yes	yes	yes

1067 – TCP Host Admin Unreachable	The TCP host was administratively unreachable. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.	no	no	no	no	yes	yes	yes	yes
1068 – TCP Port Unreachable	The TCP port was unreachable. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.	no	no	no	no	yes	yes	yes	yes
1100 – Session Timeout	The session timed out because there was no activity on a PPP link. This code applies to all session types.	no	no	no	no	yes	yes	yes	yes
1101 – Security Fail	The session failed for security reasons. This code applies to all session types.	no	no	no	no	yes	yes	yes	yes
1102 – Callback	The session ended for callback. This code applies to all session types.	no	no	no	no	yes	yes	yes	yes
1120 – Unsupported	One end refused the call because the protocol was disabled or unsupported. This code applies to all session types.	no	no	no	no	yes	yes	yes	yes
1150 – Radius Disc	The RADIUS server requested the disconnect.	no	no	no	no	yes	yes	yes	yes
1151 – Local Admin Disc	The local administrator has disconnected.	no	no	no	no	yes	yes	yes	yes
1152 – SNMP Disc	Simple Network Management Protocol (SNMP) has disconnected.	no	no	no	no	yes	yes	yes	yes
1160 – V110 Retries	The allowed retries for V110 synchronization have been exceeded.	no	no	no	no	yes	yes	yes	yes
1170 – PPP Auth Timeout	Authentication timeout. This code applies to PPP sessions.	no	no	no	no	yes	yes	yes	yes
1180 – Local Hangup	The call disconnected as the result of a local hangup.	no	no	no	no	yes	yes	yes	yes
1185 – Remote Hangup	The call disconnected because the remote end hung up.	no	no	no	no	yes	yes	yes	yes
1190 – T1 Quiesced	The call disconnected because the T1 line that carried it was quiesced.	no	no	no	no	yes	yes	yes	yes
1195 – Call Duration	The call disconnected because the call duration exceeded the maximum amount of time allowed by the Max Call Mins or Max DS0 Mins parameter on the access server.	no	no	no	no	yes	yes	yes	yes
1600 – VPDN User Disconnect	The user disconnected. This value applies to virtual private dial-up network (VPDN) sessions.	no	no	no	no	no	no	yes	yes
1601 – VPDN Carrier Loss	Carrier loss has occurred. This code applies to VPDN sessions.	no	no	no	no	no	no	yes	yes
1602 – VPDN No Resources	There are no resources. This code applies to VPDN sessions.	no	no	no	no	no	no	yes	yes
1603 – VPDN Bad Control Packet	The control packet is invalid. This code applies to VPDN sessions.	no	no	no	no	no	no	yes	yes

1604 – VPDN Admin Disconnect	The administrator disconnected. This code applies to VPDN sessions.	no	no	no	no	no	no	yes	yes
1605 – VPDN Tunnel Down/Setup Fail	The tunnel is down or the setup failed. This code applies to VPDN sessions.	no	no	no	no	no	no	yes	yes
1606 – VPDN Local PPP Disconnect	There was a local PPP disconnect. This code applies to VPDN sessions.	no	no	no	no	no	no	yes	yes
1607 – VPDN Softshut/Session Limit	New sessions cannot be established on the VPN tunnel. This code applies to VPDN sessions.	no	no	no	no	no	no	yes	yes
1608 – VPDN Call Redirected	The call was redirected. This code applies to VPDN sessions.	no	no	no	no	no	no	yes	yes
1801 – Q850 Unassigned Number	The number has not been assigned. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
1802 – Q850 No Route	The equipment that is sending this code has received a request to route the call through a particular transit network that it does not recognize. The equipment that is sending this code does not recognize the transit network because either the transit network does not exist or because that particular transit network, while it does exist, does not serve the equipment that is sending this code. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
1803 – Q850 No Route To Destination	The called party cannot be reached because the network through which the call has been routed does not serve the destination that is desired. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
1806 – Q850 Channel Unacceptable	The channel that has been most recently identified is not acceptable to the sending entity for use in this call. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
1816 – Q850 Normal Clearing	The call is being cleared because one of the users who is involved in the call has requested that the call be cleared. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
1817 – Q850 User Busy	The called party is unable to accept another call because the user-busy condition has been encountered. This code may be generated by the called user or by the network. In the case of the user, the user equipment is compatible with the call. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes

1818 – Q850 No User Responding	Used when a called party does not respond to a call-establishment message with either an alerting or connect indication within the prescribed period of time that was allocated. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
1819 – Q850 No User Answer	The called party has been alerted but does not respond with a connect indication within a prescribed period of time. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
1821 – Q850 Call Rejected	The equipment that is sending this code does not wish to accept this call although it could have accepted the call because the equipment that is sending this code is neither busy nor incompatible. This code may also be generated by the network, indicating that the call was cleared due to a supplementary service constraint. The diagnostic field may contain additional information about the supplementary service and reason for rejection. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
1822 – Q850 Number Changed	The number that is indicated for the called party is no longer assigned. The new called party number may optionally be included in the diagnostic field. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
1827 – Q850 Destination Out of Order	The destination that was indicated by the user cannot be reached because the interface to the destination is not functioning correctly. The term “not functioning correctly” indicates that a signaling message was unable to be delivered to the remote party. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
1828 – Q850 Invalid Number Format	The called party cannot be reached because the called party number is not in a valid format or is not complete. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
1829 – Q850 Facility Rejected	This code is returned when a supplementary service that was requested by the user cannot be provided by the network. This code applies to ISDN or modem calls that have come in over ISDN.	no	no	no	no	no	no	no	yes
1830 – Q850 Responding to Status Enquiry	This code is included in the STATUS message when the reason for generating the STATUS message was the prior receipt of a STATUS ENQUIRY message. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
1831 – Q850 Unspecified Cause	No other code applies. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes

1834 – Q850 No Circuit Available	No circuit or channel is available to handle the call. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
1838 – Q850 Network Out of Order	The network is not functioning correctly and the condition is likely to last a relatively long period of time. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
1841 – Q850 Temporary Failure	The network is not functioning correctly and the condition is not likely to last a long period of time. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
1842 – Q850 Network Congestion	The network is congested. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
1843 – Q850 Access Info Discarded	This code indicates that the network could not deliver access information to the remote user as requested. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
1844 – Q850 Requested Channel Not Available	This code is returned when the circuit or channel that is indicated by the requesting entity cannot be provided by the other side of the interface. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
1845 – Q850 Call Pre-empted	The call was preempted. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
1847 – Q850 Resource Unavailable	This code is used to report a resource-unavailable event only when no other code in the resource-unavailable class applies. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
1850 – Q850 Facility Not Subscribed	Not a subscribed facility. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
1852 – Q850 Outgoing Call Barred	Although the calling party is a member of the closed user group for the outgoing closed user group call, outgoing calls are not allowed for this member. This code applies to ISDN or modem calls that came in over ISDN.	no	no	no	no	no	no	no	yes
Q850 Incoming Call Barred (1854)	Although the called party is a member of the closed user group for the incoming closed user group call, incoming calls are not allowed to this member. This code applies to ISDN or modem calls that have come in over ISDN.	no	no	no	no	no	no	no	yes
1858 – Q850 Bearer Capability Not Available	The user has requested a bearer capability that is implemented by the equipment that generated this code but that is not available at this time. This code applies to ISDN or modem calls that have come in over ISDN.	no	no	no	no	no	no	no	yes

1863 – Q850 Service Not Available	The code is used to report a service- or option-not-available event only when no other code in the service- or option-not-available class applies. This code applies to ISDN or modem calls that have come in over ISDN.	no	no	no	no	no	no	no	yes
1865 – Q850 Bearer Capability Not Implemented	The equipment that is sending this code does not support the bearer capability that was requested. This code applies to ISDN or modem calls that have come in over ISDN.	no	no	no	no	no	no	no	yes
1866 – Q850 Channel Not Implemented	The equipment that is sending this code does not support the channel type that was requested. This code applies to ISDN or modem calls that have come in over ISDN.	no	no	no	no	no	no	no	yes
1869 – Q850 Facility Not Implemented	The supplementary service requested by the user cannot be provided by the network. This code applies to ISDN or modem calls that have come in over ISDN.	no	no	no	no	no	no	no	yes
1881 – Q850 Invalid Call Reference	The equipment that is sending this code has received a message having a call reference that is not currently in use on the user-network interface. This code applies to ISDN or modem calls that have come in over ISDN.	no	no	no	no	no	no	no	yes
1882 – Q850 Channel Does Not Exist	The channel most recently identified is not acceptable to the sending entity for use in this call. This code applies to ISDN or modem calls that have come in over ISDN. This code applies to ISDN or modem calls that have come in over ISDN.	no	no	no	no	no	no	no	yes
1888 – Q850 Incompatible Destination	The equipment that is sending this code has received a request to establish a call that has low-layer compatibility or other compatibility attributes that cannot be accommodated. This code applies to ISDN or modem calls that have come in over ISDN.	no	no	no	no	no	no	no	yes
1896 – Q850 Mandatory Info Element Is Missing	The equipment that is sending this code has received a message that is missing an information element that must be present in the message before that message can be processed. This code applies to ISDN or modem calls that have come in over ISDN.	no	no	no	no	no	no	no	yes
1897 – Q850 Non Existent Message Type	The equipment that is sending this code has received a message with a message type that it does not recognize either because this is a message that is not defined or that is defined but not implemented by the equipment that is sending this code. This code applies to ISDN or modem calls that have come in over ISDN.	no	no	no	no	no	no	no	yes



“

”

.



Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





Flexible Packet Matching

First Published: October 31, 2006

Last Updated: August 7, 2008

Flexible Packet Matching (FPM) is the next generation access control list (ACL) pattern matching tool, providing more thorough and customized packet filters. FPM enables users to match on arbitrary bits of a packet at an arbitrary depth in the packet header and payload. FPM removes constraints to specific fields that had limited packet inspection.

FPM is useful because it enables users to create their own stateless packet classification criteria and to define policies with multiple actions (such as drop, log, or send Internet Control Message Protocol [ICMP] unreachable¹) to immediately block new viruses, worms, and attacks.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Flexible Packet Matching” section on page 15](#).

Use Cisco Feature Navigator to find information about platform support and Cisco IOS, Catalyst OS, and Cisco IOS XE software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required

Contents

- [Prerequisites for Flexible Packet Matching, page 2](#)
- [Restrictions for Flexible Packet Matching, page 2](#)
- [Information About Flexible Packet Matching, page 2](#)
- [How to Configure a Flexible Packet Matching Traffic Class and Traffic Policy, page 5](#)
- [Configuration Examples for FPM Configuration, page 9](#)

1. Send ICMP unreachable is currently not supported on the Supervisor Engine 32 PISA.



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007, 2008 Cisco Systems, Inc. All rights reserved.

- [Additional References, page 13](#)
- [Command Reference, page 14](#)
- [Feature Information for Flexible Packet Matching, page 15](#)

Prerequisites for Flexible Packet Matching

- In Cisco IOS Release 12.4(4)T, FPM is available only in advanced security images.
- In Cisco IOS Release 12.2(18)ZY, FPM is also available in ipbase and ipservices images for the Supervisor Engine 32 Programmable Intelligent Services Accelerator (PISA) platform.
- Although access to an XML editor is not required, XML will ease the creation of protocol header description files (PHDFs).

Restrictions for Flexible Packet Matching

- FPM cannot be used to mitigate an attack that requires stateful classification.
- Because FPM is stateless, it cannot keep track of port numbers being used by protocols that dynamically negotiate ports. Thus, when using FPM, port numbers must be explicitly specified.
- FPM cannot perform IP fragmentation or TCP flow reassembly.
- FPM inspects only IPv4 unicast packets.
- FPM cannot classify packets with IP options.
- FPM does not support multicast packet inspection.
- FPM is not supported on tunnel and MPLS interfaces.
- FPM cannot be configured on FlexWAN cards.
- Noninitial fragments will not be matched by the FPM engine.
- Offset can be only a constant in a match start construct.
- FPM cannot match across packets.
- Mapping of FPM policies to control-plane is not supported.

Information About Flexible Packet Matching

Before configuring FPM, you should understand the following concept:

- [Flexible Packet Matching Functional Overview, page 3](#)
- [Traffic Classification Definition Files \(TCDFs\) for the Flexible Packet Matching XML Configuration, page 4](#)
- [FPM on PISA Overview, page 4](#)

Flexible Packet Matching Functional Overview

FPM allows customers to create their own filtering policies that can immediately detect and block new viruses and attacks.

A filtering policy is defined via the following tasks:

- Load a PHDF (for protocol header field matching)
- Define a class map and define the protocol stack chain (traffic class)
- Define a service policy (traffic policy)
- Apply the service policy to an interface

Protocol Header Description File

Protocol headers are defined in separate files called PHDFs; the field names that are defined within the PHDFs are used for defining the packet filters. A PHDF is a file that allows the user to leverage the flexibility of XML to describe almost any protocol header. The important components of the PHDF are the version, the XML file schema location, and the protocol field definitions. The protocol field definitions name the appropriate field in the protocol header, allow for a comment describing the field, provide the location of the protocol header field in the header (the offset is relative to the start of the protocol header), and provide the length of the field. Users can choose to specify the measurement in bytes or in bits.

**Note**

The total length of the header must be specified at the end of each PHDF.

Users can write their own custom PHDFs via XML for existing or proprietary protocols. However, the following standard PHDFs can also be loaded onto the router via the **load protocol** command: ip.phdf, ether.phdf, tcp.phdf, and udp.phdf.

**Note**

Because PHDFs are defined via XML, they are not shown in a running configuration. However, you can use the **show protocol phdf** command to verify the loaded PHDF.

Standard PHDFs are available on Cisco.com at the following URL:
<http://www.cisco.com/cgi-bin/tablebuild.pl/fpm>

Filter Description

A filter description is a definition of a traffic class that can contain the header fields defined in a PHDF (using the **match field** command). If a PHDF is not loaded, the traffic class can be defined via the datagram header start (Layer 2) or the network header start (Layer 3) (using the **match start** command). If a PHDF has been loaded onto the router, the class specification begins with a list of the protocol headers in the packet.

A filter definition also includes the policy map; that is, after a class map has been defined, a policy map is needed to bind the match to an action. A policy map is an ordered set of classes and associated actions, such as drop, log, or send ICMP unreachable.

For information on how to configure a class map and a policy map for FPM, see the following section “[How to Configure a Flexible Packet Matching Traffic Class and Traffic Policy](#).”

Traffic Classification Definition Files (TCDFs) for the Flexible Packet Matching XML Configuration

FPM uses a traffic classification definition file (TCDF) to define policies that can block attacks on the network. Before Cisco IOS Release 12.4(6)T, FPM defined traffic classes (class maps), policies (policy maps), and service policies (attach policy maps to class maps) through the use of CLI commands. With TCDFs, FPM can use XML as an alternative to the CLI to define classes of traffic and specify actions to apply to the traffic classes. Traffic classification behavior is the same whether you create the behavior using a TCDF or configure it using CLI commands. Once a TCDF is created, it can be loaded on any FPM-enabled device in the network.

For more information on configuring FPM using TCDFs, see [Flexible Packet Matching XML Configuration](#).

FPM on PISA Overview

The PISA functions as a network-processor based daughter card that is mounted on the Catalyst 6500 Supervisor. PISA provides a superset of the multilayer switch feature card 2a (MSFC2a) capabilities. In addition to performing all of the same functions as the MSFC2a, PISA also provides a dedicated hardware to accelerate certain features, such as FPM.

FPM occurs before Network-Based Application Recognition (NBAR); thus, packets that are dropped by FPM are not processed by NBAR.

Logging FPM Activity

In software-based FPM logging, every flow is logged and aggregated statistics are provided for each flow. Logging every flow for FPM on PISA would overwhelm the CPU; thus, only selective packets are logged. That is, when a packet matches a policy that is to be logged or the first time, the packet is logged, time-stamped, and stored. For every subsequent packet that matches any policy with a log action, the packet is checked for the difference between the current time (which is clocked by the global timer) and the last time stamp. If the current time is greater than the last time stamp, the packet is logged and the “stamp time” is updated with the current time.

Memory Requirements



Note

Because memory requirements vary among system configurations, the requirements listed in this document are estimates.

- PISA will support a maximum of 1024 interfaces; however, it is expected that no more than 256 interfaces will be configured with FPM.
- A maximum of 32 classes per policy map, and a total of 1024 classes globally, are supported.
- A maximum of 32 filters (such as match entries) per class map are supported. (However, some optimizations for better performance are possible with match-any type of class maps that have filters starting at same the same offset and the same size.)

How to Configure a Flexible Packet Matching Traffic Class and Traffic Policy

This section contains the following procedures that should be followed when configuring a FPM traffic class and traffic policy within your network:

- [Creating a Traffic Class for Flexible Packet Matching, page 5](#)
- [Creating a Traffic Policy for Flexible Packet Matching, page 7](#)

Creating a Traffic Class for Flexible Packet Matching

Perform this task to create an FPM traffic class; that is, create a stateless packet classification criteria that, when used in conjunction with an appropriately defined policy, can mitigate network attacks.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **load protocol** *location:filename*
4. **class-map** [**type** {**stack** | **access-control**}] *class-map-name* [**match-all** | **match-any**]
5. **description** *character-string*
6. **match field** *protocol protocol-field* {**eq** [*mask*] | **neq** [*mask*] | **gt** | **lt** | **range** *range* | **regex** *string*} *value* [**next** *next-protocol*]
7. **match start** {**l2-start** | **l3-start**} **offset** *number* **size** *number* {**eq** | **neq** | **gt** | **lt** | **range** *range* | **regex** *string*} *value* [*value2*]
8. **exit**
9. **show class-map** [**type** {**stack** | **access-control**}] [*class-map-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	load protocol <i>location:filename</i> Example: Router(config)# load protocol disk2:udp.phdf	(Optional) Loads a PHDF onto a router. <ul style="list-style-type: none">• The specified location must be local to the router. Note If a PHDF is not loaded, only the match start command can be used; that is, you cannot issue the match field command.

	Command or Action	Purpose
Step 4	class-map [type { stack access-control }] <i>class-map-name</i> [match-all match-any] Example: Router(config)# class-map type access-control slammer match-all	Creates a class map to be used for matching packets to a specified class and enters class-map configuration mode. <ul style="list-style-type: none"> • type stack —Enables FPM to determine the correct protocol stack in which to examine. • type access-control—Determines the exact pattern to look for in the protocol stack of interest. • <i>class-map-name</i>—Can be a maximum of 40 alphanumeric characters. • If match-all or match-any are not specified, traffic must match all the match criterion to be classified as part of the traffic class.
Step 5	description <i>character-string</i> Example: Router(config-cmap)# description "match on slammer packets"	(Optional) Adds a description to the class map.
Step 6	match field <i>protocol protocol-field</i> { eq [<i>mask</i>] neq [<i>mask</i>] gt lt range <i>range</i> regex <i>string</i> } <i>value</i> [next <i>next-protocol</i>] Example: Router(config-cmap)# match field udp dest-port eq 0x59A	(Optional) Configures the match criteria for a class map on the basis of the fields defined in the PHDFs.
Step 7	match start { l2-start l3-start } offset <i>number</i> size <i>number</i> { eq neq gt lt range <i>range</i> regex <i>string</i> } <i>value</i> [<i>value2</i>] Example: Router(config-cmap)# match start l3-start offset 224 size 4 eq 0x4011010	(Optional) Configures the match criteria for a class map on the basis of the datagram header (Layer 2) or the network header (Layer 3).
Step 8	exit Example: Router(config-cmap)# exit Example: Router(config)# exit	Exits class-map configuration mode and global configuration mode.
Step 9	show class-map [type { stack access-control }] [<i>class-map-name</i>] Example: Router# show class-map type access-control slammer	(Optional) Displays all configured FPM class maps.

Troubleshooting Tips

To track all FPM events, issue the **debug fpm event** command.

The following sample output is from the **debug fpm event** command:

```
*Jun 21 09:22:21.607: policy-classification-inline(): matches class: class-default *Jun 21
09:22:21.607: packet-access-control(): policy-map: fpm-policy, dir: input, match. retval:
0x0, ip-flags: 0x80000000
```

What to Do Next

After you have defined at least one class map for your network, you must create a traffic policy and apply that policy to an interface as shown in the following task “[Creating a Traffic Policy for Flexible Packet Matching](#).”

Creating a Traffic Policy for Flexible Packet Matching

Perform this task to create an FPM traffic policy and apply the policy to a given interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** [type access-control] *policy-map-name*
4. **description** *character-string*
5. **class** *class-name* [insert-before *class-name*]
6. **drop**
7. **service-policy** *policy-map-name*
8. **exit**
9. **interface** *type name*
10. **service-policy** [type access-control] { **input** | **output** } *policy-map-name*
11. **exit**
12. **show policy-map interface** [type access-control] *interface-name* [**input** | **output**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
	Example: Router> enable	
Step 2	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	

	Command or Action	Purpose
Step 3	policy-map [type access-control] <i>policy-map-name</i> Example: Router(config)# policy-map type access-control fpm-udp-policy	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy and enters policy-map configuration mode.
Step 4	description <i>character-string</i> Example: Router(config-pmap)# description "policy for UDP based attacks"	(Optional) Adds a description to the policy map.
Step 5	class <i>class-name</i> [insert-before <i>class-name</i>] Example: Router(config-pmap)# class slammer	Specifies the name of a predefined traffic class, which was configured with the class-map command, used to classify traffic to the traffic policy. <ul style="list-style-type: none"> insert-before class-name—Adds a class map to any location within the policy map. If this option is not issued, the class map is appended to the end of the policy map.
Step 6	drop Example: Router(config-pmap)# drop	(Optional) Configures a traffic class to discard packets belonging to a specific class. If this command is issued, note the following restrictions: <ul style="list-style-type: none"> Discarding packets is the only action that can be configured in a traffic class. When a traffic class is configured with the drop command, a “child” (nested) policy cannot be configured for this specific traffic class through the service policy command. Discarding packets cannot be configured for the default class specified via the class class-default command.
Step 7	service-policy <i>policy-map-name</i> Example: Router(config-pmap-c)# service policy fpm-udp-policy	Creates hierarchical service policies.
Step 8	exit Example: Router(config-pmap-c)# exit Example: Router(config-pmap)# exit	Exits policy-map class configuration mode and policy-map configuration mode.
Step 9	interface <i>type number</i> Example: Router(config)# interface gigabitEthernet 0/1	Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 10	service-policy [type access-control] { input output } <i>policy-map-name</i> Example: Router(config-if)# service-policy type access-control input fpm-policy	Specifies the type and the name of the traffic policy to be attached to the input or output direction of an interface.
Step 11	exit Example: Router(config-if)# exit Example: Router(config)# exit	Exits interface configuration and global configuration modes.
Step 12	show policy-map interface [type access-control] <i>interface-name</i> [input output] Example: Router# show policy-map interface type access-control interface gigabit 0/1	(Optional) Verifies the FPM configuration.

Configuration Examples for FPM Configuration

This section contains the following configuration examples:

- [Configuring FPM for Slammer Packets: Example, page 9](#)
- [Configuring FPM for Blaster Packets: Example, page 11](#)
- [Configuring FPM for MyDoom Packets: Example, page 12](#)

Configuring FPM for Slammer Packets: Example

The following example shows how to define FPM traffic classes for slammer packets (UDP port 1434). The match criteria defined within the class maps is for slammer packets with an IP length not to exceed 404 bytes, UDP port 1434, and pattern 0x4011010 at 224 bytes from start of IP header. This example also shows how to define the service policy “fpm-policy” and apply it to the Gigabit Ethernet interface. Show commands have been issued to verify the FPM configuration. (Note that PHDFs are not displayed in show output because they are in XML format.)

```
Router(config)# load protocol disk2:ip.phdf
Router(config)# load protocol disk2:udp.phdf

Router(config)# class-map type stack match-all ip-udp
Router(config-cmap)# description "match UDP over IP packets"
Router(config-cmap)# match field ip protocol eq 0x11 next udp

Router(config)# class-map type access-control match-all slammer
Router(config-cmap)# description "match on slammer packets"
Router(config-cmap)# match field udp dest-port eq 0x59A
Router(config-cmap)# match field ip length eq 0x194
Router(config-cmap)# match start 13-start offset 224 size 4 eq 0x4011010
```

```

Router(config)# policy-map type access-control fpm-udp-policy
Router(config-pmap)# description "policy for UDP based attacks"
Router(config-pmap)# class slammer
Router(config-pmap-c)# drop

Router(config)# policy-map type access-control fpm-policy
Router(config-pmap)# description "drop worms and malicious attacks"
Router(config-pmap)# class ip-udp
Router(config-pmap-c)# service-policy fpm-udp-policy

Router(config)# interface gigabitEthernet 0/1
Router(config-if)# service-policy type access-control input fpm-policy

Router# show policy-map type access-control interface gigabit 0/1

GigabitEthernet0/1
Service-policy access-control input: fpm-policy
Class-map: ip-udp (match-all)
0 packets, 0 bytes
3 minute offered rate 0 bps
Match: field IP protocol eq 0x11 next UDP
Service-policy access-control : fpm-udp-policy
Class-map: slammer (match-all)
0 packets, 0 bytes
3 minute offered rate 0 bps, drop rate 0 bps
Match: field UDP dest-port eq 0x59A
Match: field IP length eq 0x194
Match: start 13-start offset 224 size 4 eq 0x4011010
drop
Class-map: class-default (match-any)
0 packets, 0 bytes
3 minute offered rate 0 bps, drop rate 0 bps
Match: any
Class-map: class-default (match-any)
0 packets, 0 bytes
3 minute offered rate 0 bps, drop rate 0 bps
Match: any

Router# show protocol phdf ip

Protocol ID: 1
Protocol name: IP
Description: Definition-for-the-IP-protocol
Original file name: disk2:ip.phdf
Header length: 20
Constraint(s):
Total number of fields: 12
Field id: 0, version, IP-version
Fixed offset. offset 0
Constant length. Length: 4
Field id: 1, ihl, IP-Header-Length
Fixed offset. offset 4
Constant length. Length: 4
Field id: 2, tos, IP-Type-of-Service
Fixed offset. offset 8
Constant length. Length: 8
Field id: 3, length, IP-Total-Length
Fixed offset. offset 16
Constant length. Length: 16
Field id: 4, identification, IP-Identification

```

```

Fixed offset. offset 32
Constant length. Length: 16
Field id: 5, flags, IP-Fragmentation-Flags
Fixed offset. offset 48
Constant length. Length: 3
Field id: 6, fragment-offset, IP-Fragmentation-Offset
Fixed offset. offset 51
Constant length. Length: 13
Field id: 7, ttl, Definition-for-the-IP-TTL
Fixed offset. offset 64
Constant length. Length: 8
Field id: 8, protocol, IP-Protocol
Fixed offset. offset 72
Constant length. Length: 8
Field id: 9, checksum, IP-Header-Checksum
Fixed offset. offset 80
Constant length. Length: 16
Field id: 10, source-addr, IP-Source-Address
Fixed offset. offset 96
Constant length. Length: 32
Field id: 11, dest-addr, IP-Destination-Address
Fixed offset. offset 128
Constant length. Length: 32

```

```
Router# show protocol phdf udp
```

```

Protocol ID: 3
Protocol name: UDP
Description: UDP-Protocol
Original file name: disk2:udp.phdf
Header length: 8
Constraint(s):
Total number of fields: 4
Field id: 0, source-port, UDP-Source-Port
Fixed offset. offset 0
Constant length. Length: 16
Field id: 1, dest-port, UDP-Destination-Port
Fixed offset. offset 16
Constant length. Length: 16
Field id: 2, length, UDP-Length
Fixed offset. offset 32
Constant length. Length: 16
Field id: 3, checksum, UDP-Checksum
Fixed offset. offset 48
Constant length. Length: 16

```

Configuring FPM for Blaster Packets: Example

The following example shows how to configure FPM for blaster packets. The class map contains the following match criteria: TCP port 135, 4444 or UDP port 69; and pattern 0x0030 at 3 bytes from start of IP header.

```

Router(config)# load protocol disk2:ip.phdf
Router(config)# load protocol disk2:tcp.phdf
Router(config)# load protocol disk2:udp.phdf

Router(config)# class-map type stack match-all ip-tcp
Router(config-cmap)# match field ip protocol eq 0x6 next tcp

Router(config)# class-map type stack match-all ip-udp
Router(config-cmap)# match field ip protocol eq 0x11 next udp

```



```

Router(config)# class-map type access-control match-all blaster1
Router(config-cmap)# match field tcp dest-port eq 135
Router(config-cmap)# match start 13-start offset 3 size 2 eq 0x0030

Router(config)# class-map type access-control match-all blaster2
Router(config-cmap)# match field tcp dest-port eq 4444
Router(config-cmap)# match start 13-start offset 3 size 2 eq 0x0030

Router(config)# class-map type access-control match-all blaster3
Router(config-cmap)# match field udp dest-port eq 69
Router(config-cmap)# match start 13-start offset 3 size 2 eq 0x0030

Router(config)# policy-map type access-control fpm-tcp-policy
Router(config-pmap)# class blaster1
Router(config-pmap-c)# drop
Router(config-pmap-c)# class blaster2
Router(config-pmap-c)# drop

Router(config)# policy-map type access-control fpm-udp-policy
Router(config-pmap)# class blaster3
Router(config-pmap-c)# drop

Router(config)# policy-map type access-control fpm-policy
Router(config-pmap)# class ip-tcp
Router(config-pmap-c)# service-policy fpm-tcp-policy
Router(config-pmap)# class ip-udp
Router(config-pmap-c)# service-policy fpm-udp-policy

Router(config)# interface gigabitEthernet 0/1
Router(config-if)# service-policy type access-control input fpm-policy

```

Configuring FPM for MyDoom Packets: Example

The following example shows how to configure FPM for MyDoom packets. The match criteria is as follows:

- 90 > IP length > 44
- pattern 0x47455420 at 40 bytes from start of IP header
- or
- IP length > 44
- pattern 0x6d3a3830 at 48 bytes from start of IP header
- pattern 0x47455420 at 40 bytes from start of IP header

```

Router(config)# load protocol disk2:ip.phdf
Router(config)# load protocol disk2:tcp.phdf

Router(config)# class-map type stack match-all ip-tcp
Router(config-cmap)# match field ip protocol eq 0x6 next tcp

Router(config)# class-map type access-control match-all mydoom1
Router(config-cmap)# match field ip length gt 44
Router(config-cmap)# match field ip length lt 90
Router(config-cmap)# match start 13-start offset 40 size 4 eq 0x47455420

```

```

Router(config)# class-map type access-control match-all mydoom2
Router(config-cmap)# match field ip length gt 44
Router(config-cmap)# match start 13-start offset 40 size 4 eq 0x47455420
Router(config-cmap)# match start 13-start offset 78 size 4 eq 0x6d3a3830

Router(config)# policy-map type access-control fpm-tcp-policy
Router(config-pmap)# class mydoom1
Router(config-pmap-c)# drop
Router(config-pmap-c)# class mydoom2
Router(config-pmap-c)# drop

Router(config)# policy-map type access-control fpm-policy
Router(config-pmap)# class ip-tcp
Router(config-pmap-c)# service-policy fpm-tcp-policy

Router(config)# interface gigabitEthernet 0/1
Router(config-if)# service-policy type access-control input fpm-policy

```

Additional References

The following sections provide references related to Flexible Packet Matching.

Related Documents

Related Topic	Document Title
Configuring FPM using traffic classification definition files (TCDFs).	Flexible Packet Matching XML Configuration
Complete suite of QoS commands	Cisco IOS Quality of Service Solutions Command Reference

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Security Command Reference* at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or a Cisco IOS master commands list.

- **class (policy-map)**
- **class-map**
- **debug fpm event**
- **description (class-map)**
- **load protocol**
- **match field**
- **match start**
- **policy-map**
- **service-policy**
- **show class-map**
- **show policy-map interface**
- **show protocol phdf**

Feature Information for Flexible Packet Matching

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Flexible Packet Matching

Feature Name	Releases	Feature Information
Flexible Packet Matching	12.4(4)T 12.2(18)ZY	FPM is a packet classification feature that allows users to define one or more classes of network traffic by pairing a rich set of standard matching operators with user-defined protocol header fields. In Cisco IOS Release 12.2(18)ZY, FPM was implemented on the Catalyst 6500 series of switches equipped with the PISA.
FPM Full Packet Filtering	12.4(15)T	In Cisco IOS Release 12.4(15)T, FPM now supports searching for patterns up to 56 bytes long anywhere within the entire packet. Prior to 12.4(15)T, FPM only supported searching for patterns up to 32 bytes long within the first 256 bytes of the packet.
Enhance FPM Search Window Size To 128 bytes	12.2(18)ZYA	FPM now supports searching for patterns up to 128 bytes long anywhere within the entire packet. Also, the number of filters that can be configured per class map has increased from 8 to 32. The additional filters can help offset adverse CPU performance that may occur if the “window” for pattern searching is increased. (However, some optimizations for better performance are possible with match-any type of class maps that have filters starting at same the same offset and the same size.)

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007-2008 Cisco Systems, Inc. All rights reserved



Flexible Packet Matching XML Configuration

First Published: March 3, 2006

Last Updated: March 3, 2006

The Flexible Packet Matching XML Configuration feature allows the use of eXtensible Markup Language (XML) to define traffic classes and actions (policies) to assist in blocking network attacks. The XML file used by Flexible Packet Matching (FPM) is called the traffic classification definition file (TCDF).

The TCDF gives you an alternative to the command-line interface (CLI) as a method to define traffic classification behavior. Traffic classification behavior is identical regardless of the method you use.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Flexible Packet Matching XML Configuration”](#) section on [page 18](#).

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for the Flexible Packet Matching XML Configuration, page 2](#)
- [Restrictions for the Flexible Packet Matching XML Configuration, page 2](#)
- [Information About the Flexible Packet Matching XML Configuration, page 2](#)
- [How to Create and Load Traffic Classification Definition Files for the FPM XML Configuration, page 7](#)
- [Configuration Examples for Creating and Loading Traffic Classification Definition Files for the FPM XML Configuration, page 13](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Additional References, page 15](#)
- [Command Reference, page 16](#)
- [Glossary, page 18](#)
- [Feature Information for Flexible Packet Matching XML Configuration, page 18](#)

Prerequisites for the Flexible Packet Matching XML Configuration

The Flexible Packet Matching XML Configuration feature has the following prerequisites:

- A protocol header definition file (PHDF) relevant to the TCDF must be loaded on the router.
- Although access to an XML editor is not required, using one might make the creation of the TCDF easier.
- You must be familiar with XML file syntax.

Restrictions for the Flexible Packet Matching XML Configuration

The Flexible Packet Matching XML Configuration has the following restrictions:

- The FPM TCDF cannot be used to mitigate an attack that requires stateful classification.
- Because FPM is stateless, it cannot keep track of port numbers being used by protocols that dynamically negotiate ports. Thus, when using the FPM TCDF, port numbers must be explicitly specified.
- FPM cannot perform IP fragmentation or TCP flow reassembly.

Information About the Flexible Packet Matching XML Configuration

Before you create and load the TCDF XML configuration files for use with FPM, you should understand the following concepts.

- [Traffic Classification Definition Files for the Flexible Packet Matching XML Configuration, page 3](#)
- [Protocol Header Definition Files for Traffic Classification Definitions, page 3](#)
- [Traffic Classification Description File Format and Use, page 3](#)
- [Traffic Class Definitions for a Traffic Classification Definition File, page 4](#)
- [Policy Definitions for a Traffic Classification Definition File, page 6](#)

Traffic Classification Definition Files for the Flexible Packet Matching XML Configuration

FPM uses a TCDF to define policies that can block attacks on the network. FPM is a packet classification feature that allows users to define one or more classes of network traffic by pairing a rich set of standard matching operators with user-defined protocol header fields. FPM users can create their own stateless packet classification criteria and define policies with multiple actions (such as drop, log, or send Internet Control Message Protocol [ICMP] unreachable) to immediately block new viruses, worms, and attacks on the network.

Before the release of the Flexible Packet Matching XML Configuration feature, FPM defined traffic classes (class maps), policies (policy maps), and service policies (attach policy maps to a class maps) through the use of CLI commands. With TCDFs, FPM can use XML as an alternative to the CLI to define classes of traffic and specify actions to apply to the traffic classes. Traffic classification behavior is the same whether you create the behavior using a TCDF or configure it using CLI commands. Once a TCDF is created, it can be loaded on any FPM-enabled device in the network.

For more information on FPM, see the [Flexible Packet Matching](#) feature module.

Protocol Header Definition Files for Traffic Classification Definitions

TCDFs require that a relevant PHDF is already loaded on the device. A PHDF defines each field contained in the header of a particular protocol. Each field is described with a name, optional comment, an offset (the location of the protocol header field in relation to the start of the protocol header), and the length of the field. The total length is specified at the end of each PHDF.

The description of a traffic class in a TCDF file can contain header fields defined in a PHDF. If the PHDF is loaded on the router, the class specification to match begins with a list of the protocol headers in the packet. In the TCDF, the traffic class is associated with a policy that binds the match to an action, such as drop, log, or send ICMP unreachable.

FPM provides ready-made definitions for these standard protocols, which can be loaded onto the router with the **load protocol** command: ether.phdf, ip.phdf, tcp.phdf, and udp.phdf. You can also write your own custom PHDFs using XML if one is required for the TCDF.



Note

Because PHDFs are defined via XML, they are not shown in a running configuration.

For more information about PHDFs, see the [Flexible Packet Matching](#) feature module.

Traffic Classification Description File Format and Use

In the TCDF, you can define one or more classes of traffic and policies that describe specified actions for each class of traffic. The TCDF is an XML file that you create in a text file or with an XML editor. The file that you create must have a filename that has the .tcd extension.

The TCDF has the following basic format. XML tags are shown in bold text for example purposes only.

```
<tdcf>
  <class ...> ... </class>
  ...
  <policy> ... </policy>
  ...
</tdcf>
```


For a traffic class, you can identify a match for any field or fields against any part of the packet.



Note

FPM is stateless and cannot be used to mitigate an attack that requires stateful classification, that is classify across IP fragments, across packets in a TCP stream, or peer-to-peer protocol elements.

Policies can be anything from access control, quality of service (QoS), or even routing decisions. For FPM, the associated actions (policies) might include permit, drop, log, or send ICMP unreachable.

Once loaded, the TCDF-defined classes and policies can be applied to any interface or subinterface and behave in an identical manner as the CLI-defined classes and policies. You can define policies in the TCDF and apply them to any entry point to the network to block new attacks.

Traffic Class Definitions for a Traffic Classification Definition File

A class can be any traffic stream of interest. You define a traffic stream of interest by matching a particular interface or port, a source address or destination IP address, a protocol or an application. The following sections contain information you should understand before you define the traffic class in the TCDF for FPM configuration:

- [Class Element Attributes for a Traffic Classification Definition File, page 4](#)
- [Match Element for a Traffic Classification Definition File, page 5](#)
- [Operator Element Attributes for a Traffic Classification Definition File, page 5](#)

Class Element Attributes for a Traffic Classification Definition File

[Table 1](#) lists and describes the attributes that you can associate with the **class** element in a TCDF for the FPM XML configuration. The **class** element contains attributes you can use to specify the traffic class name, its description and type, where to look in the packet, what kind of match, and when the actions should apply to the traffic.

Table 1 *Attributes for Use with the Class Element in a TCDF for the FPM XML Configuration*

Attribute Name	Use	Type
name (required)	Specifies the name of the class. Note When you use the class element inside policy elements, you need specify the name attribute only.	String
type (required)	Specifies the type of class.	Keywords: stack or access-control
stack start	Specifies where to look in the packet. By default, the match starts at Layer 3.	Keyword: l2-start

Table 1 *Attributes for Use with the Class Element in a TCDF for the FPM XML Configuration (continued)*

Attribute Name	Use	Type
match	Specifies the type of match to be performed on the class.	Keywords: all or any <ul style="list-style-type: none"> all—All class matches must be met to perform the policy actions. any—One or more matches within the class must be met to perform the policy actions.
undo	Directs the device to remove the class-map when set to true.	Keywords: true or false

For example, XML syntax for a stack class describing an IP, User Datagram Protocol (UDP), Simple Management Protocol (SNMP) stack might look like this:

```
<class name="snmp-stack" type="stack">
  <match>
    <eq field="ip.protocol" value="x"></eq>
    <eq field="udp.dport" value="161"></eq>
  </match>
</class>
```

Match Element for a Traffic Classification Definition File

The **match** element in the TCDF for FPM XML configuration contains **operator** elements. **Operator** elements are the following: **eq** (equal to), **neq** (not equal to), **lt** (less than), **gt** (greater than), **range** (a value in a specific range, for example, **range 1 – 25**), and **regex** (regular expression string with a maximum length of 32 characters).

In following sections, these various operators are collectively called the operator element.

Operator Element Attributes for a Traffic Classification Definition File

[Table 2](#) lists and describes direct matching attributes that you can associate with the **operator** element in a TCDF for the FPM XML configuration.

Table 2 *Direct Matching Attributes to Use with a Match Element in a TCDF for the FPM XML Configuration*

Attribute Name	Use	Type
start	Begin the match on a predefined keyword or Protocol.Field , if given.	Keyword: l2-start or l3-start Otherwise, a field of a protocol as defined in the PHDF, for example, the source field in the IP protocol.
offset	Used with start attribute. Offset from the start point.	Hexadecimal or decimal number, or string constants, Protocol.Field , or combination of a constant and Protocol.Field with +, -, *, /, &, or l.

Table 2 *Direct Matching Attributes to Use with a Match Element in a TCDF for the FPM XML Configuration (continued)*

Attribute Name	Use	Type
size	Used together with start and offset attributes. How much to match.	Specifies the size of the match in bytes.
mask	Number specifying bits to be matched in protocol or field attributes. Used exclusively with field type of bitset to specify the bits of interest in a bit map.	Decimal or hexadecimal number
value	Value on which to match.	String, number, or regular expression
field	Specifies the name of the field to be compared.	Name of field as defined in the PHDF
next	Identifies the next layer of the protocol. This attribute can be used only in stack type classes.	Keyword that is the name of a protocol defined in the PHDF.
undo	Directs the device to remove the particular match operator when set to true.	Keywords: true or false

Policy Definitions for a Traffic Classification Definition File

A policy is any action that you apply to a class. You should understand the following information before defining the policy in a TCDF for the FPM XML configuration:

- [Policy Element Attributes for a Traffic Classification Definition File, page 6](#)
- [Action Element for a Traffic Classification Definition File, page 7](#)

Policy Element Attributes for a Traffic Classification Definition File

Policies can be anything from access control, QoS, or even routing decisions. For FPM, the associated actions or policies might include drop, log, or send ICMP unreachable. Policies describe the action to take to mitigate attacks on the network.

[Table 3](#) lists and describes the attributes that you can use with the **policy** element in the TDCF for FPM XML configuration.

Table 3 *Attributes for Use with the Policy Element in a TCDF for the FPM XML Configuration*

Attribute Name	Use	Type
name	Name of the policy.	String
type	Specifies the type of policy map.	Keyword: access-control
undo	Directs the device to remove the policy map when set to true.	Keywords: true or false

The policy name in this example is sql-slammer, and the action defined for the policy is to drop the packet. This action is to be applied to the class that has the same name as the policy (class name=“sql-slammer”).

```
<policy name="sql-slammer">
  <class name="sql-slammer"></class>
  <action>drop</action>
</policy>
```

Action Element for a Traffic Classification Definition File

The **action** element is used to specify actions to associate with a policy. The policy with the **action** element is applied to a defined class. The **action** element can contain any of the following: permit, drop, Log, SendBackIcmp, set, RateLimit, alarm, ResetTcpConnection, and DropFlow. For example:

```
<action>
  log
</action>
```

How to Create and Load Traffic Classification Definition Files for the FPM XML Configuration

Perform the following tasks to create and load TCDFs for the FPM XML configuration. You can define traffic classes and policies with multiple actions (such as drop, log, or send Internet Control Message Protocol [ICMP] unreachable) in a TCDF to assist in the blocking of new viruses, worms, and attacks on the network.

- [Creating a Traffic Classification Definition File for the FPM XML Configuration, page 7](#) (required)
- [Loading a Traffic Classification Definition File for the FPM XML Configuration, page 9](#) (required)
- [Associating a Traffic Classification Definition File with an Interface or Subinterface, page 11](#) (required)
- [Displaying TCDF-Defined Traffic Classes and Policies, page 12](#) (optional)

Creating a Traffic Classification Definition File for the FPM XML Configuration

Perform the following task to create a TCDF for FPM XML configuration. The TCDF is used to define traffic classes and the associated policies with specified actions for the purpose of blocking new viruses, worms, and attacks on the network.

The TCDF is configured in a text or XML editor. The syntax of the TCDF must comply with the XML Version 1.0 syntax and the TCDF schema. For information about Version 1.0 XML syntax, see the document at the following url:

<http://www.w3.org/TR/REC-xml/>

Traffic Classification Definition File Syntax Guidelines

The following list describes required and optional syntax for the TCDF:

- The TCDF filename must end in the .tcd extension, for example, sql_slammer.tcd.
- The TCDF contains descriptions for one or more traffic classes and one or more policy actions.

- The file is encoded in the XML notation.
- The TCDF file should begin with the following version encoding:
`<?xml version="1.0" encoding="UTF-8"?>`

SUMMARY STEPS

1. Open a text file or an XML editor and begin the file with the XML version and encoding declaration.
2. Identify the file as a TCDF.
3. Define the traffic class of interest.
4. Identify matching criteria for the defined class of traffic.
5. Define the action to apply to the defined class.
6. End the traffic classification definition.
7. Save the TCDF file with a filename that has a .tcd extension.

DETAILED STEPS

- Step 1** Open a text file or an XML editor and begin the file with the XML version and encoding declaration.

```
<?xml version="1.0" encoding="UTF-8"?>
```

- Step 2** Identify the file as a TCDF. For example:

```
<tcd>
```

- Step 3** Define the traffic class of interest.

For example, a stack class describing an IP and UDP stack might be described as follows. In this example, the name of the traffic class is “ip-udp,” and the class type is “stack.”

```
<class name="ip-udp" type="stack"></class>
```

In the following example, the name of the traffic class is slammer, the class type is access control, and the match criteria is all:

```
<class name="slammer" type="access-control" match="all"></class>
```

- Step 4** Identify matching criteria for the defined classes of traffic. For example:

```
<class name="ip-udp" type="stack">
  <match>
    <eq field="ip.protocol" value="0x11" next="udp"></eq>
  </match>
</class>

<class name="slammer" type="access-control" match="all">
  <match>
    <eq field="udp.dest-port" value="0x59A"></eq>
    <eq field="ip.length" value="0x194"></eq>
    <eq start="13-start" offset="224" size="4" value="0x00401010"></eq>
  </match>
</class>
```

The traffic of interest in this TCDF matches fields defined in the PHDF files, ip.phdf and udp.phdf. The matching criteria for slammer packets is a UDP destination port number 1434 (0x59A), an IP length not to exceed 404 (0x194) bytes, and a Layer 3 position with a pattern 0x00401010 at 224 bytes from start (offset) of the IP header.

Step 5 Define the action to apply to the defined class. For example:

```
<policy name="fpm-udp-policy">
  <class name="slammer"></class>
  <action>Drop</action>
</policy>
```

The policy name in this example is fpm-udp-policy, and the action defined for the policy is to drop the packet. This action is to be applied to the class that has the name slammer.

Step 6 End the traffic classification definition. For example:

```
</tcdf>
```

Step 7 Save the TCDF file with a filename that has a .tcd file extension, for example: slammer.tcd.

Loading a Traffic Classification Definition File for the FPM XML Configuration

Perform this task to load a TCDF for the FPM XML configuration. After the TCDF is successfully loaded, you can use service-policy CLI to attach TCDF policies to a specific interface or interfaces (see the [“Associating a Traffic Classification Definition File with an Interface or Subinterface”](#) section on page 11).

SUMMARY STEPS

1. **enable**
2. **show protocol phdf** *protocol-name*
3. **configure terminal**
4. **load protocol** *location:filename*
5. **load classification** *location:filename*
6. **end**
7. **show class-map** [**type** {**stack** | **access-control**}] [*class-map-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.
	Example: Router> enable	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	show protocol phdf <i>protocol-name</i>	Displays protocol information from a specific PHDF.
	Example: Router# show protocol phdf ip	<ul style="list-style-type: none"> • Use this command to verify that a PHDF file relevant to the TCDF is loaded on the device.
Step 3	configure terminal	Enters global configuration mode.
	Example: Router# configure terminal	

	Command or Action	Purpose
Step 4	load protocol <i>location:filename</i> Example: Router(config)# load protocol localdisk1:ip.phdf	(Optional) Loads a PHDF onto a router. <ul style="list-style-type: none"> The specified location must be local to the router. Note If the required PHDF is already loaded on the router (see Step 2), skip this step and proceed to Step 5).
Step 5	load classification <i>location:filename</i> Example: Router(config)# load classification localdisk1:slammer.tcdf	Loads a TCDF onto a router. <ul style="list-style-type: none"> The specified location must be local to the router.
Step 6	end Example: Router(config)# end	Exits to privileged EXEC mode.
Step 7	show class-map [type { stack access-control }] [<i>class-map-name</i>] Example: Router# show class-map sql-slammer	(Optional) Displays a class map and its matching criteria. <ul style="list-style-type: none"> Use this command to verify that a class defined in the TCDF file is available on the device. The <i>class-map-name</i> argument is the name of a class in the TCDF.

Examples

The following is sample output from a **show class-map** command that displays the traffic classes defined in the TCDF after it is loaded on the router:

```
Router# show class-map
.
.
.
class-map type stack match-all ip-udp
  match field IP protocol eq 0x11 next UDP

class-map type access-control match-all slammer
  match field UDP dest-port eq 0x59A
  match field IP length eq 0x194
  match start 13-start offset 224 size 4 eq 0x4011010
.
.
.
```

What to Do Next

After you have defined the TCDF, you must apply that policy to an interface as shown in the following task “[Associating a Traffic Classification Definition File with an Interface or Subinterface](#).”

Associating a Traffic Classification Definition File with an Interface or Subinterface

Perform the following task to associate a TCDF with an interface or subinterface.

After the TCDF is loaded, traffic classification behavior defined using the TCDF is identical to the same behavior defined using the CLI.

Prerequisites

The TCDP and FPM must be configured on the device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **service-policy** [**type access-control**] {**input** | **output**} *policy-map-name*
5. **end**
6. **show policy-map interface** [**type access-control**] *interface-name slot/port* [**input** | **output**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type slot/port</i> Example: Router(config)# interface gigabitEthernet 0/1	Configures an interface type and enters interface configuration mode.
Step 4	service-policy [type access-control] { input output } <i>policy-map-name</i> Example: Router(config-if)# service-policy type access-control input sql-slammer	Specifies the type and the name of the traffic policy to be attached to the input or output direction of an interface. <ul style="list-style-type: none">• The <i>policy-map-name</i> argument is the name of a policy in the TCDF.

	Command or Action	Purpose
Step 5	end Example: Router(config-if)# end	Exits to privileged EXEC mode.
Step 6	show policy-map interface [type access-control] interface-name slot/port [input output] Example: Router# show policy-map interface gigabitEthernet 0/1	(Optional) Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface. <ul style="list-style-type: none">Use this command to verify that policy defined in TCDF is associated with the named interface.

Displaying TCDF-Defined Traffic Classes and Policies

Perform this task to display TCDF-defined traffic classes and policies.

SUMMARY STEPS

1. **enable**
2. **show class-map** [type {stack | access-control}] [class-map-name]
3. **show class-map type stack** [class-map-name]
4. **show class-map type access-control** [class-map-name]
5. **show policy-map** [policy-map]
6. **exit**

DETAILED STEPS

Step 1	enable Use this command to enable privileged EXEC mode. Enter your password if prompted. For example: <pre>Router> enable Router#</pre>
Step 2	show class-map [type {stack access-control}] [class-map-name] Use this command to verify that a class defined in the TCDF file is available on the device. For example: <pre>Router# show class-map . . . class-map type stack match-all ip-udp match field IP protocol eq 0x11 next UDP class-map type access-control match-all slammer match field UDP dest-port eq 0x59A match field IP length eq 0x194 match start 13-start offset 224 size 4 eq 0x4011010 . . .</pre>

Step 3 **show class-map type stack** [*class-map name*]

Use this command to display the stack type defined for the class of traffic in the TCDF file. For example:

```
Router# show class-map type stack ip-udp

class-map type stack match-all ip-udp
  match field IP protocol eq 0x11 next UDP
```

Step 4 **show class-map type access-control** [*class-map-name*]

Use this command to display the access type defined for the class in the TCDF file. For example:

```
Router# show class-map type access-control slammer

class-map type access-control match-all slammer
  match field UDP dest-port eq 0x59A
  match field IP length eq 0x194
  match start 13-start offset 224 size 4 eq 0x4011010
```

Step 5 **show policy-map** [*policy-map*]

Use this command to display the contents of a policy map defined in the TCDF. For example:

```
Router# show policy-map fpm-udp-policy

policy-map type access-control fpm-udp-policy
  class slammer
    drop
```

Step 6 **exit**

Use this command to exit to user EXEC mode. For example:

```
Router# exit
Router>
```

Configuration Examples for Creating and Loading Traffic Classification Definition Files for the FPM XML Configuration

This section contains the following configuration examples:

- [Creating and Loading a Traffic Classification Definition File for Slammer Packets for the FPM XML Configuration: Example, page 14](#)
- [Creating and Loading a Traffic Classification Definition File for MyDoom Packets for the FPM XML Configuration: Example, page 14](#)

**Note**

The TCDF files are created in a text file or with an XML editor. In the following examples, XML tags are shown in bold text and field names in italic text. The values for the attributes are entered in quotation marks ("value").

Creating and Loading a Traffic Classification Definition File for Slammer Packets for the FPM XML Configuration: Example

The following example shows how to create and load a TCDF for slammer packets (UDP 1434) for the FPM configuration. The match criteria defined within the **class** element is for slammer packets with an IP length not to exceed 404 (0x194) bytes, UDP destination port 1434 (0x59A), and pattern 0x00401010 at 224 bytes from start of IP header. This example also shows how to define the policy “sql-slammer” with the action to drop slammer packets.

```
<?xml version="1.0" encoding="UTF-8"?>
<tcdf>
  <class name="ip-udp" type="stack">
    <match>
      <eq field="ip.protocol" value="0x11" next="udp"></eq>
    </match>
  </class>

  <class name="slammer" type="access-control" match="all">
    <match>
      <eq field="udp.dest-port" value="0x59A"></eq>
      <eq field="ip.length" value="0x194"></eq>
      <eq start="13-start" offset="224" size="4" value="0x00401010"></eq>
    </match>
  </class>

  <policy type="access-control" name="fpm-udp-policy">
    <class name="slammer"></class>
    <action>Drop</action>
  </policy>
</tcdf>
```

The following example shows how to load the TCDF file onto the device and apply the policy defined in the file to the interface Gigabit Ethernet 0/1:

```
configure terminal
load classification localdisk1:sql-slammer.tcdf
policy-map type access-control my-policy-1
class ip-udp
service-policy fpm-udp-policy
interface gigabitEthernet 0/1
service-policy type access-control input my-policy-1
end
```

Creating and Loading a Traffic Classification Definition File for MyDoom Packets for the FPM XML Configuration: Example

The following example shows how to create and load a TCDF for MyDoom packets in a text file or XML editor for the FPM XML configuration. The match criteria for the MyDoom packets are as follows:

- 90 > IP length > 44
- pattern 0x47455420 at 40 bytes from start of IP header
- or
- IP length > 44
- pattern 0x47455420 at 40 bytes from start of IP header

```

<tcdcf>
  <class name="md-stack" type="stack">
    <match>
      <eq field="ip.protocol" value="6" next="tcp"></eq>
    </match>
  </class>
  <class type="access-control" name="mydoom1">
    <match>
      <gt field="ip.length" value="44"/>
      <lt field="ip.length" value="90"/>
      <eq start="ip.version" offset="tcp.headerlength*4+20" size="4"
        value="0x47455420"/>
    </match>
  </class>
  <class type="access-control" name="mydoom2">
    <match>
      <gt field="ip.length" value="44"/>
      <eq start="ip.version" offset="tcp.headerlength*4+58" size="4"
        value="0x6d3a3830"/>
      <eq start="ip.version" offset="tcp.headerlength*4+20" size="4"
        value="0x47455420"/>
    </match>
  </class>

  <policy name="fpm-md-stack-policy">
    <class name="mydoom1"></class>
    <action>drop</action>
  </policy>

  <policy name="fpm-md-stack-policy">
    <class name="mydoom2"></class>
    <action>drop</action>
  </policy>
</tcdcf>

```

The following example shows how to load the TCDF file onto the device and apply the policy defined in the file to the interface Ethernet 0/1:

```

configure terminal
load classification localdisk1:sql-slammer.tcdf
policy-map type access-control my-policy-2
class md-stack
service-policy fpm-md-stack-policy
interface Ethernet 0/1
  service-policy type access-control input my-policy-2
end

```

Additional References

The following sections provide references related to the Flexible Packet Matching XML Configuration feature.

Related Documents

Related Topic	Document Title
Additional configuration information for class maps and policy maps	The section “ Modular Quality of Service Command-Line Interface ” in the <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> , Release 12.4
Information about and configuration tasks for FPM	Flexible Packet Matching

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
The Cisco Technical Support and Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

The following commands are introduced or modified in the feature or features

- **load classification**

For information about these commands, see the Cisco IOS Security Command Reference at http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the Master Command List.

Glossary

FPM—Flexible Packet Matching. Packet classification feature that allows users to define one or more classes of network traffic by pairing a rich set of standard matching operators with user-defined protocol header fields.

packet—Logical grouping of information that includes a header containing control information and (usually) user data. Packets most often are used to refer to network layer units of data. The terms datagram, frame, message, and segment also are used to describe logical information groupings at various layers of the OSI reference model and in various technology circles.

stateful classification—Classification that requires state maintenance to identify classes of packets, for example, classifying across IP fragments, classifying across packets in a TCP stream, or classifying peer-to-peer protocols.

stateless classification—Classification that supports a match on any field or fields anywhere in Layer 2 to Layer 7 within the packet. Stateless classification can identify a packet as belonging to a class while utilizing no information other than what is in the packet itself and the class specification.

TCDF—traffic classification definition file. Extensible Markup Language (XML) file created for the purpose of defining traffic classes and policies for Flexible Packet Matching (FPM) that can assist in the blocking of attacks on the network.

XML—eXtensible Markup Language. Standard maintained by the World Wide Web Consortium (W3C). It defines a syntax that lets you create markup languages to specify information structures, which define the type of information, for example, subscriber name or address, not how the information looks (bold, italic, and so on). External processes can manipulate these information structures and publish them in a variety of formats. Text markup language designed to enable the use of SGML on the World Wide Web. XML allows you to define your own customized markup language.

**Note**

See the Cisco [Dictionary of Internetworking Terms and Acronyms](#) for terms not included in this glossary.

Feature Information for Flexible Packet Matching XML Configuration

[Table 4](#) lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

**Note**

[Table 4](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 4 **Feature Information for Flexible Packet Matching XML Configuration**

Feature Name	Releases	Feature Information
Flexible Packet Matching XML Configuration	12.4(6)T	<p>The Flexible Packet Matching XML Configuration feature provides an Extensible Markup Language (XML)-based configuration file for Flexible Packet Matching (FPM) that can be used to define traffic classes and actions (policies) to assist in the blocking of attacks on a network. The XML file used by FPM is called the traffic classification definition file (TCDF).</p> <p>The TCDF gives you an alternative to the command-line interface (CLI) as a method to define traffic classification behavior. Traffic classification behavior is identical regardless of the method you use.</p> <p>This feature was introduced in Cisco IOS Release 12.4(6)T.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Traffic Classification Definition Files for the Flexible Packet Matching XML Configuration, page 3 • Traffic Classification Description File Format and Use, page 3 • Creating a Traffic Classification Definition File for the FPM XML Configuration, page 7 • Loading a Traffic Classification Definition File for the FPM XML Configuration, page 9 • Associating a Traffic Classification Definition File with an Interface or Subinterface, page 11 • Displaying TCDF-Defined Traffic Classes and Policies, page 12 <p>The following command was introduced by this feature: load classification.</p>

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and

coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.