



## **Cisco IOS Security Configuration Guide: Securing User Services**

Release 12.4

### **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, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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

*Cisco IOS Security Configuration Guide: Securing User Services*  
© 2009 Cisco Systems, Inc. All rights reserved.



# About Cisco IOS and Cisco IOS XE Software Documentation

---

**Last Updated: March 5, 2009**

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 <b>^D</b> or <b>Ctrl-D</b> 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
<b>bold</b>	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.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
	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.
<b>Bold Courier font</b>	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, Cisco IOS XE, 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/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.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
<p><i>Cisco IOS Bridging and IBM Networking Configuration Guide</i></p> <p><i>Cisco IOS Bridging Command Reference</i></p> <p><i>Cisco IOS IBM Networking Command Reference</i></p>	<ul style="list-style-type: none"> <li>• Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRSM).</li> <li>• 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.</li> </ul>
<p><i>Cisco IOS Broadband and DSL Configuration Guide</i></p> <p><i>Cisco IOS XE Broadband and DSL Configuration Guide</i></p> <p><i>Cisco IOS Broadband and DSL Command Reference</i></p>	<p>Point-to-Point Protocol (PPP) over ATM (PPPoA) and PPP over Ethernet (PPPoE).</p>
<p><i>Cisco IOS Carrier Ethernet Configuration Guide</i></p> <p><i>Cisco IOS Carrier Ethernet Command Reference</i></p>	<p>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).</p>
<p><i>Cisco IOS Configuration Fundamentals Configuration Guide</i></p> <p><i>Cisco IOS XE Configuration Fundamentals Configuration Guide</i></p> <p><i>Cisco IOS Configuration Fundamentals Command Reference</i></p>	<p>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.</p>
<p><i>Cisco IOS DECnet Configuration Guide</i></p> <p><i>Cisco IOS XE DECnet Configuration Guide</i></p> <p><i>Cisco IOS DECnet Command Reference</i></p>	<p>DECnet protocol.</p>
<p><i>Cisco IOS Dial Technologies Configuration Guide</i></p> <p><i>Cisco IOS XE Dial Technologies Configuration Guide</i></p> <p><i>Cisco IOS Dial Technologies Command Reference</i></p>	<p>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).</p>
<p><i>Cisco IOS Flexible NetFlow Configuration Guide</i></p> <p><i>Cisco IOS Flexible NetFlow Command Reference</i></p>	<p>Flexible NetFlow.</p>

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

<b>Configuration Guide and Command Reference Titles</b>	<b>Features/Protocols/Technologies</b>
<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 Services Gateway Configuration Guide</i> <i>Cisco IOS Intelligent Services 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)**

<b>Configuration Guide and Command Reference Titles</b>	<b>Features/Protocols/Technologies</b>
<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:  <a href="http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html">http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html</a>
<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)

<b>Configuration Guide and Command Reference Titles</b>	<b>Features/Protocols/Technologies</b>
<p><i>Cisco IOS Multiprotocol Label Switching Configuration Guide</i></p> <p><i>Cisco IOS XE Multiprotocol Label Switching Configuration Guide</i></p> <p><i>Cisco IOS Multiprotocol Label Switching Command Reference</i></p>	MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS Traffic Engineering (TE), and MPLS Embedded Management (EM) and MIBs.
<p><i>Cisco IOS Multi-Topology Routing Configuration Guide</i></p> <p><i>Cisco IOS Multi-Topology Routing Command Reference</i></p>	Unicast and multicast topology configurations, traffic classification, routing protocol support, and network management support.
<p><i>Cisco IOS NetFlow Configuration Guide</i></p> <p><i>Cisco IOS XE NetFlow Configuration Guide</i></p> <p><i>Cisco IOS NetFlow Command Reference</i></p>	Network traffic data analysis, aggregation caches, export features.
<p><i>Cisco IOS Network Management Configuration Guide</i></p> <p><i>Cisco IOS XE Network Management Configuration Guide</i></p> <p><i>Cisco IOS Network Management Command Reference</i></p>	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).
<p><i>Cisco IOS Novell IPX Configuration Guide</i></p> <p><i>Cisco IOS XE Novell IPX Configuration Guide</i></p> <p><i>Cisco IOS Novell IPX Command Reference</i></p>	Novell Internetwork Packet Exchange (IPX) protocol.
<p><i>Cisco IOS Optimized Edge Routing Configuration Guide</i></p> <p><i>Cisco IOS Optimized Edge Routing Command Reference</i></p>	Optimized edge routing (OER) monitoring, policy configuration, routing control, logging and reporting, and VPN IPsec/generic routing encapsulation (GRE) tunnel interface optimization.
<p><i>Cisco IOS Quality of Service Solutions Configuration Guide</i></p> <p><i>Cisco IOS XE Quality of Service Solutions Configuration Guide</i></p> <p><i>Cisco IOS Quality of Service Solutions Command Reference</i></p>	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).
<p><i>Cisco IOS Security Configuration Guide</i></p> <p><i>Cisco IOS XE Security Configuration Guide</i></p> <p><i>Cisco IOS Security Command Reference</i></p>	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)**

<b>Configuration Guide and Command Reference Titles</b>	<b>Features/Protocols/Technologies</b>
<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>	Virtual switch redundancy, high availability, and packet handling; converting between standalone and virtual switch modes; virtual switch link (VSL); Virtual Switch Link Protocol (VSLP).  <b>Note</b> 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.
<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 <b>debug</b> 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>
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: <a href="http://www.rfc-editor.org/">http://www.rfc-editor.org/</a>

## 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 HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0812R)

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

© 2008–2009 Cisco Systems, Inc. All rights reserved.



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

---

**Last Updated: March 5, 2009**

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 <b>logout</b> or <b>exit</b> command.	<ul style="list-style-type: none"> <li>• Change terminal settings.</li> <li>• Perform basic tests.</li> <li>• Display device status.</li> </ul>
Privileged EXEC	From user EXEC mode, issue the <b>enable</b> command.	Router#	Issue the <b>disable</b> command or the <b>exit</b> command to return to user EXEC mode.	<ul style="list-style-type: none"> <li>• Issue <b>show</b> and <b>debug</b> commands.</li> <li>• Copy images to the device.</li> <li>• Reload the device.</li> <li>• Manage device configuration files.</li> <li>• Manage device file systems.</li> </ul>
Global configuration	From privileged EXEC mode, issue the <b>configure terminal</b> command.	Router(config)#	Issue the <b>exit</b> command or the <b>end</b> command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, issue the <b>interface</b> command.	Router(config-if)#	Issue the <b>exit</b> command to return to global configuration mode or the <b>end</b> command to return to privileged EXEC mode.	Configure individual interfaces.
Line configuration	From global configuration mode, issue the <b>line vty</b> or <b>line console</b> command.	Router(config-line)#	Issue the <b>exit</b> command to return to global configuration mode or the <b>end</b> 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 <b>reload</b> command. Press the <b>Break</b> 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 <b>continue</b> command.	<ul style="list-style-type: none"> <li>Run as the default operating mode when a valid image cannot be loaded.</li> <li>Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted.</li> <li>Perform password recovery when a CTRL-Break sequence is issued within 60 seconds of a power-on or reload event.</li> </ul>
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"> <li>A user-configured access policy was configured using the <b>transport-map</b> command, which directed the user into diagnostic mode.</li> <li>The router was accessed using an RP auxiliary port.</li> <li>A break signal (<b>Ctrl-C</b>, <b>Ctrl-Shift-6</b>, or the <b>send break</b> command) was entered, and the router was configured to enter diagnostic mode when the break signal was received.</li> </ul>	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"> <li>Inspect various states on the router, including the Cisco IOS state.</li> <li>Replace or roll back the configuration.</li> <li>Provide methods of restarting the Cisco IOS software or other processes.</li> <li>Reboot hardware, such as the entire router, an RP, an ESP, a SIP, a SPA, or possibly other hardware components.</li> <li>Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.</li> </ul>

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
<b>help</b>	Provides a brief description of the help feature in any command mode.
<b>?</b>	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](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 **show**. 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
<b>h</b>	help
<b>lo</b>	logout
<b>p</b>	ping
<b>s</b>	show
<b>u</b> or <b>un</b>	undebug
<b>w</b>	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](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](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](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 ASR 1000 Series Aggregation Services Routers Software Configuration Guide*:  
[http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/Using\\_CLI.html](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>
- 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/pcgi-bin/Support/OutputInterpreter/home.pl>

---

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0812R)

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

© 2008–2009 Cisco Systems, Inc. All rights reserved.





# Securing User Services Overview

---

**First Published: June 5, 2009**

**Last Updated: June 5, 2009**

The Securing User Services Overview document covers the topics of identifying users through the authentication, authorization, and accounting (AAA) protocol, controlling user access to remote devices and using security server information to track services on Cisco IOS networking devices.

## Finding Feature Information

Your software release may not support all the features documented in this overview module. For the latest feature information and caveats, see the release notes for your platform and software release.

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

- [AutoSecure, page 2](#)
- [Authentication, Authorization, and Accounting, page 2](#)
- [Security Server Protocols, page 4](#)
- [RADIUS and TACACS+ Attributes, page 5](#)
- [Secure Shell, page 5](#)
- [Cisco IOS Login Enhancements, page 6](#)
- [Cisco IOS Resilient Configuration, page 6](#)
- [Image Verification, page 6](#)
- [IP Source Tracker, page 6](#)
- [Role-Based CLI Access, page 6](#)



---

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

- [Security with Passwords, Privileges, and Login Usernames for CLI Sessions on Networking Devices, page 7](#)
- [Kerberos, page 7](#)
- [Lawful Intercept, page 7](#)

## AutoSecure

The AutoSecure feature simplifies the security configuration of a router and hardens the router configuration by disabling common IP services that can be exploited for network attacks and enable IP services and features that can aid in the defense of a network when under attack.

AutoSecure secures both the management and forwarding planes in the following ways:

- Securing the management plane is accomplished 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.
- Securing the forwarding plane is accomplished by enabling Cisco Express Forwarding (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.

## Authentication, Authorization, and Accounting

Cisco's authentication, authorization, and accounting (AAA) paradigm is an architectural framework for configuring a set of three independent security functions in a consistent, modular manner. AAA provides a 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 Authentication, Authorization, and Accounting chapters. You can configure up to four sequential backup methods.



---

**Note** If backup methods are not configured, access is denied to the device if the username/password database cannot be accessed for any reason.

---

The following sections discuss the AAA security functions in greater detail:

- [Authentication, page 3](#)
- [Authorization, page 3](#)
- [Accounting, page 3](#)
- [Authentication Proxy, page 3](#)
- [802.1x Authentication Services, page 4](#)
- [Network Admission Control, page 4](#)

## Authentication

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. AAA authentication is configured by defining a named list of authentication methods and then applying that list to various interfaces.

## Authorization

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, Internetwork Packet Exchange (IPX), AppleTalk Remote Access (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

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.

---

## Authentication Proxy

The Cisco IOS Firewall Authentication Proxy feature is used by network administrators to apply dynamic, per-user authentication and authorization security policies, which authenticates users in addition to industry standard TACACS+ and RADIUS authentication protocols. Authenticating and authorizing connections by users provides more robust protection against network attacks because users can be identified and authorized on the basis of their per-user policy.

Once the authentication proxy feature is implemented, users can log into the network or access the Internet through 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.

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.

## 802.1x Authentication Services

802.1x Authentication Services feature is used to configure local 802.1x port-based authentication and Virtual Private Network (VPN) access on Cisco integrated services routers (ISRs) through the IEEE 802.1X protocol framework. 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.

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.

## Network Admission Control

The Cisco Network Admission Control (NAC) feature addresses the increased threat and impact of worms and viruses have on business networks. This feature is part of the Cisco Self-Defending Network Initiative that helps customers identify, prevent, and adapt to security threats.

NAC enables Cisco routers to enforce access privileges when an endpoint attempts to connect to a network. This access decision can be made on the basis of information about the endpoint device, such as its current antivirus state, which includes information such as version of antivirus software, virus definitions, and version of scan engine.

NAC allows 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 NAC is the Cisco Trust Agent (CTA), which resides on an endpoint system and communicates with Cisco routers on the network. The CTA 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.

## Security Server Protocols

AAA security protocols are used on a router or network access server administers its security functions. AAA is the means through which communication is established between the network access server and Cisco supported RADIUS and TACACS+ security server protocols.

If the database on a security server is used to store login username/password pairs, the router or access server must be configured to support the applicable protocol; in addition, because most supported security protocols must be administered through the AAA security services, AAA must be enabled.

The following sections discuss the RADIUS and TACACS+ security server protocols in greater detail:

- [RADIUS, page 5](#)
- [TACACS+, page 5](#)

## RADIUS

The RADIUS distributed client/server system is implemented through the AAA protocol. RADIUS 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+

The TACACS+ security application is implemented through AAA and 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.

The protocol was designed to scale as networks grow and to adapt to new security technology. The underlying architecture of the TACACS+ protocol complements the independent AAA architecture.

## RADIUS and TACACS+ Attributes

There are various vendor interpretations of the RADIUS and TACACS+ RFCs. Although different vendors can be in compliance with any RFC does not guarantee interoperability. Interoperability is guaranteed only if standard RFCs are used for the RADIUS and TACACS+ protocols.

When nonstandard RADIUS and TACACS+ RFCs are used, attributes must be developed and implemented by vendors so that their respective devices can interoperate with each other.

The following sections discuss the RADIUS and TACACS+ attributes in greater detail:

- [RADIUS Attributes, page 5](#)
- [TACACS+ Attributes, page 5](#)

## RADIUS Attributes

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

## TACACS+ Attributes

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

## Secure Shell

The Secure Shell (SSH) feature 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.

## Cisco IOS Login Enhancements

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.

## 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).

## Image Verification

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.

## IP Source Tracker

The IP Source Tracker feature allows information to be gathered about the traffic 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.

## 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.

# Security with Passwords, Privileges, and Login Usernames for CLI Sessions on Networking Devices

There are conditions where networking devices are installed on the network with no security options configured, or a networking device is installed and help is needed to understand how baseline of security is implemented on the Cisco IOS CLI operating system session running on the networking device.

In this document, the following basic security topics are discussed:

- Different levels of authorization for CLI sessions can be differentiated to control access to commands that can modify the status of the networking device versus commands that are used to monitor the device
- Passwords can be assigned to CLI sessions
- Users can be required to log in to a networking device with a username
- Privilege levels of commands can be changed to create new authorization levels for CLI sessions

## Kerberos

The Kerberos feature is 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 and is based on the concept of a trusted third-party that performs secure verification of users and services. It is primarily used to verify that users and the network services they use are really who and what they claim to be. To accomplish this verification, a trusted Kerberos server issues tickets that 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.

## Lawful Intercept

The Lawful Intercept (LI) feature supports service providers in meeting the requirements of law enforcement agencies to provide the ability to intercept Voice over IP (VoIP) or data traffic going through the edge routers. The Lawful Intercept (LI) architecture includes the Cisco Service Independent Intercept architecture and PacketCable Lawful Intercept architecture.

---

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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.

© 2009 Cisco Systems, Inc. All rights reserved.



# AutoSecure

---

**First Published: September 27, 2007**

**Last Updated: February 27, 2009**

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.

## 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 AutoSecure” section on page 14](#).

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 AutoSecure, page 2](#)
- [Information About AutoSecure, page 2](#)
- [How to Configure AutoSecure, page 6](#)
- [Configuration Examples for AutoSecure, page 9](#)
- [Additional References, page 12](#)
- [Command Reference, page 13](#)
- [Feature Information for AutoSecure, page 14](#)



---

**Americas Headquarters:**

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

# Restrictions for AutoSecure

The AutoSecure feature should be used in a test environment and not in production networks.

## 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 Cisco Configuration Professional (CCP), 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—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	<b>enable</b>  <b>Example:</b> Router> enable	Enables higher privilege levels, such as privileged EXEC mode.  Enter your password if prompted.
Step 2	<b>auto secure</b> [ <b>management</b>   <b>forwarding</b> ] [ <b>no-interact</b>   <b>full</b> ] [ <b>ntp</b>   <b>login</b>   <b>ssh</b>   <b>firewall</b>   <b>tcp-intercept</b> ]  <b>Example:</b> Router# auto secure	Secures the management and forwarding planes of the router.  <ul style="list-style-type: none"> <li>• <b>management</b>—Only the management plane will be secured.</li> <li>• <b>forwarding</b>—Only the forwarding plane will be secured.</li> <li>• <b>no-interact</b>—The user will not be prompted for any interactive configurations.</li> <li>• <b>full</b>—The user will be prompted for all interactive questions. This is the default.</li> </ul>

## 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	<b>enable</b>  <b>Example:</b> Router> enable	Enables higher privilege levels, such as privileged EXEC mode.  Enter your password if prompted.
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>security passwords min-length length</b>  <b>Example:</b> Router(config)# security passwords min-length 6	Ensures that all configured passwords are at least a specified length.  <ul style="list-style-type: none"> <li><i>length</i>—Minimum length of a configured password.</li> </ul>
Step 4	<b>enable password {password   [encryption-type] encrypted-password}</b>  <b>Example:</b> Router(config)# enable password elephant	Sets a local password to control access to various privilege levels.
Step 5	<b>security authentication failure rate threshold-rate log</b>  <b>Example:</b> Router(config)# security authentication failure rate 10 log	Configures the number of allowable unsuccessful login attempts.  <ul style="list-style-type: none"> <li><i>threshold-rate</i>—Number of allowable unsuccessful login attempts.</li> <li><b>log</b>—Syslog authentication failures if the rate exceeds the threshold.</li> </ul>

## 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	<b>enable</b>  <b>Example:</b> Router> enable	Enables higher privilege levels, such as privileged EXEC mode.  Enter your password if prompted.
Step 2	<b>show auto secure config</b>  <b>Example:</b> Router# show auto secure config	(Optional) Displays all configuration commands that have been added as part of the AutoSecure configuration.

## 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 services 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:example.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 example.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.example.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</i> , Release 12.3T
Additional router configuration commands	<i>Cisco IOS Configuration Fundamentals Command Reference</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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## 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
<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 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).

- **auto secure**
- **security passwords min-length**
- **show auto secure config**

# Feature Information for AutoSecure

Table 1 lists the features in this module and provides links to specific configuration information.

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, Catalyst OS, and Cisco IOS XE 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 AutoSecure

Feature Name	Releases	Feature Information
AutoSecure	12.3(1) 12.2(18)S 12.3(8)T 12.2(27)SBC Cisco IOS XE Release 2.3	<p>By using a single command-line interface (CLI), the AutoSecure feature allows a user to perform the following functions:</p> <ul style="list-style-type: none"> <li>• Disable common IP services that can be exploited for network attacks</li> <li>• Enable IP services and features that can aid in the defense of a network when under attack</li> </ul> <p>This feature also simplifies the security configuration of a router and hardens the router configuration.</p> <p>In Cisco IOS Release 12.3(1)S, this feature was introduced.</p> <p>This feature was integrated into Cisco IOS Release 12.2(18)S.</p> <p>In Cisco IOS Release 12.3(8)T, support for the roll-back functionality and system logging messages were added.</p> <p>This feature was integrated into Cisco IOS Release 12.(27)SBC.</p> <p>This feature was integrated into Cisco IOS XE Release 2.3.</p> <p>No commands were introduced or modified.</p>

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

---

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.

© 2007-2009 Cisco Systems, Inc. All rights reserved.

---





## **Authentication, Authorization, and Accounting (AAA)**





## **Authentication**





# Configuring Authentication

---

**First Published: October 26, 1998**

**Last Updated: June 19, 2009**

Authentication provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the selected security protocol, encryption. Authentication is the way a user is identified prior to being allowed access to the network and network services.

## 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 Configuring Authentication” section on page 52](#).

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

- [Named Method Lists for Authentication](#)
- [How to Configure AAA Authentication Methods](#)
- [Non-AAA Authentication Methods](#)
- [Authentication Examples](#)
- [Additional References](#)
- [Feature Information for Configuring Authentication](#)



---

**Americas Headquarters:**

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

# Prerequisites for Configuring Authentication

The Cisco IOS software implementation of authentication is divided into AAA Authentication and non-authentication methods. Cisco recommends that, whenever possible, AAA security services be used to implement authentication.

## Restrictions for Configuring Authentication

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

## Information About Configuring Authentication

The following section describes how AAA authentication is configured by defining a named list of authentication methods and then applying that list to various interfaces.

## Named Method Lists for Authentication

A named list of authentication methods must first be defined to configure AAA authentication, and then this named list is applied 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.

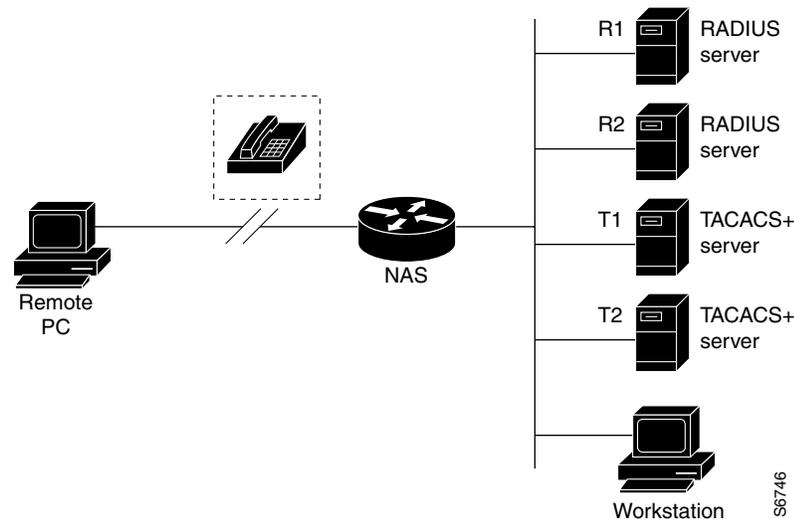
This section contains the following subsections:

- [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.

## How to Configure AAA Authentication Methods

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](#)
- [Preventing an Access Request with a Blank Username from Being Sent to the RADIUS Server](#)
- [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)# <b>aaa new-model</b>	Enables AAA globally.
Step 2	Router(config)# <b>aaa authentication login</b> { <b>default</b>   <i>list-name</i> } <i>method1</i> [ <i>method2...</i> ]	Creates a local authentication list.
Step 3	Router(config)# <b>line</b> [ <b>aux</b>   <b>console</b>   <b>tty</b>   <b>vty</b> ] <b>line-number</b> [ <b>ending-line-number</b> ]	Enters line configuration mode for the lines to which you want to apply the authentication list.
Step 4	Router(config-line)# <b>login authentication</b> { <b>default</b>   <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
<b>enable</b>	Uses the enable password for authentication.
<b>krb5</b>	Uses Kerberos 5 for authentication.
<b>krb5-telnet</b>	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.
<b>line</b>	Uses the line password for authentication.
<b>local</b>	Uses the local username database for authentication.
<b>local-case</b>	Uses case-sensitive local username authentication.
<b>none</b>	Uses no authentication.
<b>group radius</b>	Uses the list of all RADIUS servers for authentication.

**Table 4** AAA Authentication Login Methods (continued)

Keyword	Description
<code>group tacacs+</code>	Uses the list of all TACACS+ servers for authentication.
<code>group group-name</code>	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the <code>aaa group server radius</code> or <code>aaa group server tacacs+</code> 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](#)” section on page 28 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](#)” section on page 30 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)# <b>aaa new-model</b>	Enables AAA globally.
Step 2	Router(config)# <b>aaa authentication ppp</b> {default   list-name} method1 [method2...]	Creates a local authentication list.

	Command	Purpose
Step 3	Router(config)# <b>interface</b> <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)# <b>ppp authentication</b> { <i>protocol1</i> [ <i>protocol2</i> ...]} [ <b>if-needed</b> ] [ <b>default</b>   <i>list-name</i> ] [ <b>callin</b> ] [ <b>one-time</b> ][ <b>optional</b> ]	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
<b>if-needed</b>	Does not authenticate if user has already been authenticated on a TTY line.
<b>krb5</b>	Uses Kerberos 5 for authentication (can only be used for PAP authentication).
<b>local</b>	Uses the local username database for authentication.
<b>local-case</b>	Uses case-sensitive local username authentication.
<b>none</b>	Uses no authentication.
<b>group radius</b>	Uses the list of all RADIUS servers for authentication.

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

Keyword	Description
<b>group tacacs+</b>	Uses the list of all TACACS+ servers for authentication.
<b>group</b> <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the <b>aaa group server radius</b> or <b>aaa group server tacacs+</b> 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-Session-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)# <b>aaa processes</b> <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
<b>Step 1</b>	Router(config)# <b>aaa new-model</b>	Enables AAA globally.
<b>Step 2</b>	Router(config)# <b>aaa authentication arap</b> { <b>default</b>   <i>list-name</i> } <i>method1</i> [ <i>method2...</i> ]	Enables authentication for ARAP users.
<b>Step 3</b>	Router(config)# <b>line</b> <i>number</i>	(Optional) Changes to line configuration mode.
<b>Step 4</b>	Router(config-line)# <b>autoselect arap</b>	(Optional) Enables autoselection of ARAP.
<b>Step 5</b>	Router(config-line)# <b>autoselect during-login</b>	(Optional) Starts the ARAP session automatically at user login.
<b>Step 6</b>	Router(config-line)# <b>arap authentication</b> <i>list-name</i>	(Optional—not needed if <b>default</b> is used in the <b>aaa authentication arap</b> 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
<b>auth-guest</b>	Allows guest logins only if the user has already logged in to EXEC.
<b>guest</b>	Allows guest logins.
<b>line</b>	Uses the line password for authentication.
<b>local</b>	Uses the local username database for authentication.
<b>local-case</b>	Uses case-sensitive local username authentication.
<b>group radius</b>	Uses the list of all RADIUS servers for authentication.
<b>group tacacs+</b>	Uses the list of all TACACS+ servers for authentication.
<b>group</b> <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the <b>aaa group server radius</b> or <b>aaa group server tacacs+</b> 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 (NASl) 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)# <b>aaa new-model</b>	Enables AAA globally.
Step 2	Router(config)# <b>aaa authentication nasi</b> { <b>default</b>   <i>list-name</i> } <i>method1</i> [ <i>method2...</i> ]	Enables authentication for NASI users.
Step 3	Router(config)# <b>line</b> <i>number</i>	(Optional—not needed if <b>default</b> is used in the <b>aaa authentication nasi</b> command) Enters line configuration mode.
Step 4	Router(config-line)# <b>nasi authentication</b> <i>list-name</i>	(Optional—not needed if <b>default</b> is used in the <b>aaa authentication nasi</b> 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
<b>enable</b>	Uses the enable password for authentication.
<b>line</b>	Uses the line password for authentication.
<b>local</b>	Uses the local username database for authentication.
<b>local-case</b>	Uses case-sensitive local username authentication.
<b>none</b>	Uses no authentication.
<b>group radius</b>	Uses the list of all RADIUS servers for authentication.
<b>group tacacs+</b>	Uses the list of all TACACS+ servers for authentication.
<b>group</b> <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the <b>aaa group server radius</b> or <b>aaa group server tacacs+</b> 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)# <b>timeout login response</b> <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)# <b>aaa authentication enable default</b> <i>method1 [method2...]</i>	<p>Enables user ID and password checking for users requesting privileged EXEC level.</p> <p><b>Note</b> All <b>aaa authentication enable default</b> 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
<b>enable</b>	Uses the enable password for authentication.
<b>line</b>	Uses the line password for authentication.
<b>none</b>	Uses no authentication.
<b>group radius</b>	Uses the list of all RADIUS hosts for authentication. <b>Note</b> The RADIUS method does not work on a per-username basis.
<b>group tacacs+</b>	Uses the list of all TACACS+ hosts for authentication.
<b>group</b> <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the <b>aaa group server radius</b> or <b>aaa group server tacacs+</b> 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)# <b>aaa authentication password-prompt</b> <i>text-string</i>	Changes the default text displayed when a user is prompted to enter a password.

## Preventing an Access Request with a Blank Username from Being Sent to the RADIUS Server

The following configuration steps provide the ability to prevent an Access Request with a blank username from being sent to the RADIUS server. This functionality ensures that unnecessary RADIUS server interaction is avoided, and RADIUS logs are kept short.



### Note

The **aaa authentication suppress null-username** command is available only in Cisco IOS XE Release 2.4 and Cisco IOS Release 12.2(33)SRD.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication suppress null-username**

## 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)# configure terminal	Enables AAA globally.
Step 4	<b>aaa authentication suppress null-username</b>  <b>Example:</b> Router(config)# aaa authentication suppress null-username	Prevents an Access Request with a blank username from being sent to the RADIUS server.

## 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)# <b>aaa new-model</b>	Enables AAA.
Step 2	Router(config)# <b>aaa authentication banner</b> <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)# <b>aaa new-model</b>	Enables AAA.
Step 2	Router(config)# <b>aaa authentication fail-message</b> <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)# <b>aaa accounting network default</b> <i>start-stop radius</i>	Enables AAA accounting records.
Step 2	Router(config)# <b>aaa accounting delay-start</b>	(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)# <b>aaa pod server server-key</b> <i>string</i>	Enables POD reception.
Step 4	Router(config)# <b>radius-server host</b> <i>IP address</i> <b>non-standard</b>	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](#).

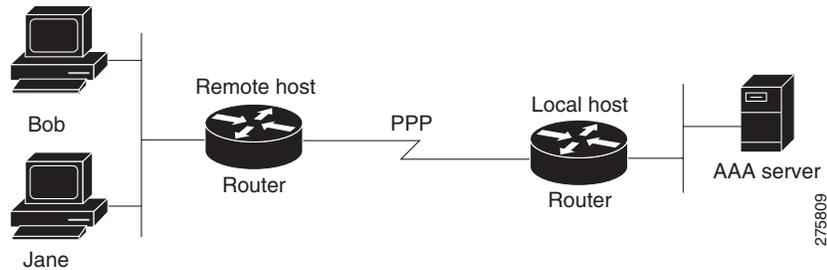
---

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> <b>access-profile</b> [ <b>merge</b>   <b>replace</b> ] [ <b>ignore-sanity-checks</b> ]	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 “[Authentication, Authorization, and Accounting \(AAA\)](#)” part of 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 <b>show ip trigger-authentication</b> command.)
Step 3	<code>Router# debug ip trigger-authentication</code>	Displays <b>debug</b> 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

This task is used to provide access control on a terminal line by entering the password and establishing password checking.

**Note**

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.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **line [aux | console | tty | vty] line-number [ending-line-number]**
4. **password password**
5. **login**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<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>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>line [aux   console   tty   vty] line-number [ending-line-number]</b>  <b>Example:</b> Router(config)# line console 0	Enters line configuration mode.
<b>Step 4</b>	<b>password password</b>  <b>Example:</b> Router(config-line)# secret word	Assigns a password to a terminal or other device on a line. 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.
<b>Step 5</b>	<b>login</b>  <b>Example:</b> Router(config-line)# login	Enables password checking at login.  You can disable line password verification by disabling password checking by using the <b>no</b> version of this command.  <b>Note</b> The <b>login</b> 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.
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
<code>Router(config-if)# ppp authentication {protocol1 [protocol2...]} [if-needed] {default   list-name} [callin] [one-time]</code>	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 <i>username</i> password <i>password</i></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	<code>Router(config-if)# encapsulation ppp</code>	Enables PPP encapsulation.
Step 2	<code>Router(config-if)# ppp authentication ms-chap [if-needed] [list-name   default] [callin] [one-time]</code>	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-Session-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=10.0.0.0 255.0.0.0",
      cisco-avpair = "ip:route#6=10.10.0.0 255.0.0.0",
      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"

```

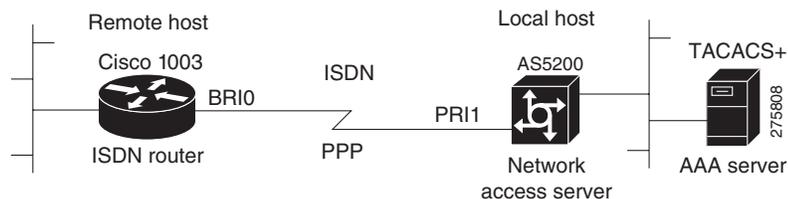
## Complete Configuration with TACACS+ Example

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="10.0.0.0 255.0.0.0"
    route#6="10.10.0.0 255.0.0.0"
}

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 172.16.2.75
! **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.

## Additional References

The following sections provide references related to the Configuring Authentication feature.

### Related Documents

Related Topic	Document Title
Authorization	<a href="#">Configuring Authorization</a>
Accounting	<a href="#">Configuring Accounting</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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### RFCs

RFC	Title
RFC 2903	Generic AAA Architecture
RFC 2904	AAA Authorization Framework
RFC 2906	AAA Authorization Requirements
RFC 2989	Criteria for Evaluating AAA Protocols for Network Access

## 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 Configuring Authentication

Table 10 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.

For information on a feature in this technology that is not documented here, see the [Select Your Product](#) page to find product documentation support for your Cisco IOS release.

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 10 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 10** Feature Information for Configuring Authentication

Feature Name	Releases	Feature Information
Authentication	12.0	The Authentication feature was introduced in the Cisco IOS Release 12.0 software.
Authentication	XE 2.1	The Authentication feature was introduced in the Cisco IOS Release XE 2.1 software.
RADIUS - CLI to Prevent Sending of Access Request with a Blank Username	12.2(33)SRD Cisco IOS XE Release 2.4	<p>This Authentication feature prevents an Access Request with a blank username from being sent to the RADIUS server. This functionality ensures that unnecessary RADIUS server interaction is avoided, and RADIUS logs are kept short.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> <li><a href="#">Preventing an Access Request with a Blank Username from Being Sent to the RADIUS Server, page 21</a></li> </ul> <p>The following command was introduced: <b>aaa authentication suppress null-username.</b></p>

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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.

© 1998–2009 Cisco Systems, Inc. All rights reserved.





# AAA Double Authentication Secured by Absolute Timeout

---

**First Published: March 1, 2004**  
**Last Updated: May 4, 2009**

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

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 AAA Double Authentication Secured by Absolute Timeout” section on page 11](#).

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 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 3](#)
- [Examples for AAA Double Authentication Secured by Absolute Timeout, page 5](#)
- [Additional References, page 8](#)



---

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

© 2004–2009 Cisco Systems, Inc. All rights reserved.

- [Feature Information for AAA Double Authentication Secured by Absolute Timeout, page 11](#)

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

## 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  aacon2 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 = "password1",
  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 = "password1",
  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 = "password1",
  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 = "password1",
  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 autocmd 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 autocmd 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 <i>Cisco IOS Security Configuration Guide</i> , Release 12.4
Enabling AAA Double Authentication	“Configuring Authentication” chapter of the “Authentication, Authorization, and Accounting” section of the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4
Configuring RADIUS	“Configuring RADIUS” chapter of the “Security Server Protocols” section of the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4
Configuring TACACS+	“Configuring TACACS+” chapter of the “Security Server Protocols” section of the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4
Security Commands	<i>Cisco IOS Security Command Reference</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: <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>

# 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, Catalyst OS, and Cisco IOS XE 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 Cisco IOS XE Release 2.3	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.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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.

© 2004–2009 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	<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>username name [privilege level] password</b> <i>encryption-type password</i>  <b>Example:</b> Router (config)# username user1 privilege 15 password 0 cisco	Establishes a username-based authentication system.
Step 4	<b>aaa new-model</b>  <b>Example:</b> Router (config)# aaa new-model	Enables the AAA access control model.
Step 5	<b>aaa local authentication attempts max-fail</b> <i>number-of-unsuccessful-attempts</i>  <b>Example:</b> Router (config)# aaa local authentication attempts max-fail 3	Specifies the maximum number of unsuccessful attempts before a user is locked out.
Step 6	<b>aaa authentication login default method</b>  <b>Example:</b> 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

- enable
- clear aaa local user logout {username *username* | 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 aaa local user lockout {username username   all}</b>  <b>Example:</b> 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	<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 aaa local user fail-attempts {username username   all}</b>  <b>Example:</b> Router# clear aaa local user fail-attempts username user1	Clears the unsuccessful attempts of the user. <ul style="list-style-type: none"><li>• This command is useful for cases in which the user configuration was changed and the unsuccessful attempts that are already logged must be cleared.</li></ul>

## 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	<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 aaa local user locked</b>  <b>Example:</b> 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	<a href="#">Cisco IOS Security Command Reference, Release 12.3T</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: <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
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*.

- **aaa local authentication attempts max-fail**
- **clear aaa local user fail-attempts**
- **clear aaa local user lockout**

## 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 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.





## 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	<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>radius-server vsa send authentication</b>  <b>Example:</b> Router(config)# radius-server vsa send authentication	Configures the NAS to recognize and use vendor-specific attributes.
Step 4	<b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface FastEthernet 0/1	Configures an interface type and enters interface configuration mode.
Step 5	<b>ppp max-bad-auth</b> <i>number</i>  <b>Example:</b> 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"> <li>The default value for the <i>number</i> argument is 0 seconds (immediately).</li> <li>The range is between 0 and 255.</li> </ul>  <b>Note</b> 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.
Step 6	<b>ppp authentication ms-chap-v2</b>  <b>Example:</b> Router(config-if)# ppp authentication ms-chap-v2	Enables MSCHAP V2 authentication on a NAS.
Step 7	<b>end</b>  <b>Example:</b> 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	<code>show running-config interface type number</code>  <b>Example:</b> Router# show running-config interface Asynch65	Verifies the configuration of MSCHAP V2 as the authentication method for the specified interface.
Step 2	<code>debug ppp negotiation</code>  <b>Example:</b> Router# debug ppp negotiation	Verifies successful MSCHAP V2 negotiation.
Step 3	<code>debug ppp authentication</code>  <b>Example:</b> 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	<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 globally.
Step 4	<b>aaa authentication login</b> {default   list-name} <b>passwd-expiry</b> method1 [method2...]  <b>Example:</b> Router(config)# aaa authentication login userauthen passwd-expiry group radius	Enables password aging for crypto-based clients on a local authentication list.
Step 5	<b>crypto map</b> map-name <b>client authentication list</b> list-name  <b>Example:</b> 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:  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## 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.	<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 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 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 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)# <b>ppp authentication eap</b>	Enables EAP as the authentication protocol.
Router(config-if)# <b>ppp eap identity</b> <i>string</i>	(Optional) Specifies the EAP identity when requested by the peer.
Router(config-if)# <b>ppp eap password</b> [ <i>number</i> ] <i>string</i>	(Optional) Sets the EAP password for peer authentication. <b>Note</b> This command should only be configured on the client.
Router(config-if)# <b>ppp eap local</b>	(Optional) Authenticates locally instead of using a RADIUS back-end server, which is the default. <b>Note</b> This command should only be configured on the NAS.

Command	Purpose
Router(config-if)# <b>ppp eap wait</b>	(Optional) Waits for the caller to authenticate itself first. By default, the client always authenticates itself before the caller does. <b>Note</b> This command should only be configured on the NAS.
Router(config-if)# <b>ppp eap refuse</b> [ <b>callin</b> ]	(Optional) Refuses to authenticate using EAP. If the <b>callin</b> keyword is enabled, only incoming calls will not be authenticated. <b>Note</b> 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# <b>show users</b>	Displays information about the active lines on the router.
Router# <b>show interfaces</b>	Displays statistics for all interfaces configured on the router or access server.
Router# <b>show running-config</b>	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  
  password 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## 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.	<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*.

- **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 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 Packet of Disconnect

---

**First Published: March 19, 2001**

**Last Updated: January 6, 2009**

The RADIUS Packet of Disconnect feature is used to terminate a connected voice call.

## 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 RADIUS Packet of Disconnect” section on page 9](#).

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 RADIUS Packet of Disconnect, page 2](#)
- [Restrictions for RADIUS Packet of Disconnect, page 2](#)
- [Information About RADIUS Packet of Disconnect, page 2](#)
- [How to Configure the RADIUS Packet of Disconnect, page 3](#)
- [Additional References, page 7](#)
- [Command Reference, page 8](#)
- [Feature Information for RADIUS Packet of Disconnect, page 9](#)
- [Glossary, page 10](#)



---

**Americas Headquarters:**

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

## Prerequisites for RADIUS Packet of Disconnect

- Configure AAA as described in *Cisco IOS Security Configuration Guide*, Release 12.4T.
- Use Cisco IOS Release 12.2(11)T or later.

## RADIUS Packet of Disconnect Platform Support

The following platforms are supported for the RADIUS Packet of Disconnect feature:

- Cisco 3600 series
- Cisco AS5300
- Cisco AS5350
- Cisco AS5400
- Cisco AS5800
- Cisco AS5850

## Restrictions for RADIUS Packet of Disconnect

Proper matching identification information must be communicated by the following:

- Billing server and gateway configuration
- Gateway's original accounting start request
- Server's POD request

## Information About RADIUS Packet of Disconnect

The 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.

## When the POD is Needed

The POD 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.

## POD Parameters

The POD has the following parameters:

- 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.
- Cisco allocated POD code 50 as the new code value for the Voice POD Request in Cisco IOS Release 12.2(27)SB and 12.4(15)T. This change was made because RFC 3576 *Dynamic Authorization Extensions to RADIUS* recently extended RADIUS standards to officially support both a Disconnect Message (DM) and Change-of-Authorization (CoA), which is supported through the POD.

RFC 3576 specifies the following POD codes:

- 40 - Disconnect-Request
- 41 - Disconnect-ACK
- 42 - Disconnect-NAK
- 43 - CoA-Request
- 44 - CoA-ACK
- 45 - CoA-NAK

## How to Configure the RADIUS Packet of Disconnect

Use the following section to configure the RADIUS Packet of Disconnect feature.

- [Configuring the RADIUS POD](#)

### Configuring the RADIUS POD

Use the following tasks to configure the RADIUS POD:

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa pod server** [**port** *port-number*] [**auth-type** { **any** | **all** | **session-key** }] **server-key** [*encryption-type*] *string*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>Router(config)# <b>aaa pod server</b> [<b>port</b> <i>port-number</i>] [<b>auth-type</b> {<b>any</b>   <b>all</b>   <b>session-key</b>}] <b>server-key</b> [<i>encryption-type</i>] <i>string</i></p> <p><b>Example:</b> Router(config)# aaa pod server server-key xyz123</p>	<p>Enables inbound user sessions to be disconnected when specific session attributes are presented.</p> <p><b>port</b> <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><b>auth-type</b>—(Optional) The type of authorization required for disconnecting sessions.</p> <p><b>any</b>—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><b>all</b>—Only a session that matches all four key attributes is disconnected. <b>All</b> is the default.</p> <p><b>session-key</b>—Session with a matching session-key attribute is disconnected. All other attributes are ignored.</p> <p><b>server-key</b>—Configures the shared-secret text string.</p> <p><i>encryption-type</i>—(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>

	Command or Action	Purpose
Step 4	Router# <code>exit</code>	Exits global configuration mode.
Step 5	Router# <code>show running-configuration</code>  <b>Example:</b> Router# <code>show running-configuration</code> ! 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 !	Verifies that the gateway is configured correctly in privileged EXEC mode.

## Troubleshooting Tips

Use the following tips to troubleshoot POD issues:

- 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
```

## ■ How to Configure the RADIUS Packet of Disconnect

```
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:
```

# Additional References

The following sections provide references related to the <<Feature Name>> feature.

## Related Documents

Related Topic	Document Title
AAA	<i>Cisco IOS Security Configuration Guide</i> , Release 12.4T
Security commands	<i>Cisco IOS Security Command Reference</i> , Release 12.4T
CLI Configuration	<i>Cisco IOS Configuration Fundamentals Configuration Guide</i> , Release 12.4T
Configuring AAA for voice gateways	<i>Configuring AAA for Cisco Voice Gateways</i> , Release 12.4T

## 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
RFC 2865	<i>Remote Authentication Dial-in User Service</i>
RFC 3576	<i>Dynamic Authorization Extensions to RADIUS</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><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 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 pod server**
- **debug aaa pod**

# Feature Information for RADIUS Packet of Disconnect

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 Packet of Disconnect

Feature Name	Releases	Feature Information
RADIUS Packet of Disconnect	12.2(2)XB 12.1(2)XH 12.3(11)T XE Release 2.1 12.2(27)SB 12.4(15)T	<p>The RADIUS Packet of Disconnect feature is used to terminate a connected voice call.</p> <p>In Cisco IOS Release 12.2(2)XB, this feature was introduced on the Cisco 3600, Cisco 5350, and Cisco 5400.</p> <p>In Cisco IOS Release 12.1(2)XH and 12.1(3)T, this feature was introduced on the Cisco 5300 and Cisco 5800.</p> <p>In Cisco IOS Release 12.2(11)T, this feature was introduced on the Cisco 5400, Cisco 5850</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the on Cisco ASR 1000 Series Routers.</p> <p>In Cisco IOS Release 12.2(27)SB and 12.4(15)T, Cisco allocated POD code 50 as the new code value for the voice POD request</p> <p>The following commands were introduced or modified: <b>aaa pod server</b> and <b>debug aaa pod</b></p>

# 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.

---

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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.



## **Authorization**





# 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:

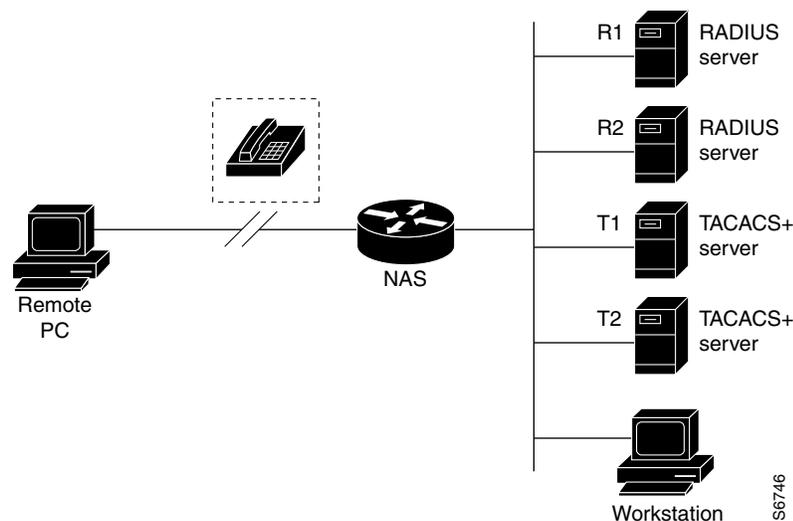
- **TACACS+**—The network access server exchanges authorization information with the TACACS+ security daemon. TACACS+ authorization defines specific rights for users by associating attribute-value pairs, which are stored in a database on the TACACS+ security server, with the appropriate user.

- **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)# <b>aaa authorization</b> { <b>auth-proxy</b>   <b>network</b>   <b>exec</b>   <b>commands</b> <i>level</i>   <b>reverse-access</b>   <b>configuration</b>   <b>ipmobile</b> } { <b>default</b>   <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)# <b>line</b> [ <b>aux</b>   <b>console</b>   <b>tty</b>   <b>vty</b> ] <i>line-number</i> [ <i>ending-line-number</i> ]  or  Router(config)# <b>interface</b> <i>interface-type</i> <i>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)# <b>authorization</b> { <b>arap</b>   <b>commands</b> <i>level</i>   <b>exec</b>   <b>reverse-access</b> } { <b>default</b>   <i>list-name</i> }  or Router(config-line)# <b>ppp authorization</b> { <b>default</b>   <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)# <b>no aaa authorization config-commands</b>	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
<pre>Router(config)# <b>aaa authorization reverse-access</b> method1 [method2 ...]</pre>	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.”

---

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.





## **Accounting**





# Configuring Accounting

---

**First Published: October 26, 1998**

**Last Updated: June 25, 2009**

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

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 Configuring Accounting”](#) section on page 30.

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 Configuring Accounting, page 2](#)
- [Restrictions for Configuring Accounting, page 2](#)
- [Information About Configuring Accounting, page 2](#)
- [How to Configure AAA Accounting, page 16](#)
- [Configuration Examples for AAA Accounting, page 23](#)
- [Additional References, page 28](#)
- [Feature Information for Configuring Accounting, page 30](#)



---

**Americas Headquarters:**

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

## 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 a Cisco router or access server, see the chapter “[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 the chapter “[Configuring RADIUS](#).” For more information about configuring the Cisco network access server to communicate with the TACACS+ security server, see the chapter “[Configuring TACACS+](#).”

## 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 the Accounting feature is implemented:

- [Named Method Lists for Accounting, page 2](#)
- [AAA Accounting Types, page 5](#)
- [AAA Accounting Enhancements, page 14](#)
- [Accounting Attribute-Value Pairs, page 15](#)

## 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.

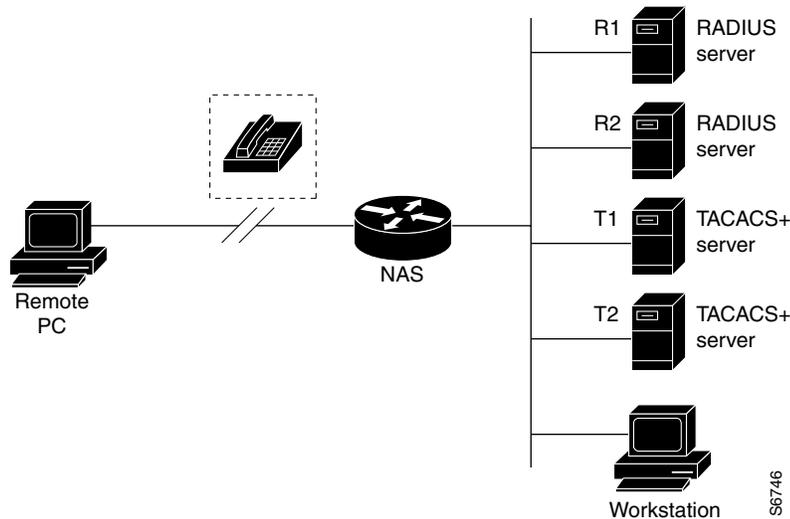
This section includes the following subsections:

- [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, page 5](#)
- [Connection Accounting, page 7](#)
- [EXEC Accounting, page 9](#)
- [System Accounting, page 11](#)
- [Command Accounting, page 11](#)
- [Resource Accounting, page 12](#)

## 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 chapter “[Configuring IP Services](#)” in the *Cisco IOS Application Services 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 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.

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*

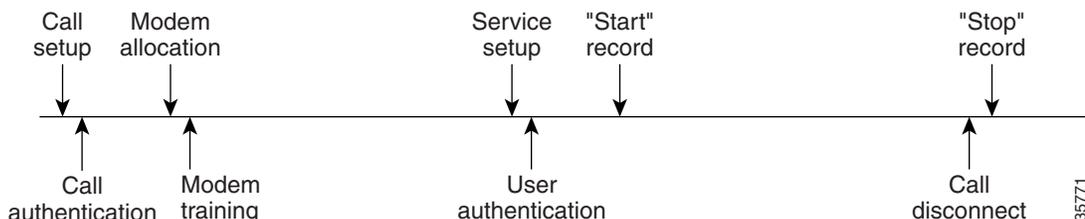


Figure 3 illustrates a call setup sequence with normal call flow (no disconnect) and with AAA resource failure stop accounting enabled.

**Figure 3** *Modem Dial-In Call Setup Sequence With Normal Flow and With Resource Failure Stop Accounting Enabled*

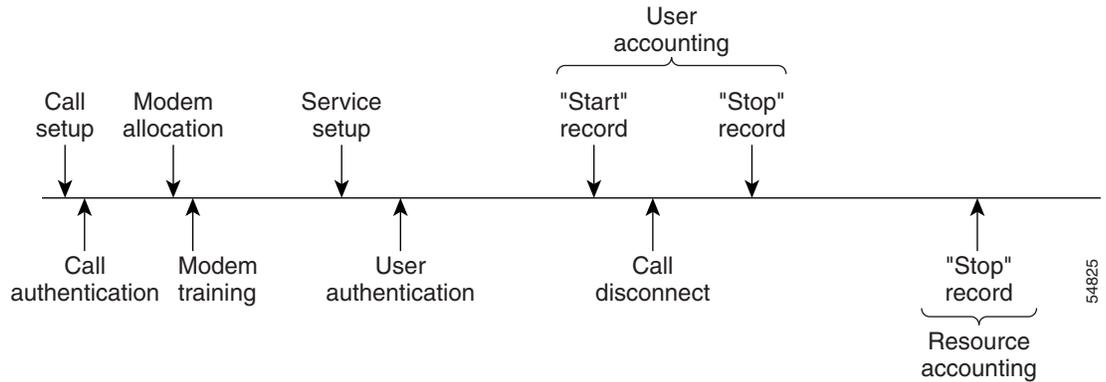


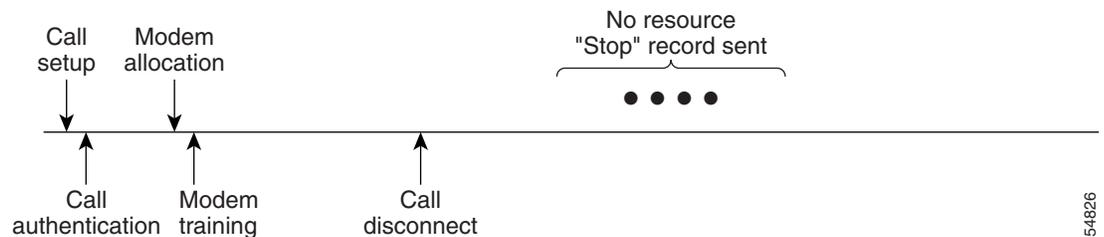
Figure 4 illustrates a call setup sequence with call disconnect occurring before user authentication and with AAA resource failure stop accounting enabled.

**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*



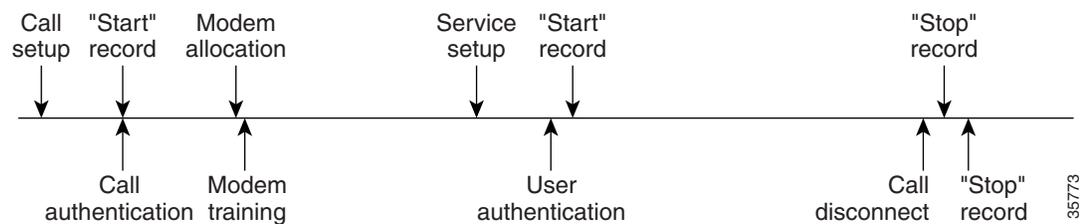
## AAA Resource Accounting for Start-Stop Records

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.

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 14](#)

### 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 11 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 11** *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 12 describes the AAA summary information provided by the AAA session MIB feature using SNMP on a per-system basis.

**Table 12** *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.

## 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.

# How to Configure AAA Accounting

This section describes the following configuration tasks involved in configuring AAA Accounting:

- [Configuring AAA Accounting Using Named Method Lists, page 16](#)
- [Suppressing Generation of Accounting Records for Null Username Sessions, page 19](#)
- [Generating Interim Accounting Records, page 19](#)
- [Generating Accounting Records for Failed Login or Session, page 19](#)
- [Specifying Accounting NETWORK-Stop Records Before EXEC-Stop Records, page 20](#)
- [Configuring AAA Resource Failure Stop Accounting, page 20](#)
- [Configuring AAA Resource Accounting for Start-Stop Records, page 21](#)
- [Configuring AAA Broadcast Accounting, page 21](#)
- [Configuring Per-DNIS AAA Broadcast Accounting, page 21](#)
- [Configuring AAA Session MIB, page 22](#)
- [Establishing a Session with a Router if the AAA Server is Unreachable, page 22](#)
- [Monitoring Accounting, page 23](#)
- [Troubleshooting Accounting, page 23](#)

## 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
<b>Step 1</b>	Router(config)# <b>aaa accounting</b> { <b>system</b>   <b>network</b>   <b>exec</b>   <b>connection</b>   <b>commands level</b> } { <b>default</b>   <i>list-name</i> } { <b>start-stop</b>   <b>stop-only</b>   <b>none</b> } [ <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.
<b>Step 2</b>	Router(config)# <b>line</b> [ <b>aux</b>   <b>console</b>   <b>tty</b>   <b>vty</b> ] <i>line-number</i> [ <i>ending-line-number</i> ]  or  Router(config)# <b>interface</b> <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.
<b>Step 3</b>	Router(config-line)# <b>accounting</b> { <b>arap</b>   <b>commands level</b>   <b>connection</b>   <b>exec</b> } { <b>default</b>   <i>list-name</i> }  or  Router(config-if)# <b>ppp accounting</b> { <b>default</b>   <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 13](#) lists the supported accounting methods.

**Table 13**      *AAA Accounting Methods*

Keyword	Description
<b>group radius</b>	Uses the list of all RADIUS servers for accounting.
<b>group tacacs+</b>	Uses the list of all TACACS+ servers for accounting.
<b>group <i>group-name</i></b>	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.
- **group radius**—To have the network access server send accounting information to a RADIUS security server, use the **group radius method** keyword.



**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.

## 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)# <b>aaa accounting suppress null-username</b>	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)# <b>aaa accounting update</b> {[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)# <b>aaa accounting send stop-record authentication failure</b>	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)# <b>aaa accounting nested</b>	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)# <b>aaa accounting resource</b> <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><b>Note</b> Before configuring this feature, the tasks described in the section <a href="#">“Prerequisites for Configuring Accounting”</a> 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 the chapter <a href="#">“Configuring SNMP Support”</a> in the <i>Cisco IOS Network Management 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
<pre>Router(config)# <b>aaa accounting resource</b> method-list <b>start-stop group server-group</b></pre>	<p>Supports the ability to send a “start” record at each call setup, followed with a corresponding “stop” record at the call disconnect.</p> <p><b>Note</b> Before configuring this feature, the tasks described in the section “<a href="#">Prerequisites for Configuring Accounting</a>” 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 the chapter “<a href="#">Configuring SNMP Support</a>” in the <i>Cisco IOS Network Management Configuration Guide</i>.</p>

## 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
<pre>Router(config)# <b>aaa accounting</b> {<b>system</b>   <b>network</b>   <b>exec</b>   <b>connection</b>   <b>commands level</b>} {<b>default</b>   <b>list-name</b>} {<b>start-stop</b>   <b>stop-only</b>   <b>none</b>} [<b>broadcast</b>] <b>method1</b> [<b>method2...</b>]</pre>	<p>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.</p>

## 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
<pre>Router(config)# <b>aaa dnis map dnis-number accounting network</b> [<b>start-stop</b>   <b>stop-only</b>   <b>none</b>] [<b>broadcast</b>] <b>method1</b> [<b>method2...</b>]</pre>	<p>Allows per-DNIS accounting configuration. This command has precedence over the global <b>aaa accounting</b> command.</p> <p>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.</p>

## Configuring AAA Session MIB

The following tasks must be performed before configuring the AAA session MIB feature:

- Configure SNMP. For information on SNMP, see the chapter “[Configuring SNMP Support](#)” in the *Cisco IOS Network Management 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)# <b>aaa session-mib disconnect</b>	Monitors and terminates authenticated client connections using SNMP.  To terminate the call, the <b>disconnect</b> 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)# <b>no aaa accounting system guarantee-first</b>	The <b>aaa accounting system guarantee-first</b> 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 <b>no aaa accounting system guarantee-first</b> 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# <b>show accounting</b>	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# <b>debug aaa accounting</b>	Displays information on accountable events as they occur.

## Configuration Examples for AAA Accounting

This section contains the following examples:

- [Configuring Named Method List: Example, page 24](#)
- [Configuring AAA Resource Accounting: Example, page 26](#)
- [Configuring AAA Broadcast Accounting: Example, page 26](#)
- [Configuring Per-DNIS AAA Broadcast Accounting: Example, page 27](#)
- [AAA Session MIB: Example, page 27](#)

## 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 14 describes the fields contained in the preceding output.

**Table 14** *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
```

# Additional References

The following sections provide references related to the Configuring Accounting feature.

## Related Documents

Related Topic	Document Title
Authorization	<a href="#">“Configuring Authorization”</a>
Authentication	<a href="#">“Configuring Authentication”</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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
RFC 2903	Generic AAA Architecture
RFC 2904	AAA Authorization Framework
RFC 2906	AAA Authorization Requirements
RFC 2989	Criteria for Evaluating AAA Protocols for Network Access

## 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 Configuring Accounting

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 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 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 Configuring Accounting

Feature Name	Releases	Feature Information
—	Cisco IOS	For information about feature support in Cisco IOS software, use Cisco Feature Navigator.
Connection Accounting	Cisco IOS XE Release 2.1	This feature was introduced on the Cisco ASR 1000 series routers. Refer to <a href="#">Connection Accounting, page 7</a> for more information.
AAA Session MIB	Cisco IOS XE Release 2.1	This feature was introduced on the Cisco ASR 1000 series routers. Refer to <a href="#">Configuring AAA Session MIB, page 22</a> for more information.
AAA Broadcast Accounting	Cisco IOS XE Release 2.2	This feature was introduced on the Cisco ASR 1000 series routers. Refer to <a href="#">Configuring AAA Broadcast Accounting, page 21</a> for more information.
AAA Interim Accounting	Cisco IOS XE Release 2.4	This feature was introduced on the Cisco ASR 1000 series routers. Refer to <a href="#">Generating Interim Accounting Records, page 19</a> for more information.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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.

© 1998—2009 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:

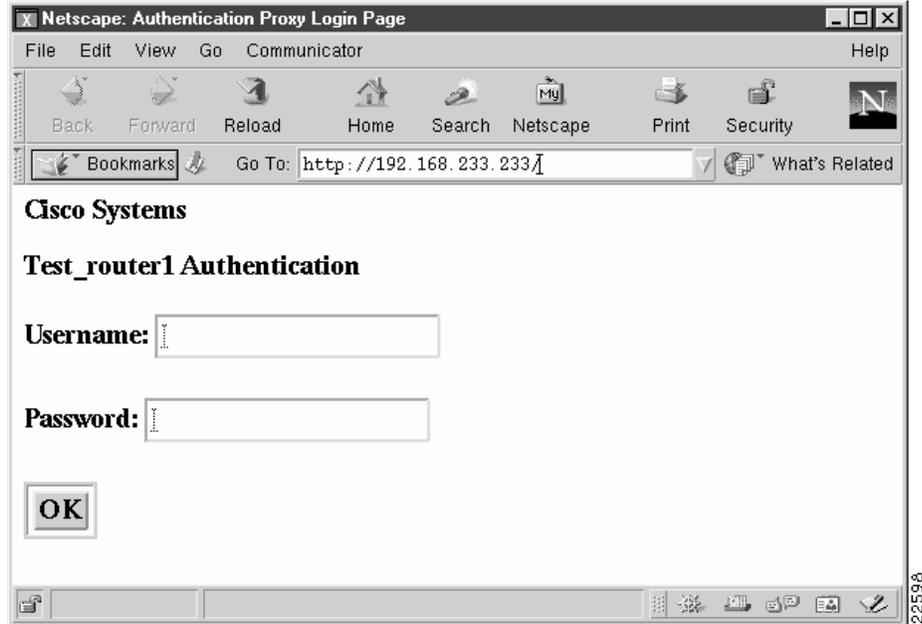
- [How the Authentication Proxy Works](#)
- [Secure Authentication](#)
- [Using the Authentication Proxy](#)
- [When to Use the Authentication Proxy](#)
- [Applying the Authentication Proxy](#)
- [Operation with One-Time Passwords](#)
- [Compatibility with Other Security Features](#)
- [Compatibility 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.

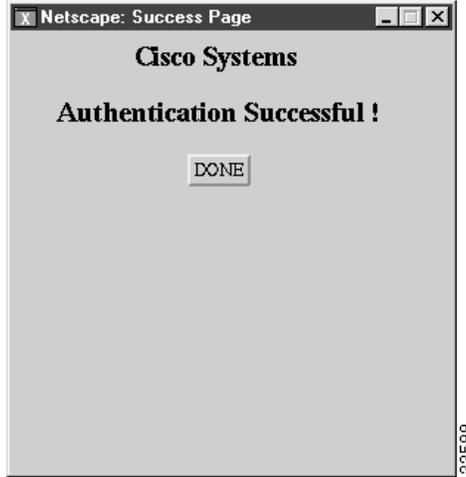
If the authentication fails, the authentication proxy reports the failure to the user and prompts the user with multiple retries. If the user fails to authenticate after five attempts, the user must wait two minutes and initiate another HTTP session to trigger authentication proxy.

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:

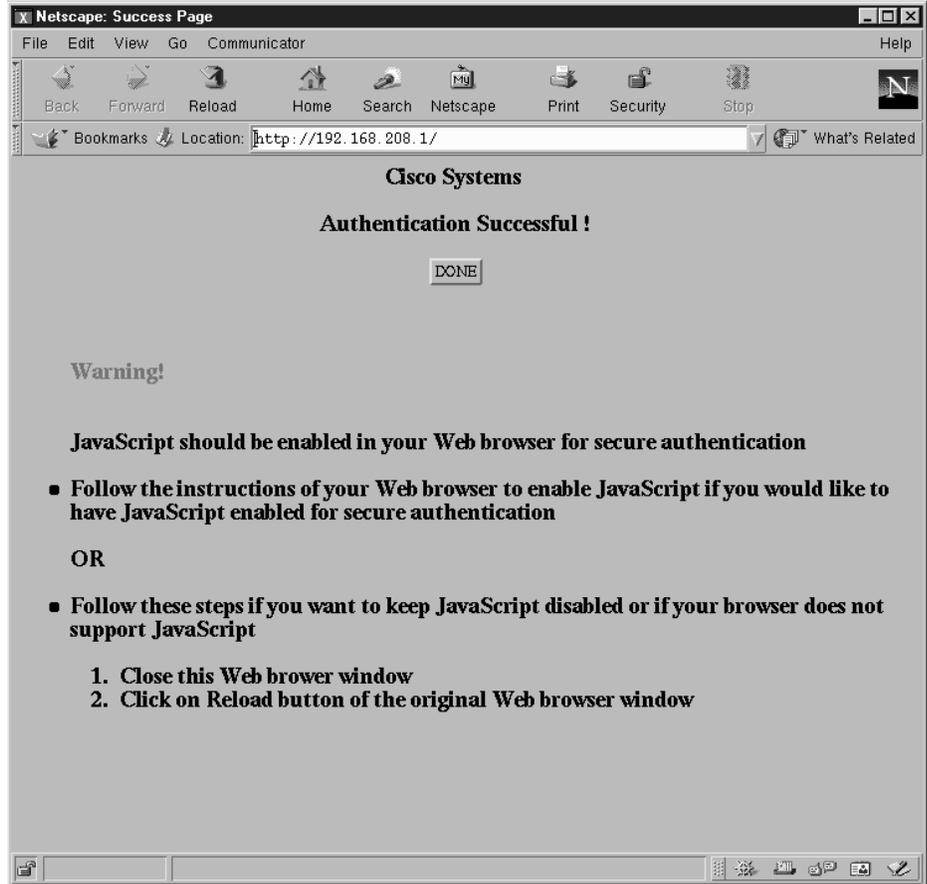
- [Operation with JavaScript](#)
- [Operation Without JavaScript](#)

### 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**

<b>Authentication Proxy Action with Client</b>	<b>Description</b>
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. <a href="#">Figure 42</a> 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 <a href="#">Figure 43</a>. 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 <a href="#">Figure 44</a>.</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

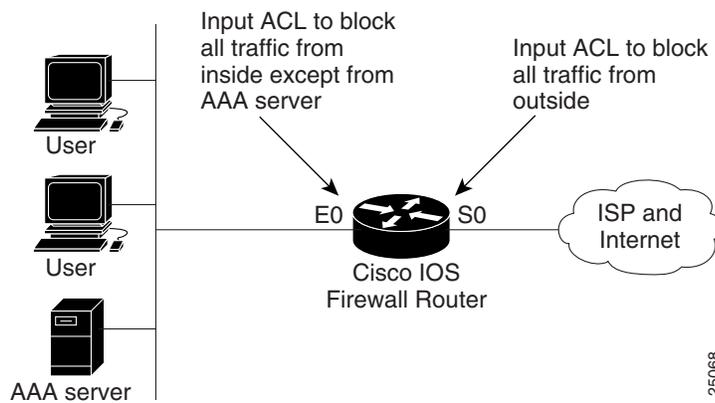
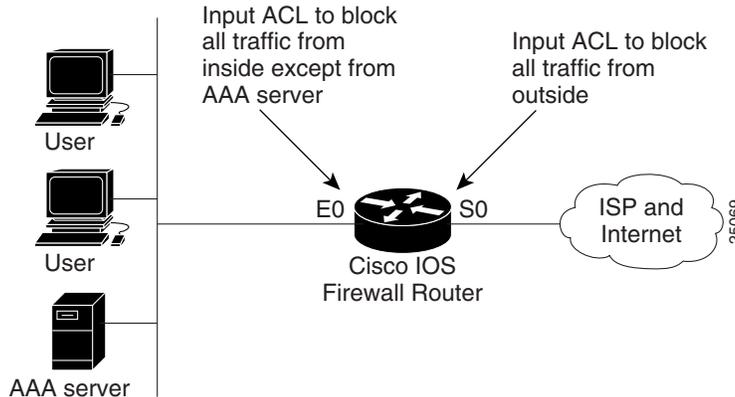


Figure 46 shows the authentication proxy applied at the dial-in interface with all network traffic blocked at each interface.

**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 <b>auth-proxy</b> 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 <b>auth-proxy</b> 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 <b>radius server host</b> 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 <b>radius server key</b> 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 <a href="#">“Interface Configuration Example.”</a>

## 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 <b>auth-cache-time</b> 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 <b>ip auth-proxy auth-cache-time</b> command.</p> <p>(Optional) The <b>list</b> 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# <b>show ip auth-proxy configuration</b>	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# <b>show ip auth-proxy cache</b>	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# <b>show ip access-lists</b>	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# <b>clear ip auth-proxy cache</b> {*   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
```

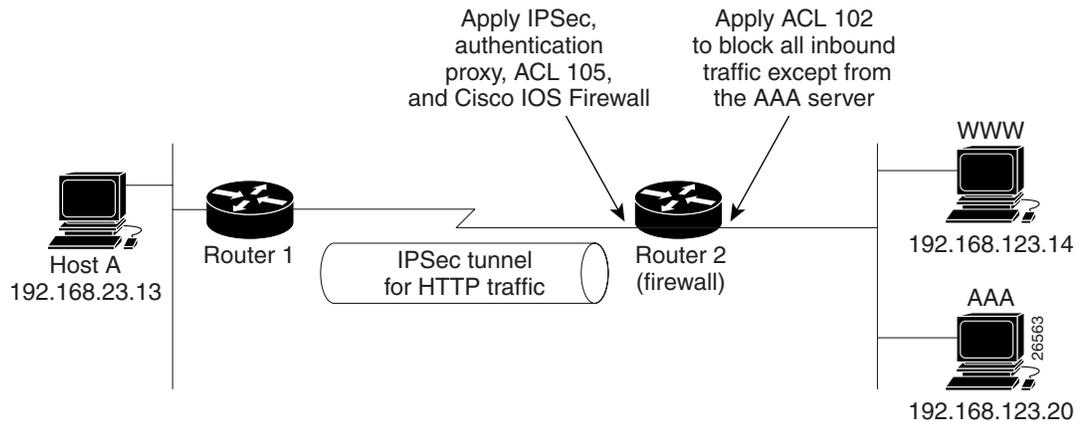
## Authentication Proxy, IPSec, and CBAC Configuration Example

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

```

```

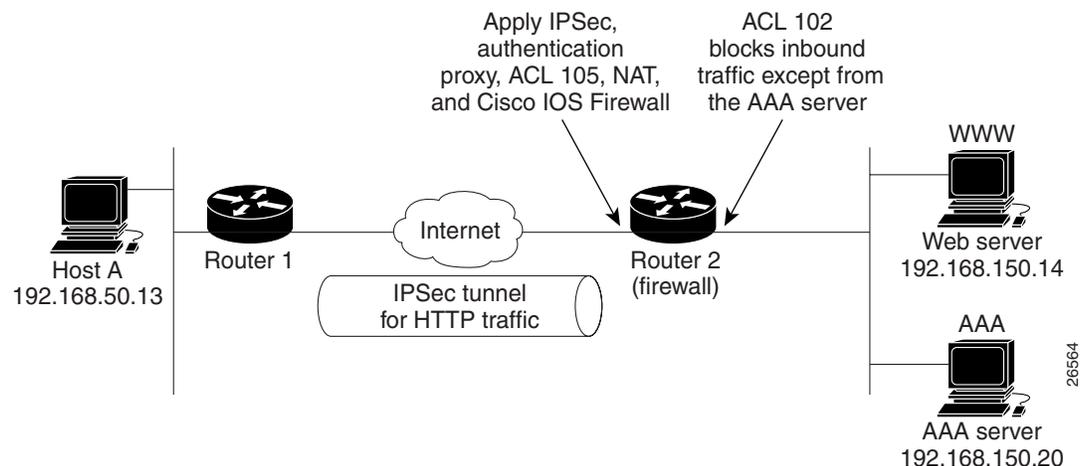
!
! Define the AAA server host and encryption key.
tacacs-server host 192.168.123.14
tacacs-server key cisco
!
line con 0
  exec-timeout 0 0
  login authentication special
  transport input none
line aux 0
  transport input all
  speed 38400
  flowcontrol hardware
line vty 0 4
  password lab

```

## 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)**.
- Scroll down to New Services.
  - Add a new service, “auth-proxy”, in the Service field. Leave the Protocol field empty.
  - Select both the User and Group check boxes for the new service.
  - Scroll down to Advance Configuration Options and check the Per-user Advance TACACS+ features.
  - Click **Submit**.
- Step 2** Click the Network Configuration icon.
- 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.
  - Select TACACS+ (Cisco) for the Authenticate Using option.
  - Click the Submit + Restart icon.
- Step 3** Click the Group Setup icon.
- Select a user group from the drop-down menu.
  - Select the Users in Group check box.
  - Select a user from the user list.
  - In the User Setup list, scroll down to TACACS+ Settings and select the “auth-proxy” check box.
  - Select the Custom Attributes check box.
  - 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.



# 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.

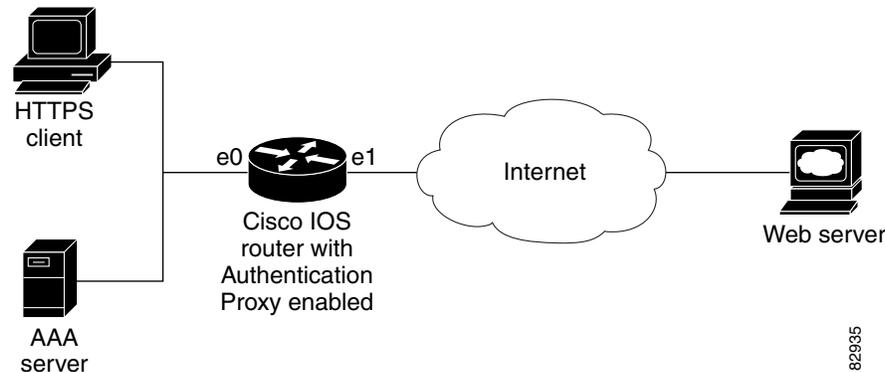
When authentication proxy is enabled on a Cisco router, users can log into the network or access the Internet via HTTP(S). When a user initiates an HTTP(S) session through the firewall, the authentication proxy is triggered. Authentication proxy first checks to see if the user has been authenticated. 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	<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 the router. <ul style="list-style-type: none"> <li>The authentication proxy uses the HTTP server to communicate with the client for user authentication.</li> </ul>
Step 4	<b>ip http authentication aaa</b> Router (config)# ip http authentication aaa	Sets the HTTP server authentication method to AAA.
Step 5	<b>ip http secure-server</b>  <b>Example:</b> Router (config)# ip http secure-server	Enables HTTPS.
Step 6	<b>ip http secure-trustpoint name</b>  <b>Example:</b> 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

- enable
- show ip auth-proxy configuration
- show ip auth-proxy cache
- show ip http server secure status

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<code>show ip auth-proxy configuration</code>  <b>Example:</b> Router# show ip auth-proxy configuration	Displays the current authentication proxy configuration.
<b>Step 3</b>	<code>show ip auth-proxy cache</code>  <b>Example:</b> 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.
<b>Step 4</b>	<code>show ip http server secure status</code>  <b>Example:</b> 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**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<code>enable</code>  <b>Example:</b> 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>Example:</b> <code>debug ip auth-proxy detailed</code>  <b>Example:</b> 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 55A47951000000000000D
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 DEEBE73E 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:  <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 <sup>1</sup>	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.	<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*.

# 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 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 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

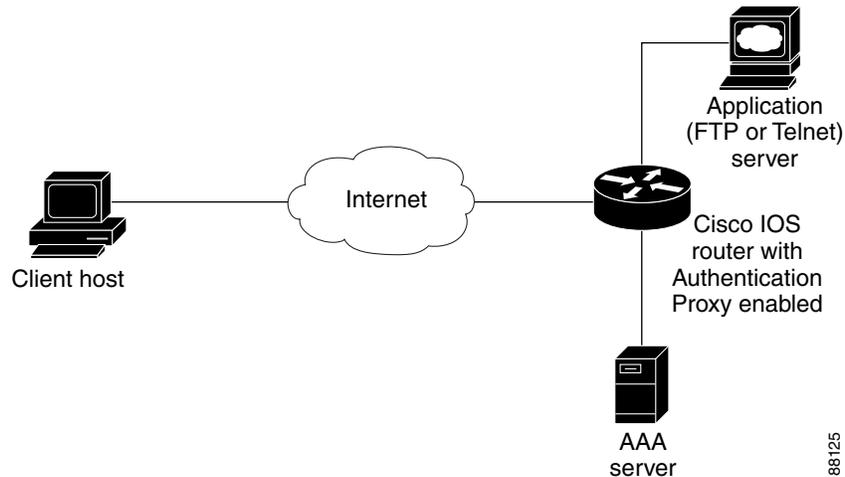
Authentication proxy for FTP and Telnet Sessions functions like authentication proxy for HTTP; that is, FTP and Telnet are independent components in the Cisco IOS software and can be enabled or disabled on the interface of an unauthenticated host.

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



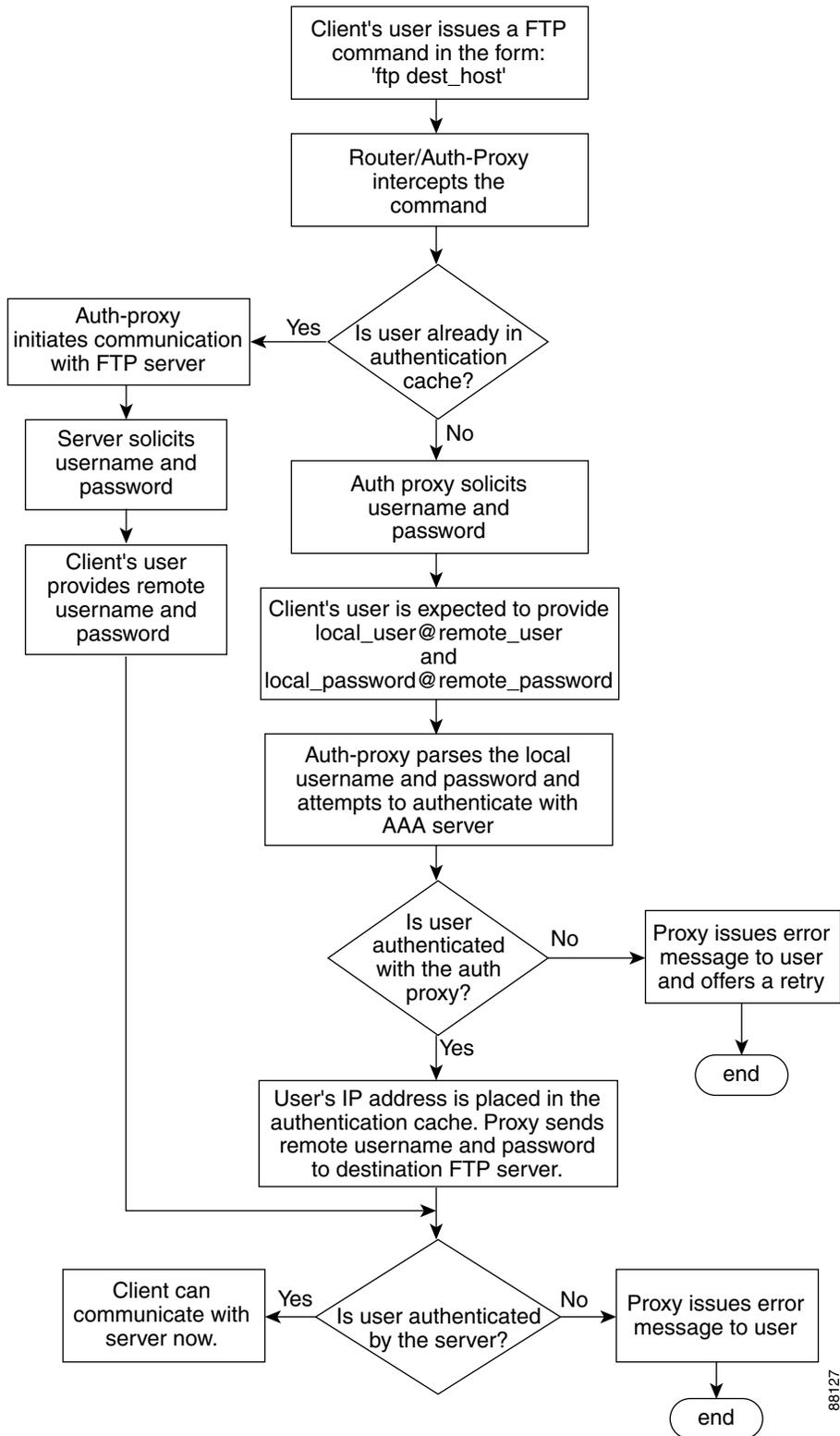
Just as with HTTP, the authentication proxy router intercepts traffic that is sent from the client host. Upon receiving a FTP or Telnet packet, the router will look into its authentication cache to check whether the client host has already been authenticated. If it has been authenticated, the router 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



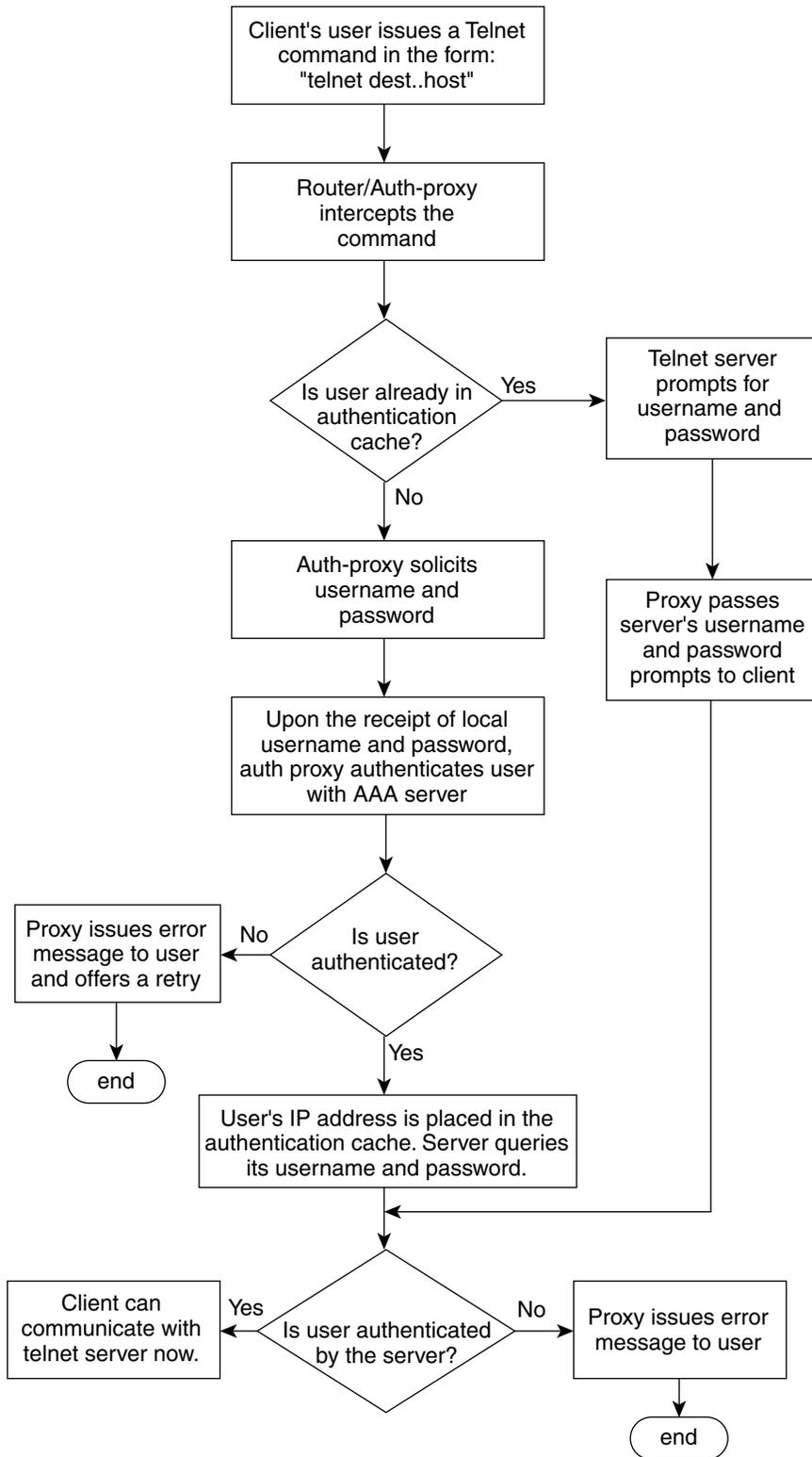
88127

## 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	<b>enable</b>  <b>Example:</b> Router> enable	Enables higher privilege levels, such as privileged EXEC mode.  Enter your password if prompted.
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 functionality on the router.
Step 4	<b>aaa authentication login default group tacacs+ group radius</b>  <b>Example:</b> Router (config)# aaa authentication login default group tacacs+ group radius	Defines the list of authentication methods at login.
Step 5	<b>aaa authorization auth-proxy default</b> [[group tacacs+] [group radius]]  <b>Example:</b> Router (config)# aaa authorization auth-proxy default group tacacs+ group radius	Uses the <b>auth-proxy</b> keyword to enable authorization proxy for AAA methods.
Step 6	<b>aaa authorization exec default</b> [group tacacs+] [group radius]  <b>Example:</b> 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><b>Example:</b></p> <pre>Router (config)# aaa accounting auth-proxy default stop-only group tacacs+ group radius</pre>	Activates authentication proxy accounting and uses the <b>auth-proxy</b> 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><b>Example:</b></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	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables higher privilege levels, such as privileged EXEC mode.</p> <p>Enter your password if prompted.</p>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><b>ip auth-proxy {inactivity-timer <i>min</i>   absolute-timer <i>min</i>}</b></p> <p><b>Example:</b> Router (config)# ip auth-proxy inactivity-timer 30</p>	<p>Sets the global authentication proxy idle timeout values in minutes.</p> <ul style="list-style-type: none"> <li>• <b>inactivity-timer <i>min</i></b>—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.</li> <li>• <b>absolute-timer <i>min</i></b>—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.</li> </ul>
Step 4	<p><b>ip auth-proxy auth-proxy-banner {ftp   http   telnet} [<i>banner-text</i>]</b></p> <p><b>Example:</b> Router (config)# ip auth-proxy auth-proxy-banner ftp hello</p>	<p>Optional) Displays the name of the firewall router in the authentication proxy login page. Disabled by default.</p> <ul style="list-style-type: none"> <li>• <b>ftp</b>—Specifies the FTP protocol.</li> <li>• <b>http</b>—Specifies the HTTP protocol.</li> <li>• <b>telnet</b>—Specifies the Telnet protocol.</li> <li>• <b><i>banner-text</i></b>—(Optional) A text string that replaces the default banner.</li> </ul>
Step 5	<p><b>ip auth-proxy name <i>auth-proxy-name</i> {ftp   http   telnet} [<i>inactivity-timer min</i>] [<i>absolute-timer min</i>] [<i>list {acl   acl-name}</i>]</b></p> <p><b>Example:</b> Router (config)# ip auth-proxy name ftp_list1 ftp absolute-timer 60 ftp list 102</p>	<p>Configures authentication proxy on an interface.</p> <ul style="list-style-type: none"> <li>• <b>ftp</b>—Specifies FTP to trigger that authentication proxy.</li> <li>• <b>http</b>—Specifies HTTP to trigger that authentication proxy.</li> <li>• <b>telnet</b>—Specifies Telnet to trigger that authentication proxy.</li> <li>• <b>inactivity-timer <i>min</i></b>—Overrides global authentication proxy cache timer for a specific authentication proxy name.</li> <li>• <b>absolute-timer <i>min</i></b>— Overrides the global value specified via the <b>ip auth-proxy</b> command.</li> <li>• <b>list {<i>acl</i>   <i>acl-name</i>}</b>—Specifies a standard (1–99), extended (1–199), or named access list to use with the authentication proxy.</li> </ul>

	Command or Action	Purpose
Step 6	<b>interface</b> <i>type</i>  <b>Example:</b> Router (config)# interface e0	Enters interface configuration mode by specifying the interface type on which to apply the authentication proxy.
Step 7	<b>ip auth-proxy</b> <i>auth-proxy-name</i>  <b>Example:</b> 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	<b>enable</b>  <b>Example:</b> Router> enable	Enables higher privilege levels, such as privileged EXEC mode.  Enter your password if prompted.
Step 2	<b>show ip auth-proxy configuration</b>  <b>Example:</b> Router# show ip auth-proxy configuration	Displays the current authentication proxy configuration.
Step 3	<b>show ip auth-proxy cache</b>  <b>Example:</b> 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**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables higher privilege levels, such as privileged EXEC mode.  Enter your password if prompted.
<b>Step 2</b>	<b>debug ip auth-proxy {detailed   ftp   function-trace   object-creation   object-deletion   telnet   timers}</b>  <b>Example:</b> 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: <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 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 auth-proxy**
- **ip auth-proxy**
- **ip auth-proxy auth-proxy-banner**
- **ip auth-proxy 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.





## **802.1X Authentication Services**





# 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>• <b>Count</b>—The number of failed passwords that triggers a lockout of the username.</li> <li>• <b>Time</b>—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} [ <b>auth-port</b> port-number] [ <b>acct-port</b> port-number] [ <b>timeout</b> seconds] [ <b>retransmit</b> retries] [ <b>key</b> 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</b> <i>port-number</i>, specify the UDP destination port for authentication requests.</li> <li>• (Optional) For <b>acct-port</b> <i>port-number</i>, specify the UDP destination port for accounting requests.</li> <li>• (Optional) For <b>timeout</b> <i>seconds</i>, 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</b> <i>retries</i>, 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</b> <i>string</i>, 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+} <i>group-name</i>	Defines the AAA server-group with a group name.
Step 6	Router(config-sg-radius)# <b>server</b> ip-address <b>auth-port</b> 1812 <b>acct-port</b> 1813	Defines the AAA server IP address, authentication port, and accounting port.
Step 7	Router(config)# <b>aaa authentication</b> login <i>named-authentication-list</i>	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 deadtime 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 deadtime 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 nhash 7 101B2A415547345A5F25790801706510064152425325720D7D04075D523D4F780A
  user ap-5 nhash 7 144231535C540C7A77096016074B51332753030D0877705A264F450A09720A7307
  user user1 nhash 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 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.





# VPN Access Control Using 802.1X Authentication

---

**First Published: August 11, 2003**

**Last Updated: June 23, 2009**

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.

An authentication manager has been added to allow more flexible authentication between different authentication methods like, dot1x, MAC address bypass, and web authentication. See the [802.1x Flexible Authentication](#) feature for more information.

## 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 VPN Access Control Using 802.1X Authentication](#)” section on [page 33](#).

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 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](#)



---

**Americas Headquarters:**

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

- [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](#)
- [Command Reference, page 31](#)
- [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 3](#)
- [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.

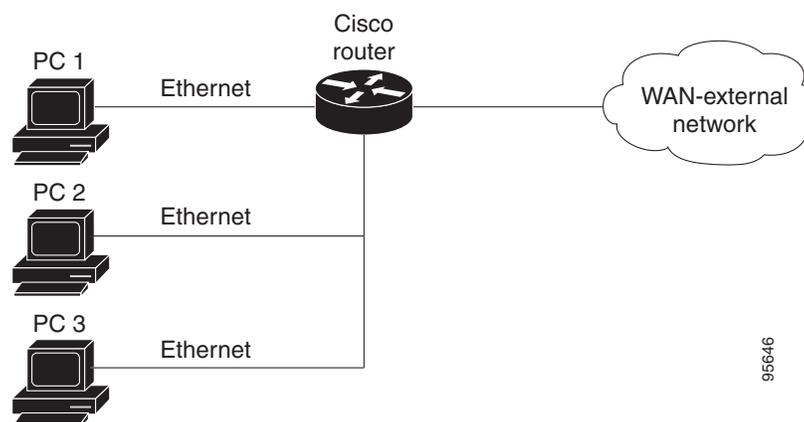
All 802.1X PDUs will be identified as such by the Ethernet driver and will be enqueued to be handled by an 802.1X process. On some platforms, Ethernet drivers have to program the interface address filter so that EAPOL packets can be accepted.

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. You can have any kind of connectivity or network beyond the Cisco router WAN.

**Note**

- 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

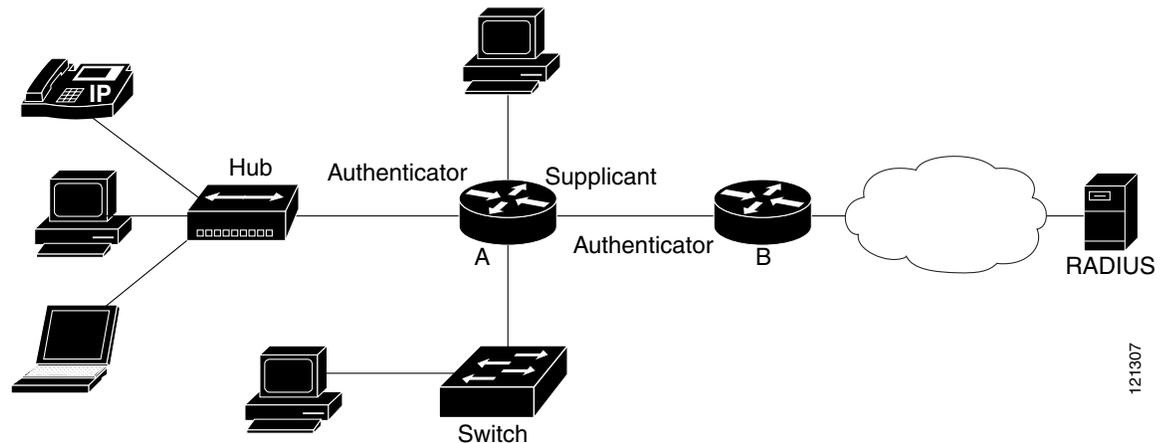
There are deployment scenarios in which a network device (a router acting as an 802.1X authenticator) is placed in an unsecured location and cannot be trusted as an authenticator. This scenario requires that a network device be able to authenticate itself against another network device. The 802.1X supplicant 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



## 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. See the [Configuring a Router As an 802.1x Supplicant, page 20](#).

## 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 a AAA RADIUS Server, page 6](#)
- [Configuring a Router, page 6](#)
- [Configuring a PC As an 802.1x Supplicant, page 18](#)
- [Monitoring VPN Access Control Using 802.1X Authentication, page 22](#)
- [Verifying VPN Access Control Using 802.1X Authentication, page 23](#)

## Configuring a AAA RADIUS Server

To configure an AAA RADIUS server, perform the following steps.

- 
- Step 1** Configure entries for the network access server and associated shared secrets.
- Note** The AAA server can be FreeRADIUS or Cisco Secure ACS or any other similar product with 802.1X support.
- Step 2** Add the username and configure the password of the user.
- Step 3** Configure a global or per-user authentication scheme.
- 

## Configuring a Router

This section contains the following procedures:

- [Enabling 802.1X Authentication, page 6](#) (required)
- [Configuring Router and RADIUS Communication, page 8](#) (required)
- [Configuring 802.1X Parameters \(Retransmissions and Timeouts\), page 9](#) (optional)
- [Configuring the Identity Profile, page 12](#) (required)
- [Configuring the Virtual Template and DHCP, page 13](#) (required)
- [Configuring the Necessary Access Control Policies, page 18](#) (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 | listname} method1 [method2...]**
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   listname} method1 [method2...]</b>  <b>Example:</b> Router (config)# aaa authentication dot1x default group radius	Creates a series of authentication methods that are used to determine user privilege to access the privileged command level.
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.
Step 7	<b>interface type slot/port</b>  <b>Example:</b> Router (config-identity-prof)# interface fastethernet 0/1	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 group radius
Router(config)# dot1x system-auth-control
Router(config)# interface fastethernet 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

Sysauthcontrol           Enabled
Dot1x Protocol Version   2

Dot1x Info for FastEthernet1
-----
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection         = Both
HostMode                  = MULTI_HOST
ReAuthentication          = Enabled
QuietPeriod               = 600
ServerTimeout             = 60
SuppTimeout               = 30
ReAuthPeriod              = 1800 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 3
TxPeriod                  = 60
RateLimitPeriod           = 60
```

## 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 fastethernet1	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 192.0.2.0	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 192.0.2.1
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

- enable**
- configure terminal**
- interface** *type slot/port*
- 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 FastEthernet 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 seconds</b>  <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 seconds</b>  <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 seconds</b>  <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 seconds</b>  <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 seconds</b>  <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 FastEthernet1
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** *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)# device authorize mac-address 1.1.1	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)# device authorize type cisco ip phone	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-templ1
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**

	<b>Command</b>	<b>Description</b>
<b>Step 1</b>	<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>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>identity profile default</b>  <b>Example:</b> Router (config)# identity profile default	Creates an identity profile and enters identity profile configuration mode.
<b>Step 4</b>	<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 virtualtemplatel	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-template)# 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</i> [ <i>mask</i> ]  <b>Example:</b> Router (dhcp-config)# network 209.165.200.225 255.255.255.224	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 (dhcp-config)# default-router 192.0.2.2	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</i> [ <i>mask</i> ]  <b>Example:</b> Router (config-dhcp)# network 209.165.200.226 255.255.255.224	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>	Specifies the default router list for a DHCP client.
	<b>Example:</b> Router (config-dhcp)# default-router 192.0.2.3	
Step 4	<b>exit</b>	Exits DHCP pool configuration mode.
	<b>Example:</b> Router (config-dhcp)# exit	

### Configuring the Interface

	Command	Description
Step 1	<b>configure terminal</b>	Enters global configuration mode.
	<b>Example:</b> Router# configure terminal	
Step 2	<b>interface</b> <i>type slot/port</i>	Enters interface configuration mode and specifies the interface to be enabled.
	<b>Example:</b> Router (config)# interface loopback 0/1	
Step 3	<b>ip address</b> <i>ip-address mask</i> [ <b>secondary</b> ]	Sets the private IP address for the interface.
	<b>Example:</b> Router (config-if)# ip address 209.165.200.227 255.255.255.224	
Step 4	<b>interface virtual-template</b> <i>number</i>	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.
	<b>Example:</b> Router (config-if)# interface virtual-template 1	
Step 5	<b>ip address</b> <i>ip-address mask</i> [ <b>secondary</b> ]	Sets the public IP address for the interface.
	<b>Example:</b> Router (config-if)# ip address 209.165.200.227 255.255.255.224	
Step 6	<b>exit</b>	Exits interface configuration mode.
	<b>Example:</b> Router (config-if)# exit	

### 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</b> <i>type slot/port</i>  <b>Example:</b> Router (config)# interface virtual-template 1	Enters interface configuration mode and specifies the interface to be enabled.
Step 4	<b>ip unnumbered</b> <i>type number</i>  <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-identity-prof)# description put the description here
Router(config-identity-prof)# template virtual-template1
Router(config-identity-prof)# exit

Router(config)# ip dhcp pool private
Router(dhcp-config)# default-router 192.0.2.0
Router(dhcp-config)# exit

Router(config)#ip dhcp pool public
Router(dhcp-config)# default-router 192.0.2.1
Router(dhcp-config)# exit
Router(config)# interface

Router(dhcp-config)# network 209.165.200.225 255.255.255.224
Router(dhcp-config)# default-router 192.0.2.1
Router(dhcp-config)# exit

Router(config)# interface loopback0
Router(config-if)# interface ethernet0
Router(config-if)# ip address 209.165.200.226 255.255.255.224
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 PC As an 802.1x Supplicant

This section includes the following procedures.

- [Configuring a PC for VPN Access Control Using 802.1X Authentication, page 18](#)
- [Enabling 802.1X Authentication on a Windows 2000/XP PC, page 18](#)
- [Enabling 802.1X Authentication on a Windows 2000 PC, page 18](#)
- [Enabling 802.1X Authentication on a Windows XP PC, page 19](#)
- [Enabling 802.1X Authentication on Windows 2000 and Windows XP PCs, page 19](#)

## 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.

- 
- Step 1** Make sure that the PC has at least Service Pack 3.
- Go to the page “Microsoft 802.1x Authentication Client” on the Microsoft Windows 2000 website at the following URL:
- <http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/8021xclient.asp>.
- At the above site, download and install 802.1X client for Windows 2000.
- 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

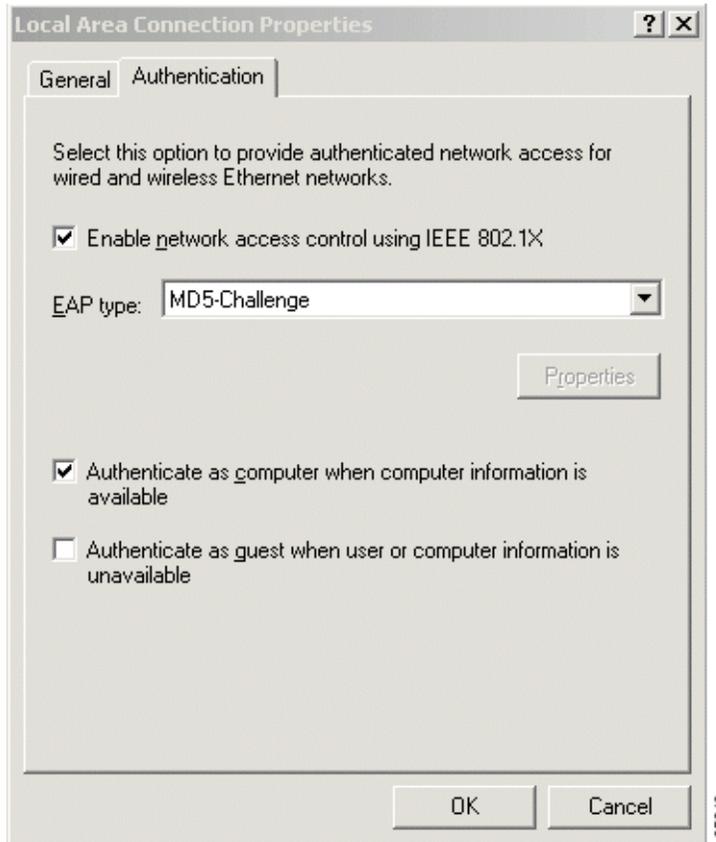
To enable 802.1X authentication on a Windows XP PC, perform the following steps.

- 
- 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

## Configuring a Router As an 802.1x Supplicant

To configure a router as an 802.1x supplicant, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authentication dot1x {default | listname} method1 [method2...]**
4. **dot1x credentials name**
5. **username name**
6. **password [0 | 7] password**
7. **interface type number**
8. **dot1x pae supplicant**
9. **dot1x credentials name**
10. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><b>aaa authentication dot1x</b> {default   listname} method1 [method2...]</p> <p><b>Example:</b> Router(config)# aaa authentication dot1x default group radius</p>	<p>Specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X.</p>
Step 4	<p><b>dot1x credentials</b> name</p> <p><b>Example:</b> Router(config)# dot1x credentials name1</p>	<p>Specifies the 802.1X credential profile to use when configuring a supplicant.</p>
Step 5	<p><b>username</b> name</p> <p><b>Example:</b> Router(config-dot1x-creden)# username name1</p>	<p>Specifies the username for an 802.1X credentials profile.</p>
Step 6	<p><b>password</b> [0   7] password</p> <p><b>Example:</b> Router(config-dot1x-creden)# password 0 password1</p>	<p>Specifies the password for an 802.1X credentials profile.</p>
Step 7	<p><b>exit</b></p> <p><b>Example:</b> Router(config-dot1x-creden)# exit</p>	<p>Enters global configuration mode.</p>
Step 8	<p><b>interface</b> type number</p> <p><b>Example:</b> Router(config)# interface FastEthernet0/0</p>	<p>Enters interface configuration mode.</p>
Step 9	<p><b>dot1x pae supplicant</b></p> <p><b>Example:</b> Router(config-if)# dot1x pae supplicant</p>	<p>Sets the Port Access Entity (PAE) type as supplicant.</p>

	Command or Action	Purpose
Step 10	<code>dot1x credentials name</code>  <b>Example:</b> Router(config-if)# dot1x credentials name1	Specifies the 802.1X credential profile to use when configuring a supplicant.
Step 11	<code>end</code>  <b>Example:</b> Router(config-if)# end	(Optional) Exits the current configuration mode.

## Troubleshooting Tips

Use the debug commands in the [Monitoring VPN Access Control Using 802.1X Authentication](#) section to debug the supplicant.

## 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 {all | interface}`
3. `clear eap sessions [credentials credentials-name | interface interface-name | method method-name | transport transport-name]`
4. `debug dot1x [all | errors | events | feature | packets | redundancy | registry | state-machine]`
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	<code>enable</code>  <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	<code>clear dot1x {all   interface}</code>  <b>Example:</b> Router# clear dot1x all	Clears 802.1X interface information.

	Command or Action	Purpose
Step 3	<pre>clear eap sessions [credentials credentials-name   interface interface-name   method method-name   transport transport-name]]</pre> <p><b>Example:</b> Router# clear eap sessions credentials type1</p>	Clears EAP information on a switch or for a specified port.
Step 4	<pre>debug dot1x [all   errors   events   feature   packets   redundancy   registry   state-machine ]</pre> <p><b>Example:</b> Router# debug dot1x all</p>	Displays 802.1X debugging information. <ul style="list-style-type: none"> <li>• <b>all</b>-Enables all 802.1X debugging messages.</li> <li>• <b>errors</b>-Provides information about all 802.1X errors.</li> <li>• <b>events</b>-Provides information about all 802.1X events.</li> <li>• <b>feature</b>-Provides information about 802.1X features for switches only.</li> <li>• <b>packets</b>-Provides information about all 802.1X packets.</li> <li>• <b>redundancy</b>-Provides information about 802.1X redundancy.</li> <li>• <b>registry</b>-Provides information about 802.1X registries.</li> <li>• <b>state-machine</b>—Provides information regarding the 802.1X state machine.</li> </ul>
Step 5	<pre>debug eap [all   method] [authenticator   peer] {all   errors   events   packets   sm}</pre> <p><b>Example:</b> Router# debug eap all</p>	Displays information about EAP.
Step 6	<pre>dot1x initialize [interface interface-name]</pre> <p><b>Example:</b> Router# dot1x initialize interface FastEthernet1</p>	Initializes an interface.
Step 7	<pre>dot1x re-authenticate interface-type interface-number</pre> <p><b>Example:</b> Router# dot1x re-authenticate FastEthernet1</p>	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> [ <b>interface</b> <i>interface-name</i> [ <b>details</b> ]]  <b>Example:</b> Router# show dot1x interface FastEthernet 1 details	Shows details for an identity profile.
Step 3	<b>show eap registrations</b> [ <b>method</b>   <b>transport</b> ]  <b>Example:</b> Router# show eap registrations method	Displays EAP registration information.
Step 4	<b>show eap 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# 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 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 : 2457 bytes
!
```

```
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 871-1
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
aaa new-model
!
!
aaa authentication dot1x default group radius group radius
!
!
aaa session-id common
!
!
dot11 syslog
ip source-route
!
ip dhcp pool private
    network 209.165.200.225 255.255.255.224
    default-router 192.0.2.18
!
ip dhcp pool public
    network 209.165.200.226 255.255.255.224
    default-router 192.0.2.17
!
ip dhcp pool name
    default-router 192.0.2.16
!
!
ip cef
no ip domain lookup
ip host sjc-tftp02 192.0.2.15
ip host sjc-tftp01 192.0.2.14
ip host dirt 192.0.2.13
!
!
!
template virtualtemplate1
!
dot1x system-auth-control
dot1x credentials basic-user
    description This credentials profile should be used for most configured ports
    username router1
    password 0 secret
!
identity profile default
    description description 1
    device authorize mac-address 0001.024b.b4e7
    device authorize mac-address 0001.0001.0001
    device authorize type cisco ip phone
    template Virtual-Template1
!
!
!
!
```

```

archive
  log config
  hidekeys
!
!
!
!
!
interface Loopback0
  ip address 209.165.200.227 255.255.255.224
!
interface FastEthernet0
!
interface FastEthernet1
  dot1x pae authenticator
  dot1x port-control auto
  dot1x timeout quiet-period 600
  dot1x timeout server-timeout 60
  dot1x timeout reauth-period 1800
  dot1x timeout tx-period 60
  dot1x timeout ratelimit-period 60
  dot1x max-req 3
  dot1x reauthentication
!
interface FastEthernet2
!
interface FastEthernet3
!
interface FastEthernet4
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface Virtual-Template1
  ip unnumbered Loopback0
!
interface Dot11Radio0
  no ip address
  shutdown
  speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0
  station-role root
  no cdp enable
!
interface Vlan1
  ip address 209.165.200.228 255.255.255.224
!
ip default-gateway 192.0.2.10
ip default-network 192.0.2.11
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.0.2.11
ip route 209.165.200.229 255.255.255.224 192.0.2.12
no ip http server
no ip http secure-server
!
!
ip radius source-interface FastEthernet1
!
!
!
radius-server host 192.0.2.9 auth-port 1645 acct-port 1646
radius-server key radiuskey
!
control-plane

```

```
!  
!  
line con 0  
  exec-timeout 30 0  
  logging synchronous  
  no modem enable  
line aux 0  
line vty 0 4  
  privilege level 15  
  password lab  
!  
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 192.0.2.8  
!  
!  
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 192.0.2.7  
  set transform-set t1  
  match address 101  
!  
no voice hpi capture buffer  
no voice hpi capture destination  
!  
interface Loopback0  
  description corporate  
  ip address 209.165.200.230 255.255.255.224  
!  
interface Loopback1
```

```
description internet
ip address 209.165.200.231 255.255.255.224
!
interface FastEthernet0/0
ip address 209.165.200.232 255.255.255.224
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
speed auto
half-duplex
pppoe enable
!
interface ATM1/0
ip address 209.165.200.233 255.255.255.224
no atm ilmi-keepalive
pvc 1/43
protocol ip 192.0.2.6 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 209.165.200.234 255.255.255.224
ip mtu 1492
crypto map test
!
!
router rip
network 192.0.2.5
network 192.0.2.4
network 192.0.2.3
network 192.0.2.2
network 192.0.2.1
!
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 209.165.200.236 255.255.255.224
  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-Templat1
! 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 209.165.200.237 255.255.255.224
  default-router 192.0.2.1
  exit
!
ip dhcp pool public
  network 209.165.200.238 255.255.255.224
  default-router 192.0.2.0
  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 209.165.200.239 255.255.255.224
!
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

```

## Additional References

The following sections provide references related to the VPN Access Control Using 802.1X Authentication feature.

## 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

Standard	Title
IEEE 802.1X protocol	—

## 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
RFC-2284	<i>“RFC 2284 (PPP Extensible Authentication Protocol [EAP])” document from 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 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 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 features in this module.

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 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.
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.

Table 1 Feature Information for VPN Access Control Using 802.1X Authentication (continued)

Feature Name	Releases	Feature Information
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, debug dot1x, debug eap, description (dot1x credentials), dot1x control-direction, dot1x credentials, dot1x default, dot1x host-mode, dot1x max-reauth-req, dot1x max-start, dot1x multiple-hosts, dot1x timeout, eap, identity profile, password (dot1x credentials), show eap registrations, show eap sessions, and 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, dot1x default, dot1x guest-vlan, dot1x host-mode, dot1x max-reauth-req, dot1x max-req, dot1x max-start, dot1x pae, dot1x port-control, dot1x re-authenticate (privileged EXEC), dot1x reauthentication, dot1x system-auth-control, dot1x timeout, macro global, macro name, and show ip igmp snooping</b>

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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

© 2003–2009 Cisco Systems, Inc. All rights reserved.



## **Network Admission Control (NAC)**





## Network Admission Control

---

**First Published: May 27, 2004**

**Last Updated: July 9, 2009**

The Network Admission Control feature addresses the increased threat and impact of worms and viruses have on business networks. 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

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 Network Admission Control” section on page 28](#).

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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. An account on Cisco.com is not required.



---

**Americas Headquarters:**

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

# 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 23](#)
- [Additional References, page 26](#)
- [Feature Information for Network Admission Control, page 28](#)
- [Glossary, page 30](#)

## Prerequisites for Network Admission Control

- The Cisco IOS router must be running Cisco IOS software Release 12.3(8)T or later.
- The Cisco Trust Agent must be installed on the endpoint devices (for example, on PCs and laptops).
- A Cisco Secure ACS is required for authentication, authorization, and accounting (AAA).
- A proficiency with configuring access control lists (ACLs) and AAA is necessary.

## 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, the following concepts need to be understood:

- [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

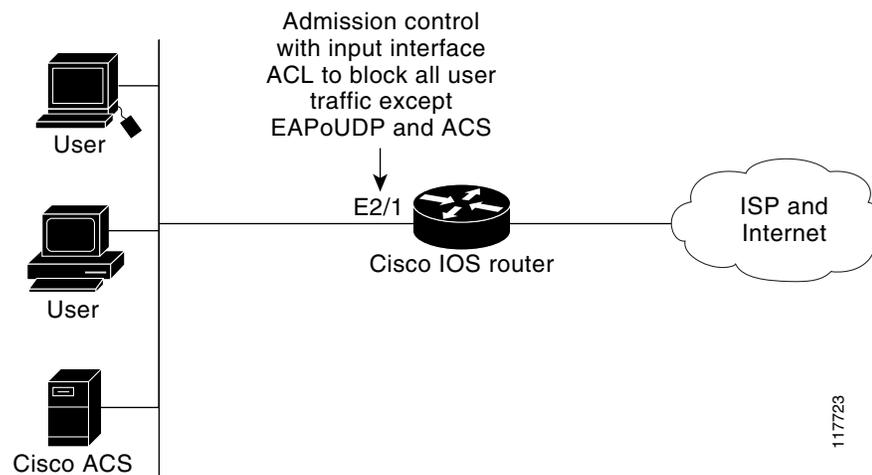
Virus infections are the single largest cause of serious security breaches for networks and often result in huge financial losses. Sources of virus infections are insecure endpoints (for example, PCs, laptops, and servers). Although the endpoints may have antivirus software installed, the software is 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), the following attribute-value pairs (AV pairs) can be set on the Cisco Secure ACS. These AV pairs are 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 to be 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 user specified value, 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, the value must be set for 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 are 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, an SNMP get operation can be performed on the `cnnEOUGlobalObjectsGroup` table or the `show eou` command can be configured 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:

- **eu initialize all**
- **eu initialize authentication clientless**
- **eu initialize authentication eap**
- **eu initialize authentication static**
- **eu initialize ip** {*ip-address*}
- **eu initialize mac** {*mac-address*}
- **eu initialize posturetoken** {*string*}
- **eu revalidate all**
- **eu revalidate authentication clientless**
- **eu revalidate authentication eap**
- **eu revalidate authentication static**
- **eu revalidate ip** {*ip-address*}
- **eu revalidate mac** {*mac-address*}
- **eu revalidate posturetoken** {*string*}

The initialization and revalidation actions can also be accomplished by performing SNMP set operations on the objects of the `cnnEouHostValidateAction` table. For more information about initializing and revalidating sessions, see the section [“CLI Commands That Correlate to `cnnEouHostValidateAction` Table Objects.”](#)

For examples of CLI commands that correlate to changes that can be made to `cnnEouHostValidateAction` 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 `cnnEouHostQueryTable` and `cnnEouHostResultTable`. The `cnnEouHostQueryTable` is used to build the query. The query is the same format as the **show eu ip** {*ip-address*} command (that is, the IP address would be shown as in the **show eu ip** command—for example, 10.1.1.1). Administrators must use the SNMP set operation on the objects of the `cnnEouHostQueryTable` to create the query. The results of the query are stored as a row in the `cnnEouHostResultTable`. 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 eu**, **show eu all**, **show eu authentication**, **show eu initialize**, **show eu ip**, **show eu mac**, **show eu posturetoken**, **show eu 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 9](#) (optional)
- [Configuring an Interface-Specific EAPoUDP Association, page 10](#) (optional)
- [Configuring AAA for EAPoUDP, page 11](#) (optional)
- [Configuring the Identity Profile and Policy, page 12](#) (required)
- [Clearing EAPoUDP Sessions That Are Associated with an Interface, page 14](#) (optional)
- [Verifying Network Admission Control, page 15](#) (optional)
- [Troubleshooting Network Admission Control, page 15](#) (optional)
- [Monitoring and Controlling NAC with the CISCO-NAC-NAD-MIB, page 16](#) (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 are 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* [**eapoudp** | **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	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><b>access-list</b> <i>access-list-number</i> {<b>permit</b>   <b>deny</b>} <i>protocol source destination</i></p> <p><b>Example:</b> Router (config)# access-list 101 permit ip any 192.50.0.0 0.0.0.255</p>	<p>Defines a numbered access list.</p>
Step 4	<p><b>ip admission name</b> <i>admission-name</i> [<b>eapoudp</b>   <b>proxy</b> {<b>ftp</b>   <b>http</b>   <b>telnet</b>}] [<b>list</b> {<i>acl</i>   <i>acl-name</i>}]</p> <p><b>Example:</b> Router (config)# ip admission name greentree eapoudp list 101</p>	<p>Creates IP network admission control rules. The rules define how you apply admission control. The rules are as follows:</p> <ul style="list-style-type: none"> <li>• <b>eapoudp</b>—Specifies IP network admission control using EAPoUDP.</li> <li>• <b>proxy ftp</b>—Specifies FTP to trigger authentication proxy.</li> <li>• <b>proxy http</b>—Specifies HTTP to trigger authentication proxy.</li> <li>• <b>proxy telnet</b>—Specifies Telnet to trigger authentication proxy.</li> </ul> <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	<p><b>interface</b> <i>type slot/port</i></p> <p><b>Example:</b> Router (config)# interface ethernet 2/1</p>	<p>Defines an interface and enters interface configuration mode.</p>

	Command or Action	Purpose
Step 6	<p><b>ip address</b> <i>ip-address mask</i></p> <p><b>Example:</b> Router (config-if)# ip address 192.0.0.1 255.255.255.0</p>	Sets a primary or secondary IP address for an interface.
Step 7	<p><b>ip admission</b> <i>admission-name</i></p> <p><b>Example:</b> Router (config-if)# ip admission greentree</p>	Applies the named admission control rule at the interface.
Step 8	<p><b>exit</b></p> <p><b>Example:</b> Router (config-if)# exit</p>	Exits interface configuration mode.
Step 9	<p><b>access-list</b> <i>access-list-number {permit   deny}</i> <i>protocol source destination</i></p> <p><b>Example:</b> 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</p>	<p>Defines a numbered access list.</p> <p><b>Note</b> 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).</p> <p><b>Note</b> In the third example (under “Command or Action,” ACL “105” is 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.”</p>
Step 10	<p><b>ip access-group</b> <i>{access-list-number   access-list-name}</i> <b>in</b></p> <p><b>Example:</b> Router (config)# ip access-group 105 in</p>	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	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><b>eou {allow   clientless   default   initialize   logging   max-retry   port   rate-limit   revalidate   timeout}</b></p> <p><b>Example:</b> Router (config)# eou initialize</p>	<p>Specifies EAPoUDP values.</p> <ul style="list-style-type: none"> <li>• For a breakout of available keywords and arguments for the <b>eou</b> command, see the following commands: <ul style="list-style-type: none"> <li>– <b>eou allow</b></li> <li>– <b>eou clientless</b></li> <li>– <b>eou default</b></li> <li>– <b>eou initialize</b></li> <li>– <b>eou logging</b></li> <li>– <b>eou max-retry</b></li> <li>– <b>eou port</b></li> <li>– <b>eou rate-limit</b></li> <li>– <b>eou revalidate</b></li> <li>– <b>eou timeout</b></li> </ul> </li> </ul>

## 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

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **eou** [**default** | **max-retry** | **revalidate** | **timeout**]

## 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>interface</b> <i>type slot/port</i>  <b>Example:</b> Router (config)# interface ethernet 2/1	Defines an interface and enters interface configuration mode.
Step 4	<b>eou</b> [ <b>default</b>   <b>max-retry</b>   <b>revalidate</b>   <b>timeout</b> ]  <b>Example:</b> Router (config-if)# eou revalidate	Enables an EAPoUDP association for a specific interface. <ul style="list-style-type: none"><li>• For a breakout of available keywords and arguments for the <b>eou</b> command, see the following commands:<ul style="list-style-type: none"><li>– <b>eou default</b></li><li>– <b>eou max-retry</b></li><li>– <b>eou revalidate</b></li><li>– <b>eou timeout</b></li></ul></li></ul>

## Configuring AAA for EAPoUDP

To set up AAA for EAPoUDP, perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication eou default enable group radius**
5. **aaa authorization network default group radius**
6. **radius-server host** {*hostname* | *ip-address*}
7. **radius-server key** {*0 string* | *7 string* | *string*}

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <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	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>aaa new-model</code>  <b>Example:</b> Router (config)# aaa new-model	Enables the AAA access control model.
Step 4	<code>aaa authentication eou default enable group radius</code>  <b>Example:</b> Router (config)# aaa authentication eou default enable group radius	Sets authentication lists for an EAPoUDP association.
Step 5	<code>aaa authorization network default group radius</code>  <b>Example:</b> Router (config)# aaa authorization network default group radius	Uses the list of all RADIUS servers for authentication.
Step 6	<code>radius-server host {hostname   ip-address}</code>  <b>Example:</b> Router (config)# radius-server host 192.0.0.40	Specifies a RADIUS server host.
Step 7	<code>radius-server key {0 string   7 string   string}</code>  <b>Example:</b> 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	<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 eapoudp</b>  <b>Example:</b> Router (config)# identity profile eapoudp	Creates an identity profile and enters identity profile configuration mode.
Step 4	<b>device {authorize {ip address <i>ip-address</i> {policy <i>policy-name</i>}   mac-address <i>mac-address</i>   type {cisco   ip   phone}}   not-authorize}</b>  <b>Example:</b> Router (config-identity-prof)# device authorize ip address 10.10.142.25 policy policynam1	Statically authorizes an IP device and applies an associated policy to the device.
Step 5	<b>exit</b>  <b>Example:</b> Router (config-identity-prof)# exit	Exits identity profile configuration mode.

	Command or Action	Purpose
Step 6	<pre>identity policy policy-name [access-group group-name   description line-of-description   redirect url   template [virtual-template interface-name]]</pre> <p><b>Example:</b> Router (config-identity-prof)# identity policy policynamel </p>	Creates an identity policy and enters identity policy configuration mode.
Step 7	<pre>access-group group-name</pre> <p><b>Example:</b> Router (config-identity-policy)# access-group exempt-acl </p>	Defines network access attributes for the identity policy.
Step 8	<pre>exit</pre> <p><b>Example:</b> Router (config-identity-policy)# exit </p>	Exits identity policy configuration mode.
Step 9	<pre>exit</pre> <p><b>Example:</b> Router (config-identity-prof)# exit </p>	Exits identity profile configuration mode.
Step 10	<pre>ip access-list extended access-list-name</pre> <p><b>Example:</b> Router (config)# ip access-list extended exempt-acl </p>	Defines access control for statically authenticated devices (and enters network access control configuration mode).
Step 11	<pre>{permit   deny} source source-wildcard destination destination-wildcard</pre> <p><b>Example:</b> Router (config-ext-nacl)# permit ip any 192.50.0.0. 0.0.0.255 </p>	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	<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>clear eou all</code>  <b>Example:</b> Router# <code>clear eou all</code>	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

- `enable`
- `show eou all`
- `show ip admission eapoudp`

## 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>show eou all</code>  <b>Example:</b> Router# <code>show eou all</code>	Displays information about EAPoUDP sessions on the network access device.
Step 3	<code>show ip admission eapoudp</code>  <b>Example:</b> Router# <code>show ip admission eapoudp</code>	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	<code>enable</code>  <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	<code>debug eap {all   errors   packets   sm}</code>  <b>Example:</b> Router# debug eap all	Displays information about EAP messages.
Step 3	<code>debug eou {all   eap   errors   packets   sm}</code>  <b>Example:</b> Router# debug eou all	Displays information about EAPoUDP messages.
Step 4	<code>debug ip admission eapoudp</code>  <b>Example:</b> 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 17](#)
- [CLI Commands That Correlate to cnnEouIfConfigTable Objects, page 17](#)
- [CLI Commands That Correlate to cnnEouHostValidateAction Table Objects, page 17](#)
- [Creating MIB Query Tables, page 18](#)
- [Viewing MIB Query Results, page 21](#)

### 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 24](#).

**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 <code>cnnEouVersion</code> object. (The object value is “1.”)
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 is “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"> <li>• Format: GET <code>cnnEouIfTimeoutAAA.IfIndex</code></li> <li>• You must specify the corresponding index number of the specific interface.</li> </ul>
Maximum retries	Performs a get operation on the <code>cnnEouIfMaxRetry</code> object. <ul style="list-style-type: none"> <li>• Format: GET <code>cnnEouIfMaxRetry.IfIndex</code></li> </ul>

## 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.
- `cnnEouHostValidateIpAddrType`—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.

#### **eou initialize posturetoken**

All sessions having a particular posturetoken can be initialized using the **eou 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 eou all` Command

To build a query that provides the same results as using the **show eou 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 eou 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
<b>Step 1</b>	Set the <code>cnnEouHostQueryStatus</code> object to <code>createandgo</code> .	Creates a query row.
<b>Step 2</b>	Set the <code>cnnEouHostQueryMask</code> object to 8.	Corresponds in value to the <b>show eou all</b> command.
<b>Step 3</b>	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 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"> <li>The only address type currently supported by NAC is IPv4.</li> </ul>
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 are created in a Result table for a particular query. <ul style="list-style-type: none"> <li>If a query row is a negative number, the query is still being processed.</li> </ul>
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"> <li>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>.</li> </ul>



### 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. <b>Note</b> 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 <code>8</code> .	Correlates to the default of the <b>show eou all</b> command.
Step 3	Set <code>cnnEouHostQueryRows</code> to <code>500</code> .	Identifies the maximum number of rows to be built in the result table for this query.
Step 4	Set <code>cnnEouHostQuerySkipNHosts</code> to <code>0</code> .	Corresponds to the result rows to be created.
Step 5	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. The table is on the basis of a query having 2,000 sessions (rows).

## What to Do Next

After the above task is performed, information for the first 500 hosts (rows) is queried. To view query information for the next 500 hosts (rows), perform the same five steps, with the exception of changing the `cnnEouHostQuerySkipNHosts` object value to `500` in Step 4. This task results in query information for rows 501 through 1000. In the same way, to obtain query information for the remaining hosts (through 2000), perform the same five steps again, with the exception of changing the `cnnEouHostQuerySkipNHosts` object values in Step 4 to `1000` and `1500`, respectively.

# Configuration Examples for Network Admission Control

This section includes the following example.

- [Network Admission Control: Example, page 23](#)
- [NAC MIB Output: Examples, page 24](#)

## 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	“ <a href="#">Access Control Lists: Overview and Guidelines</a> ” chapter of the “Traffic Filtering and Firewalls” section of the <i>Cisco IOS Security Configuration Guide: Securing User Services</i> , Release 12.4T.
Authentication, authorization, and accounting	“ <a href="#">Authentication, Authorization, and Accounting</a> ” section of <i>Cisco IOS Security Configuration Guide: Securing User Services</i> , Release 12.4T.
Interfaces, configuring	<a href="#">Cisco IOS Interface and Hardware Component Configuration Guide</a> , Release 12.4T.
SNMP and SNMP get and set operations	<ul style="list-style-type: none"> <li>“<a href="#">Simple Network Management Protocol</a>” section of the <i>Internetworking Technology Handbook</i></li> <li>“<a href="#">Configuring SNMP Support</a>” section of the <i>Cisco IOS Configuring Fundamentals Configuration Guide</i>, Release 12.4T.</li> </ul>

### 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>	<p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

# 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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. 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"> <li>• <a href="#">Prerequisites for Network Admission Control, page 2</a></li> <li>• <a href="#">Restrictions for Network Admission Control, page 2</a></li> <li>• <a href="#">Information About Network Admission Control, page 2</a></li> <li>• <a href="#">How to Configure Network Admission Control, page 7</a></li> <li>• <a href="#">Configuration Examples for Network Admission Control, page 23</a></li> </ul> <p>The following commands were introduced or modified by this feature: <b>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).</b></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"> <li>• <a href="#">“NAC MIB” section on page 5</a></li> <li>• <a href="#">“Monitoring and Controlling NAC with the CISCO-NAC-NAD-MIB” section on page 16</a></li> </ul> <p>The following commands were introduced or modified by this feature: <b>show ip device tracking</b>.</p>
	12.2(33)SXI	This feature was integrated into Cisco IOS Release 12.2(33)SXI.

# 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.

---

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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, 2007–2008 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 implemented on the Cisco ASR 1000 series routers.
Cisco IOS XE Release 2.3	Support for this feature was integrated into Cisco IOS XE Release 2.3.

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, see the [Cisco IOS Security Command Reference](#). To locate documentation of other commands that appear in this chapter, use 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).

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](#)



---

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

© 2007–2009 Cisco Systems, Inc. All rights reserved.

- [RADIUS Attributes](#)
- [RADIUS Configuration Examples](#)

## 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 Deadtime](#) (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 <b>auth-port</b> <i>port-number</i> option to configure a specific UDP port on this RADIUS server to be used solely for authentication. Use the <b>acct-port</b> <i>port-number</i> option to configure a specific UDP port on this RADIUS server to be used solely for accounting. Use the <b>alias</b> 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><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 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	<pre>Router(config)# radius-server key {0 string   7 string   string}</pre>	Specifies the shared secret text string used between the router and a RADIUS server. Use the <b>0 line</b> option to configure an unencrypted shared secret. Use the <b>7 line</b> option to configure an encrypted shared secret.
Step 2	<pre>Router(config)# radius-server retransmit retries</pre>	Specifies how many times the router transmits each RADIUS request to the server before giving up (the default is 3).
Step 3	<pre>Router(config)# radius-server timeout seconds</pre>	Specifies for how many seconds a router waits for a reply to a RADIUS request before retransmitting the request.
Step 4	<pre>Router(config)# radius-server deadtime minutes</pre>	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)# <b>radius-server vsa send</b> [ <b>accounting</b>   <b>authentication</b> ]	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-proprietary 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-proprietary RADIUS attributes.

As mentioned earlier, to configure RADIUS (whether vendor-proprietary 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-proprietary implementation of RADIUS, use the **radius-server host non-standard** command. Vendor-proprietary attributes will not be supported unless you use the **radius-server host non-standard** command.

To specify a vendor-proprietary RADIUS server host and a shared secret text string, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>radius-server host</b> {hostname   ip-address} <b>non-standard</b>	Specifies the IP address or host name of the remote RADIUS server host and identifies that it is using a vendor-proprietary implementation of RADIUS.
Step 2	Router(config)# <b>radius-server key</b> {0 string   7 string   string}	Specifies the shared secret text string used between the router and the vendor-proprietary 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-proprietary 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)# <b>radius-server configure-nas</b>	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)# <b>radius-server attribute nas-port format</b>	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
<b>Step 1</b>	Router(config)# <b>radius-server vsa send</b> [ <b>accounting</b>   <b>authentication</b> ]	Enables the network access server to recognize and use vendor-specific attributes as defined by RADIUS IETF attribute 26.
<b>Step 2</b>	Router(config)# <b>aaa nas port extended</b>	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)# <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}]	Specifies and defines the IP address of the server host before configuring the AAA server-group. Refer to the section “ <a href="#">Configuring Router to RADIUS Server Communication</a> ” of this chapter for more information on the <b>radius-server host</b> command.
Step 2	Router(config-if)# <b>aaa group server</b> {radius   tacacs+} group-name	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)# <b>server ip-address</b> [auth-port port-number] [acct-port port-number]	Associates a particular RADIUS server with the defined server group. Each security server is identified by its IP address and UDP port number.  Repeat this step for each RADIUS server in the AAA server group.  <b>Note</b> Each server in the group must be defined previously using the <b>radius-server host</b> command.

## 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)# <b>aaa group server radius</b> <i>group1</i>	Defines a RADIUS type server group.
Step 2	Router(config-sg)# <b>deadtime</b> <i>1</i>	Configures and defines deadtime value in minutes. <b>Note</b> 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)# <b>exit</b>	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# <b>config term</b>	Enters global configuration mode.
Step 2	Router(config)# <b>aaa preauth</b>	Enters AAA preauthentication mode.

	Command	Purpose
Step 3	Router(config-preauth)# <b>group</b> {radius   tacacs+   server-group}	(Optional) Selects the security server to use for AAA preauthentication requests. The default is RADIUS.
Step 4	Router(config-preauth)# <b>dnis</b> [password string]	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)# <b>aaa dnis map enable</b>	Enables DNIS mapping.
Step 2	Router(config)# <b>aaa dnis map</b> <i>dnis-number</i> <b>authentication ppp group</b> <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)# <b>aaa dnis map</b> <i>dnis-number</i> <b>authorization network group</b> <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)# <b>aaa dnis map</b> <i>dnis-number</i> <b>accounting</b> <b>network</b> [ <b>none</b>   <b>start-stop</b>   <b>stop-only</b> ] <b>group</b> <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
<b>Step 1</b>	Router(config)# <b>aaa preauth</b>	Enters AAA preauthentication configuration mode.
<b>Step 2</b>	Router(config-preauth)# <b>group</b> <i>server-group</i>	Specifies the AAA RADIUS server group to use for preauthentication.
<b>Step 3</b>	Router(config-preauth)# <b>clid</b> [ <b>if-avail</b>   <b>required</b> ] [ <b>accept-stop</b> ] [ <b>password</b> <i>string</i> ]	Preauthenticates calls on the basis of the CLID number.
<b>Step 4</b>	Router(config-preauth)# <b>ctype</b> [ <b>if-avail</b>   <b>required</b> ] [ <b>accept-stop</b> ] [ <b>password</b> <i>string</i> ]	Preauthenticates calls on the basis of the call type.
<b>Step 5</b>	Router(config-preauth)# <b>dnis</b> [ <b>if-avail</b>   <b>required</b> ] [ <b>accept-stop</b> ] [ <b>password</b> <i>string</i> ]	Preauthenticates calls on the basis of the DNIS number.
<b>Step 6</b>	Router(config-preauth)# <b>dnis bypass</b> { <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
<b>Step 1</b>	Router(config)# <b>aaa preauth</b>	Enters AAA preauthentication mode.
<b>Step 2</b>	Router(config-preauth)# <b>group</b> { <b>radius</b>   <b>tacacs+</b>   <i>server-group</i> }	(Optional) Selects the security server to use for AAA preauthentication requests. The default is RADIUS.
<b>Step 3</b>	Router(config-preauth)# <b>dnis</b> [ <b>password</b> <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. <b>Note</b> 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)# <b>isdn guard-timer</b> <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)# <b>call guard-timer</b> <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)# <b>aaa new-model</b>	Enables the AAA access control model.
Step 2	Router(config)# <b>aaa route download min</b>	Enables the download static route feature and sets the amount of time between downloads.
Step 3	Router(config)# <b>aaa authorization configuration default</b>	Downloads static route configuration information from the AAA server using TACACS+ or RADIUS.
Step 4	Router(config)# <b>interface dialer 1</b>	Defines a dialer rotary group.
Step 5	Router(config-if)# <b>dialer aaa</b>	Allows a dialer to access the AAA server for dialing information.
Step 6	Router(config-if)# <b>dialer aaa suffix suffix password password</b>	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# <b>debug radius</b>	Displays information associated with RADIUS.
Router# <b>show radius statistics</b>	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 10.45.1.2
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 10.1.1.1 auth-port 1645 acct-port 1646
  server 10.2.2.2 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 10.2.2.2 auth-port 2000 acct-port 2001
  server 10.3.3.3 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 10.1.1.1 auth-port 1645 acct-port 1646
radius-server host 10.2.2.2 auth-port 2000 acct-port 2001
radius-server host 10.3.3.3 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
  dnis password Cisco-DNIS
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
  dnis required

```

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.

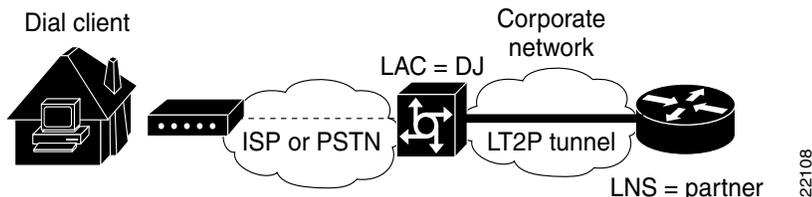
```
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
 cas-custom 0
 call guard-timer 20000 on-expiry accept

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 171.19.1.1 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 hgwl

```

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 10.1.1.1 auth-port 1645 acct-port 1646
radius-server key <deleted>

```

---

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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.

© 2007–2009 Cisco Systems, Inc. All rights reserved.



# AAA Dead-Server Detection

---

**First Published: February 13, 2004**

**Last Updated: May 4, 2009**

The AAA Dead-Server Detection feature allows you to configure the criteria to be used to mark a RADIUS server as dead. If no criteria are explicitly configured, the criteria are 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

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 AAA Dead-Server Detection”](#) section on page 9.

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 7](#)
- [Command Reference, page 8](#)
- [Feature Information for AAA Dead-Server Detection, page 9](#)



---

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

© 2004–2009 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	<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>radius-server deadtime minutes</b>  <b>Example:</b> 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	<b>radius-server dead-criteria [time seconds] [tries number-of-tries]</b>  <b>Example:</b> 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	<code>enable</code>  <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	<code>debug aaa dead-criteria transactions</code>  <b>Example:</b> Router# debug aaa dead-criteria transactions	Displays AAA dead-criteria transaction values.
Step 3	<code>show aaa dead-criteria</code>  <b>Example:</b> Router# show aaa dead-criteria	Displays dead-criteria information for a AAA server.
Step 4	<code>show aaa servers [private   public]</code>  <b>Example:</b> 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"><li>• The <b>private</b> keyword optionally displays the AAA servers only.</li><li>• The <b>public</b> keyword optionally displays the AAA servers only.</li></ul>

## 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	“ <a href="#">Configuring RADIUS</a> ” chapter of <i>Cisco IOS Security Configuration Guide</i>
Configuring AAA	“ <a href="#">Authentication, Authorization, and Accounting (AAA)</a> ” section of <i>Cisco IOS Security Configuration Guide</i>
Security commands	<a href="#">Cisco IOS Security Command Reference</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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### RFCs

RFCs	Title
RFC 2865	<i>Remote Authentication Dial In User Service (RADIUS)</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><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 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 aaa dead-criteria transactions**
- **radius-server dead-criteria**
- **show aaa dead-criteria**
- **show aaa servers**

# Feature Information for AAA Dead-Server Detection

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, Catalyst OS, and Cisco IOS XE 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 Dead-Server Detection

Feature Name	Releases	Feature Information
AAA Dead-Server Detection	12.3(6) 12.3(7)T Cisco IOS XE Release 2.1	Allows you to configure the criteria to be used to mark a RADIUS server as dead.  The following commands were introduced or modified: <b>debug aaa dead-criteria transactions, radius-server dead-criteria, show aaa dead-criteria, show aaa servers.</b>

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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.

© 2004–2009 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>  <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>configure terminal</code>  <b>Example:</b> Router# <code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>radius-server attribute 11 direction default [inbound   outbound]</code>  <b>Example:</b> 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	<code>enable</code>  <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	<code>more system:running-config</code>  <b>Example:</b> Router# more system:running-config	Displays the contents of the current running configuration file.
Step 3	<code>debug radius</code>  <b>Example:</b> 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	<a href="#">Cisco IOS Dial Technologies Configuration Guide</a> , Release 12.4
Cisco IOS security configuration	<a href="#">Cisco IOS Security Configuration Guide</a> , Release 12.4
Cisco IOS security commands	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Security Command Reference</a>, Release 12.4T</li> <li>• <a href="#">Cisco IOS Security Command Reference</a>, Release 12.2SB</li> <li>• <a href="#">Cisco IOS Security Command Reference</a>, Release 12.2 SR</li> </ul>
Configuring IP services	“ <a href="#">Configuring IP Services</a> ” section of the chapter “IP Addressing and Services” of the <a href="#">Cisco IOS IP Addressing Services Configuration Guide</a> , 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## 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.	<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*.

- **radius-server attribute 11 direction default**

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.





# 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	<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>radius-server attribute list</b> <i>listname</i>  <b>Example:</b> Router (config)# radius-server attribute list attrlist	Defines an attribute list.
Step 4	<b>attribute</b> <i>value1</i> [ <i>value2</i> [ <i>value3...</i> ]]  <b>Example:</b> Router (config)# attribute 6-10, 12	Adds attributes to an accept or reject list.
Step 5	<b>aaa group server radius</b> <i>group-name</i>  <b>Example:</b> 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	<pre>authorization [request   reply] [accept   reject] listname</pre> <p>or</p> <pre>accounting [request   reply] [accept   reject] listname</pre> <p><b>Example:</b> Router (config-sg-radius)# <b>authorization</b> request accept attrlist</p> <p>or</p> <p><b>Example:</b> Router (config-sg-radius)# <b>accounting</b> 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"> <li>The <b>request</b> keyword defines filters for outgoing authorization Access Requests.</li> <li>The <b>reply</b> keyword defines filters for incoming authorization Accept and Reject packets and for outgoing accounting requests.</li> </ul>

## 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	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<pre>aaa authorization template</pre> <p><b>Example:</b> 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	<b>aaa authorization network default group radius</b>  <b>Example:</b> Router (config)# aaa authorization network default group radius	Sets parameters that restrict user access to a network.
Step 5	<b>radius-server attribute list list-name</b>  <b>Example:</b> Router (config)# radius-server attribute list attlist	Defines an accept or reject list name.
Step 6	<b>attribute value1 [value2 [value3...]]</b>  <b>Example:</b> 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	<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 radius</b>  <b>Example:</b> 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	<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>
RADIUS attribute lists	<a href="#">RADIUS Attribute Screening</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: <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/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*.

- **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: <b>authorization (server-group)</b>.</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](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 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 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.



# 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	<code>enable</code>  <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	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>aaa user profile profile-name</code>  <b>Example:</b> Router(config)# aaa user profile profilenamel	Creates a user profile.
Step 4	<code>aaa attribute {dnis   clid}</code>  <b>Example:</b> 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	<code>exit</code>	Exit Global Configuration mode.
Step 6	<pre>Router# test aaa group {group-name   radius} username password new-code [profile profile-name]</pre> <p><b>Example:</b></p> <pre>Router# test aaa group radius secret new-code profile profilename1</pre>	<p>Associates a DNIS or CLID named user profile with the record sent to the RADIUS server.</p> <p><b>Note</b> The <i>profile-name</i> must match the <i>profile-name</i> specified in the <b>aaa user profile</b> command.</p>

## Verifying the Enhanced Test Command Configuration

To verify the Enhanced Test Command configuration, use the following commands in privileged EXEC mode:

Command	Purpose
Router# <code>debug radius</code>	Displays information associated with RADIUS.
Router# <code>more system:running-config</code>	Displays the contents of the current running configuration file. (Note that the <b>more system:running-config</b> command has replaced the <b>show running-config</b> 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
    T=NAS-IP-Address[4]                              L=06 V=10.0.1.81
                                                    [1]

*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	<a href="#">Cisco IOS Security Command Reference</a>

### 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### 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><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 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 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: <b>aaa attribute</b>, <b>aaa user profile</b>, <b>test aaa group</b></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: V11 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## 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><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></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](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	The Framed-Route in RADIUS Accounting feature provides for the presence of Framed-Route (RADIUS attribute 22) information in RADIUS Accounting-Request accounting records.  This feature was introduced in Cisco IOS Release 12.3(4)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.

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)# <b>radius-server attribute 44 extend-with-addr</b>	<p>Adds the accounting IP address in front of the existing AAA session ID.</p> <p><b>Note</b> 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).</p>

### 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)# <b>radius-server attribute 44 sync-with-client</b>	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# <b>more system:running-config</b>	Displays the contents of the current running configuration file. (Note that the <b>more system:running-config</b> command has replaced the <b>show running-config</b> command.)
Router(config)# <b>debug radius</b>	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 Documents<sup>1</sup>

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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## 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>	<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 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*.

- **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: May 4, 2009**

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, a customer template can be used, 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

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 Per VRF AAA” section on page 31](#).

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 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 19](#)
- [Additional References, page 29](#)



---

**Americas Headquarters:**

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

- [Command Reference, page 30](#)
- [Feature Information for Per VRF AAA, page 31](#)
- [Glossary, page 32](#)

## 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*.)

## 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 functionality 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
<b>Note</b>		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 <b>aaa accounting delay-start</b> command for the customer template.
account-send-stop	string	This VSA must be “on.” The functionality of this VSA is equal to the <b>aaa accounting send stop-record authentication</b> command with the <b>failure</b> keyword.
account-send-success-remote	string	This VSA must be “on.” The functionality of this VSA is equal to the <b>aaa accounting send stop-record authentication</b> command with the <b>success</b> keyword.
attr-44	string	This VSA must be “access-req.” The functionality of this VSA is equal to the <b>radius-server attribute 44 include-in-access-req</b> 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=192.168.202.169 255.255.255.255
ip-unnumbered	string	This VSA specifies the name of an interface on the router. The functionality of this VSA is equal to the <b>ip unnumbered</b> 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 <b>ip vrf forwarding</b> 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 <b>ip local pool</b> 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 <b>aaa accounting network mylist</b> 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 <b>aaa authentication ppp mylist</b> 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 <b>aaa authorization network mylist</b> 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>
<p><b>Note</b> 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.</p>		
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 <b>radius-server attribute list filtername</b> 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 <b>ip vrf</b> <b>forwarding</b> 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 6](#) (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 18](#) (optional)
- [Troubleshooting Per VRF AAA Configurations, page 19](#) (optional)

## Configuring Per VRF AAA

This section contains the following procedures.

- [Configuring AAA, page 6](#)
- [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	<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 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	<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 globally.

	Command or Action	Purpose
Step 4	<pre>aaa group server radius groupname</pre> <p><b>Example:</b> Router(config)# aaa group server radius v2.44.com</p>	Groups different RADIUS server hosts into distinct lists and distinct methods. Enters server-group configuration mode.
Step 5	<pre>server-private ip-address [auth-port port-number   acct-port port-number] [non-standard] [timeout seconds] [retransmit retries] [key string]</pre> <p><b>Example:</b> Router(config-sg-radius)# server-private 10.10.130.2 auth-port 1600 key ww</p>	<p>Configures the IP address of the private RADIUS server for the group server.</p> <p><b>Note</b> If private server parameters are not specified, global configurations will be used. If global configurations are not specified, default values will be used.</p>
Step 6	<pre>exit</pre> <p><b>Example:</b> Router(config-sg-radius)# exit</p>	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	<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 globally.
Step 4	<b>aaa authentication ppp {default   list-name} method1 [method2...]</b>  <b>Example:</b> 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	<b>aaa authorization {network   exec   commands level   reverse-access   configuration} {default   list-name} method1 [method2...]</b>  <b>Example:</b> 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	<b>aaa accounting system default [vrf vrf-name] {start-stop   stop-only   none} [broadcast] group groupname</b>  <b>Example:</b> 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
<p><b>Step 7</b> <code>aaa accounting delay-start [vrf vrf-name]</code></p> <p><b>Example:</b> Router(config)# aaa accounting delay-start vrf v2.44.com</p>	<p>Displays generation of the start accounting records until the user IP address is established.</p>
<p><b>Step 8</b> <code>aaa accounting send stop-record authentication {failure   success remote-server} [vrf vrf-name]</code></p> <p><b>Example:</b> Router(config)# aaa accounting send stop-record authentication failure vrf v2.44.com</p>	<p>Generates accounting stop records.</p> <p>When using the <b>failure</b> keyword a “stop” record will be sent for calls that are rejected during authentication.</p> <p>When using the <b>success</b> keyword a “stop” record will be sent for calls that meet one of the following criteria:</p> <ul style="list-style-type: none"> <li>• Calls that are authenticated by a remote AAA server when the call is terminated.</li> <li>• Calls that are not authenticated by a remote AAA server and the start record has been sent.</li> <li>• Calls that are successfully established and then terminated with the “stop-only” <b>aaa accounting</b> configuration.</li> </ul> <p><b>Note</b> The <b>success</b> and <b>remote-server</b> keywords are available in Cisco IOS Release 12.4(2)T and later releases.</p> <p><b>Note</b> The <b>success</b> and <b>remote-server</b> keywords are not available in Cisco IOS Release 12.2SX.</p>

## 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	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
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>subinterface-name</i> [ <b>vrf</b> <i>vrf-name</i> ]  <b>Example:</b> 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	<b>radius-server attribute 44</b> <b>include-in-access-req</b> [ <b>vrf</b> <i>vrf-name</i> ]  <b>Example:</b> 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	<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 number [name-tag]</i>  <b>Example:</b> Router(config)# interface loopback11	Configures an interface type and enters interface configuration mode.
Step 4	<b>ip vrf forwarding</b> <i>vrf-name</i>  <b>Example:</b> Router(config-if)# ip vrf forwarding v2.44.com	Associates a VRF with an interface.
Step 5	<b>ppp authentication</b> <i>{protocol1 [protocol2...]} listname</i>  <b>Example:</b> 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	<b>ppp authorization</b> <i>list-name</i>  <b>Example:</b> Router(config-if)# ppp authorization V2_44_com	Enables AAA authorization on the selected interface.
Step 7	<b>ppp accounting default</b>  <b>Example:</b> Router(config-if)# ppp accounting default	Enables AAA accounting services on the selected interface.
Step 8	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits interface configuration mode.

## Configuring Per VRF AAA Using Local Customer Templates

This section contains the following procedures:

- [Configuring AAA, page 13](#)
- [Configuring Server Groups, page 13](#)
- [Configuring Authentication, Authorization, and Accounting for Per VRF AAA, page 13](#)

- [Configuring Authorization for Per VRF AAA with Local Customer Templates, page 13](#)
- [Configuring Local Customer Templates, page 14](#)

## Configuring AAA

Perform the tasks as outlined in the “[Configuring Per VRF AAA](#)” section on page 6.

## 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	<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	<code>aaa authorization template</code>  <b>Example:</b> Router(config)# aaa authorization template	Enables the use of local or remote templates.
Step 4	<code>aaa authorization network default local</code>  <b>Example:</b> 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	<code>enable</code>  <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	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>vpdn search-order domain</code>  <b>Example:</b> Router (config)# vpdn search-order domain	Looks up the profiles based on domain.

	Command or Action	Purpose
Step 4	<p><b>template</b> <i>name</i> [<b>default</b>   <b>exit</b>   <b>multilink</b>   <b>no</b>   <b>peer</b>   <b>ppp</b>]</p> <p><b>Example:</b> Router (config)# template v2.44.com</p>	<p>Creates a customer profile template and assigns a unique name that relates to the customer that will be receiving it.</p> <p>Enters template configuration mode.</p> <p> <b>Note</b> Steps 5, 6, and 7 are optional. Enter <b>multilink</b>, <b>peer</b>, and <b>ppp</b> keywords appropriate to customer application requirements.</p>
Step 5	<p><b>peer default ip address pool</b> <i>pool-name</i></p> <p><b>Example:</b> Router(config-template)# peer default ip address pool v2_44_com_pool</p>	(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	<p><b>ppp authentication</b> {<i>protocol1</i> [<i>protocol2...</i>]} [<b>if-needed</b>] [<i>list-name</i>   <b>default</b>] [<b>callin</b>] [<b>one-time</b>]</p> <p><b>Example:</b> Router(config-template)# ppp authentication chap</p>	(Optional) Sets the PPP link authentication method.
Step 7	<p><b>ppp authorization</b> [<b>default</b>   <i>list-name</i>]</p> <p><b>Example:</b> Router(config-template)# ppp authorization v2_44_com</p>	(Optional) Sets the PPP link authorization method.
Step 8	<p><b>aaa accounting</b> {<b>auth-proxy</b>   <b>system</b>   <b>network</b>   <b>exec</b>   <b>connection</b>   <b>commands level</b>} {<b>default</b>   <i>list-name</i>} [<b>vrf vrf-name</b>] {<b>start-stop</b>   <b>stop-only</b>   <b>none</b>} [<b>broadcast</b>] <b>group</b> <i>groupname</i></p> <p><b>Example:</b> Router(config-template)# aaa accounting v2_44_com</p>	(Optional) Enables AAA operational parameters for the specified customer profile.
Step 9	<p><b>exit</b></p> <p><b>Example:</b> Router(config-template)# exit</p>	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 16](#)
- [Configuring Server Groups, page 16](#)

- [Configuring Authentication for Per VRF AAA with Remote Customer Profiles, page 16](#)
- [Configuring Authorization for Per VRF AAA with Remote Customer Profiles, page 17](#)
- [Configuring the RADIUS Profile on the SP RADIUS Server, page 18](#)

## Configuring AAA

Perform the tasks as outlined in the “[Configuring Per VRF AAA](#)” section on page 6.

## Configuring Server Groups

Perform the tasks as outlined in the “[Configuring Server Groups](#)” section on page 13.

## 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	<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	<pre>aaa authentication ppp {default   list-name} method1 [method2...]</pre> <p><b>Example:</b> Router(config)# ppp authentication ppp default group radius</p>	Specifies one or more authentication, authorization, and accounting (AAA) authentication methods for use on serial interfaces that are running PPP.
Step 4	<pre>aaa authorization {network   exec   commands level   reverse-access   configuration} {default   list-name} [[method1 [method2...]]</pre> <p><b>Example:</b> Router(config)# aaa authorization network default group sp</p>	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	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal</p>	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<code>aaa authorization template</code>	Enables use of local or remote templates.
	<b>Example:</b> Router(config)# aaa authorization template	
Step 4	<code>aaa authorization {network   exec   commands level   reverse-access   configuration} {default   list-name} [[method1 [method2...]]</code>	Specifies the server group that is named as the default method for authorization.
	<b>Example:</b> Router(config)# aaa authorization network default sp	

## Configuring the RADIUS Profile on the SP RADIUS Server

Configure the RADIUS profile on the Service Provider (SP) RADIUS server. See the [“Per VRF AAA Using a Remote RADIUS Customer Template: Example” section on page 20](#) 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	<code>enable</code>	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	<code>configure terminal</code>	Enters global configuration mode.
	<b>Example:</b> Router# configure terminal	
Step 3	<code>show ip route vrf vrf-name</code>	Displays the IP routing table associated with a VRF.
	<b>Example:</b> Router(config)# show ip route vrf northvrf	

## 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# <code>debug aaa accounting</code>	Displays information on accountable events as they occur.
Router# <code>debug aaa authentication</code>	Displays information on AAA authentication.
Router# <code>debug aaa authorization</code>	Displays information on AAA authorization.
Router# <code>debug ppp negotiation</code>	Displays information on traffic and exchanges in an internetwork implementing PPP.
Router# <code>debug radius</code>	Displays information associated with RADIUS.
Router# <code>debug vpdn event</code>	Displays Layer 2 Transport Protocol (L2TP) errors and events that are a part of normal tunnel establishment or shutdown for VPNs.
Router# <code>debug vpdn error</code>	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 21](#)
- [AAA Accounting Stop Records: Examples, page 23](#)

### 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 20](#)
- [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 21](#)
- [Remotely Configured Customer Template with RADIUS Attribute Screening and Broadcast Accounting: Example, page 22](#)

### 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 SCCRP, 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 SCCRP
*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 SCCRP
*Jul 7 03:28:33.571: Tnl 5192 L2TP: I SCCRP, 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 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 tnlid 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@example.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@example.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=10.0.0.2"
*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 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 "10.0.0.1"
*Jul 7 03:39:49.279: RADIUS: Tunnel-Server-Endpoi[67] 10 "10.0.0.2"
*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@example.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	<a href="#">Cisco IOS Security Configuration Guide</a> , Release 12.4
RADIUS Attribute Screening	
RADIUS Debug Enhancements	
Broadcast Accounting	<a href="#">AAA Broadcast Accounting</a> , Release 12.1(1)T
Cisco IOS Security Commands	<a href="#">Cisco IOS Security Command Reference</a>
Cisco IOS Switching Services Commands	<a href="#">Cisco Switching Services Command Reference</a>
Configuring Multiprotocol Label Switching	“Configuring Multiprotocol Label Switching” chapter in the <a href="#">Cisco IOS Switching Services Configuration Guide</a> , Release 12.2
Configuring Virtual Templates section	“Virtual Templates, Profiles, and Networks” chapter in the <a href="#">Cisco IOS Dial Technologies Configuration Guide</a> , Release 12.2

## 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.	—

## 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 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**
- **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.

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, Catalyst OS, and Cisco IOS XE 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 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)SR 12.2(33)SXI 12.2(33)SXH4 Cisco IOS XE Release 2.1	<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 <b>ip vrf forwarding (server-group)</b> and <b>radius-server domain-stripping</b> commands were added.</p> <p>In 12.2(15)T, the <b>aaa authorization template</b> command was added.</p> <p>In 12.4(2)T, the <b>aaa accounting send stop-record authentication</b> 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> <p>In Cisco IOS Release 12.2(33)SXI, this feature was introduced.</p> <p>In Cisco IOS Release 12.2(33)SXH4, this feature was introduced.</p> <p>The following commands were introduced or modified: <b>aaa accounting</b>, <b>aaa accounting delay-start</b>, <b>ip radius source-interface</b>, <b>radius-server attribute 44 include-in-access-req</b>, <b>server-private (RADIUS)</b>.</p> <p>In Cisco IOS XE Release 2.1, this feature was implemented on the Cisco ASR 1000 series routers.</p>

# 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.

**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.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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

© 2001–2009 Cisco Systems, Inc. All rights reserved.



# RFC-2867 RADIUS Tunnel Accounting

---

**First Published: November 3, 2003**

**Last Updated: July 6, 2009**

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 virtual private virtual private dialup network (VPDN) commands that help users better troubleshoot VPDN session events.

## 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 RFC-2867 RADIUS Tunnel Accounting” section on page 14](#).

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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. An account on Cisco.com is not required.

## 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 12](#)
- [Command Reference, page 12](#)



---

**Americas Headquarters:**

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

# 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 <sup>1</sup>
Tunnel-Start	9	Marks the beginning of a tunnel setup with another node.	<ul style="list-style-type: none"> <li>• User-Name (1)—from client</li> <li>• NAS-IP-Address (4)—from AAA</li> <li>• Acct-Delay-Time (41)—from AAA</li> <li>• Event-Timestamp (55)—from AAA</li> <li>• Tunnel-Type (64)—from client</li> <li>• Tunnel-Medium-Type (65)—from client</li> <li>• Tunnel-Client-Endpoint (66)—from client</li> <li>• Tunnel-Server-Endpoint (67)—from client</li> <li>• Acct-Tunnel-Connection (68)—from client</li> </ul>
Tunnel-Stop	10	Marks the end of a tunnel connection to or from another node.	<ul style="list-style-type: none"> <li>• User-Name (1)—from client</li> <li>• NAS-IP-Address (4)—from AAA</li> <li>• Acct-Delay-Time (41)—from AAA</li> <li>• Acct-Input-Octets (42)—from AAA</li> <li>• Acct-Output-Octets (43)—from AAA</li> <li>• Acct-Session-Id (44)—from AAA</li> <li>• Acct-Session-Time (46)—from AAA</li> <li>• Acct-Input-Packets (47)—from AAA</li> <li>• Acct-Output-Packets (48)—from AAA</li> <li>• Acct-Terminate-Cause (49)—from AAA</li> <li>• Acct-Multi-Session-Id (51)—from AAA</li> <li>• Event-Timestamp (55)—from AAA</li> <li>• Tunnel-Type (64)—from client</li> <li>• Tunnel-Medium-Type (65)—from client</li> <li>• Tunnel-Client-Endpoint (66)—from client</li> <li>• Tunnel-Server-Endpoint (67)—from client</li> <li>• Acct-Tunnel-Connection (68)—from client</li> <li>• Acct-Tunnel-Packets-Lost (86)—from client</li> </ul>

**Table 1** RADIUS Accounting Types for the Acct-Status-Type Attribute (continued)

Type-Name	Number	Description	Additional Attributes <sup>1</sup>
Tunnel-Reject	11	Marks the rejection of a tunnel setup with another node.	<ul style="list-style-type: none"> <li>• User-Name (1)—from client</li> <li>• NAS-IP-Address (4)—from AAA</li> <li>• Acct-Delay-Time (41)—from AAA</li> <li>• Acct-Terminate-Cause (49)—from client</li> <li>• Event-Timestamp (55)—from AAA</li> <li>• Tunnel-Type (64)—from client</li> <li>• Tunnel-Medium-Type (65)—from client</li> <li>• Tunnel-Client-Endpoint (66)—from client</li> <li>• Tunnel-Server-Endpoint (67)—from client</li> <li>• Acct-Tunnel-Connection (68)—from client</li> </ul>
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"> <li>• User-Name (1)—from client</li> <li>• NAS-IP-Address (4)—from AAA</li> <li>• NAS-Port (5)—from AAA</li> <li>• Acct-Delay-Time (41)—from AAA</li> <li>• Event-Timestamp (55)—from AAA</li> <li>• Tunnel-Type (64)—from client</li> <li>• Tunnel-Medium-Type (65)—from client</li> <li>• Tunnel-Client-Endpoint (66)—from client</li> <li>• Tunnel-Server-Endpoint (67)—from client</li> <li>• Acct-Tunnel-Connection (68)—from client</li> </ul>

**Table 1** RADIUS Accounting Types for the Acct-Status-Type Attribute (continued)

Type-Name	Number	Description	Additional Attributes <sup>1</sup>
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"> <li>• User-Name (1)—from client</li> <li>• NAS-IP-Address (4)—from AAA</li> <li>• NAS-Port (5)—from AAA</li> <li>• Acct-Delay-Time (41)—from AAA</li> <li>• Acct-Input-Octets (42)—from AAA</li> <li>• Acct-Output-Octets (43)—from AAA</li> <li>• Acct-Session-Id (44)—from AAA</li> <li>• Acct-Session-Time (46)—from AAA</li> <li>• Acct-Input-Packets (47)—from AAA</li> <li>• Acct-Output-Packets (48)—from AAA</li> <li>• Acct-Terminate-Cause (49)—from AAA</li> <li>• Acct-Multi-Session-Id (51)—from AAA</li> <li>• Event-Timestamp (55)—from AAA</li> <li>• NAS-Port-Type (61)—from AAA</li> <li>• Tunnel-Type (64)—from client</li> <li>• Tunnel-Medium-Type (65)—from client</li> <li>• Tunnel-Client-Endpoint (66)—from client</li> <li>• Tunnel-Server-Endpoint (67)—from client</li> <li>• Acct-Tunnel-Connection (68)—from client</li> <li>• Acct-Tunnel-Packets-Lost (86)—from client</li> </ul>
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"> <li>• User-Name (1)—from client</li> <li>• NAS-IP-Address (4)—from AAA</li> <li>• Acct-Delay-Time (41)—from AAA</li> <li>• Acct-Terminate-Cause (49)—from AAA</li> <li>• Event-Timestamp (55)—from AAA</li> <li>• Tunnel-Type (64)—from client</li> <li>• Tunnel-Medium-Type (65)—from client</li> <li>• Tunnel-Client-Endpoint (66)—from client</li> <li>• Tunnel-Server-Endpoint (67)—from client</li> <li>• Acct-Tunnel-Connection (68)—from client</li> </ul>

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	<code>enable</code>  <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	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# <code>aaa accounting network</code> { <code>default</code>   <code>list-name</code> } { <code>start-stop</code>   <code>stop-only</code>   <code>wait-start</code>   <code>none</code> } <code>group groupname</code>	Enables network accounting. <ul style="list-style-type: none"> <li><b>default</b>—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 <b>vpdn session accounting network</b> command or the <b>vpdn tunnel accounting network</b> command is linked to the <b>default</b> method-list, all tunnel and tunnel-link accounting records are enabled for those sessions.</li> <li><i>list-name</i>—The <i>list-name</i> defined in the <b>aaa accounting</b> command must be the same as the <i>list-name</i> defined in the VPDN command; otherwise, accounting will not occur.</li> </ul>
Step 4	Router(config)# <code>vpdn enable</code>	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)# <code>vpdn tunnel accounting network</code> <i>list-name</i>	Enables Tunnel-Start, Tunnel-Stop, and Tunnel-Reject accounting records. <ul style="list-style-type: none"> <li><i>list-name</i>—The <i>list-name</i> must match the <i>list-name</i> defined in the <b>aaa accounting</b> command; otherwise, network accounting will not occur.</li> </ul>
Step 6	Router(config)# <code>vpdn session accounting network</code> <i>list-name</i>	Enables Tunnel-Link-Start, Tunnel-Link-Stop, and Tunnel-Link-Reject accounting records. <ul style="list-style-type: none"> <li><i>list-name</i>—The <i>list-name</i> must match the <i>list-name</i> defined in the <b>aaa accounting</b> command; otherwise, network accounting will not occur.</li> </ul>

## 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	<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	Router# <b>show accounting</b>	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# <b>show vpdn [session] [tunnel]</b>	Displays information about active L2TP tunnel and message identifiers in a VPDN. <ul style="list-style-type: none"> <li>• <b>session</b>—Displays a summary of the status of all active tunnels.</li> <li>• <b>tunnel</b>—Displays information about all active L2TP tunnels in summary-style format.</li> </ul>

## 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### RFCs

RFCs	Title
RFC 2867	<i>RADIUS Accounting Modifications for Tunnel Protocol Support</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><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

# Feature Information for RFC-2867 RADIUS Tunnel Accounting

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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. 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 RFC-2867 RADIUS Tunnel Accounting

Feature Name	Releases	Feature Information
RFC-2867 RADIUS Tunnel Accounting	12.2(15)B 12.3(4)T Cisco IOS XE Release 2.1	<p>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).</p> <p>This feature also introduces two virtual private virtual private dialup network (VPDN) commands that help users better troubleshoot VPDN session events.</p> <p>In 12.2(15)B, this feature was introduced on the Cisco 6400 series, Cisco 7200 series, and the Cisco 7400 series routers.</p> <p>This feature was integrated into Cisco IOS Release 12.3(4)T.</p> <p>This feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>The following commands were introduced or modified: <b>aaa accounting</b>, <b>vpdn session accounting network</b>, <b>vpdn tunnel accounting network</b>.</p>

---

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

---

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

© 2003–2009 Cisco Systems, Inc. All rights reserved.

---





## RADIUS Attribute Screening

---

**First Published: May 18, 2001**

**Last Published: July 7, 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

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 RADIUS Attribute Screening” section on page 10](#).

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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. 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
- 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	<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	Router(config)# <b>aaa authentication ppp default group group-name</b>	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
Step 4	Router(config)# <b>aaa authorization network default group group-name</b>	Sets parameters that restrict network access to the user.
Step 5	Router(config)# <b>aaa group server radius group-name</b>	Groups different RADIUS server hosts into distinct lists and distinct methods.
Step 6	Router(config-sg-radius)# <b>server ip-address</b>	Configures the IP address of the RADIUS server for the group server,
Step 7	Router(config-sg-radius)# <b>authorization [accept   reject] listname</b>  and/or  Router(config-sg-radius)# <b>accounting [accept   reject] listname</b>	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.  <b>Note</b> The <b>accept</b> keyword indicates that all attributes are rejected except for the attributes specified in the <i>listname</i> . The <b>reject</b> 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)# <b>exit</b>	Exits server-group configuration mode.
Step 9	Router(config)# <b>radius-server host {hostname   ip-address} [key string]</b>	Specifies a RADIUS server host.
Step 10	Router(config)# <b>radius-server attribute list listname</b>	Defines the list name given to the set of attributes defined in the <b>attribute</b> command.  <b>Note</b> The <i>listname</i> must be the same as the <i>listname</i> defined in Step 5.
Step 11	Router(config-sg-radius)# <b>attribute value1 [value2 [value3...]]</b>	Adds attributes to the configured accept or reject list.  <b>Note</b> 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# <b>debug aaa accounting</b>	Displays information on accountable events as they occur.
Router# <b>debug aaa authentication</b>	Displays information on AAA authentication.
Router# <b>show radius statistics</b>	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	<i>Cisco IOS Security Command Reference, Release 12.4T</i>
	<i>Cisco IOS Security Configuration Guide, Release 12.4</i>
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: <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 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><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

# 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: <b>accounting (server-group configuration)</b>, <b>authorization (server-group configuration)</b>, <b>attribute (server-group configuration)</b>, <b>radius-server attribute list</b></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
<pre>Router(config)# <b>aaa authorization cache</b> <b>filterserver default</b> <i>methodlist[methodlist2...]</i></pre>	<p>Enables AAA authorization caches and the downloading of an ACL configuration from a RADIUS filter server.</p> <ul style="list-style-type: none"> <li>• <b>default</b>—The default authorization list.</li> <li>• <i>methodlist [methodlist2...]</i>—One of the keywords listed on the <b>password</b> command page.</li> </ul>

## Configuring the Filter Cache

Follow the steps in this section to configure the AAA filter cache.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa cache filter**
4. **password {0 | 7} password**
5. **cache disable**
6. **cache clear age minutes**
7. **cache refresh**
8. **cache max number**

	Command	Purpose
Step 1	<pre><b>enable</b></pre> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre><b>configure terminal</b></pre> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<pre>Router(config)# <b>aaa cache filter</b></pre>	<p>Enables filter cache configuration and enters AAA filter configuration mode.</p>

	Command	Purpose
Step 4	Router(config-aaa-filter)# <b>password</b> {0   7} <i>password</i>	(Optional) Specifies the optional password that is to be used for filter server authentication requests. <b>0</b> —Specifies that an unencrypted password will follow. <b>7</b> —Specifies that a hidden password will follow. <i>password</i> —The unencrypted (clear text) password. <b>Note</b> If a password is not specified, the default password (“cisco”) is enabled.
Step 5	Router(config-aaa-filter)# <b>cache disable</b>	(Optional) Disables the cache.
Step 6	Router(config-aaa-filter)# <b>cache clear age</b> <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. <b>Note</b> If a time is not specified, the default (1400 minutes [1 day]) is enabled.
Step 7	Router(config-aaa-filter)# <b>cache refresh</b>	(Optional) Refreshes a cache entry when a new session begins. This command is enabled by default. To disable this functionality, use the <b>no cache refresh</b> command.
Step 8	Router(config-aaa-filter)# <b>cache max</b> <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. <b>Note</b> 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# <b>clear aaa cache filterserver acl</b> [ <i>filter-name</i> ]	Clears the cache status for a particular filter or all filters.
Router# <b>show aaa cache filterserver</b>	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: rcv 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	“ <a href="#">Configuring Authorization</a> ” chapter in the <i>Cisco IOS Security Configuration Guide</i>
Configuring RADIUS	“ <a href="#">Configuring RADIUS</a> ” chapter in the <i>Cisco IOS Security Configuration Guide</i>
Authorization Commands	<a href="#">Cisco IOS Security Command Reference</a>

### 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### 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><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 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 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: <b>aaa authorization cache filterserver</b>, <b>aaa cache filter</b>, <b>cache clear age</b>, <b>cache disable</b>, <b>cache refresh</b>, <b>clear aaa cache filterserver acl</b>, <b>debug aaa cache filterserver</b>, <b>password</b>, <b>show aaa cache filterserver</b>.</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

---

**First Published: August 12, 2002**  
**Last Updated: May 29, 2009**

This document describes the Remote Authentication Dial-In User Services (RADIUS) Debug Enhancements feature.

## 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 RADIUS Debug Enhancements”](#) section on page 8.

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 Debug Enhancements, page 2](#)
- [Restrictions for RADIUS Debug Enhancements, page 2](#)
- [Information About RADIUS Debug Enhancements, page 2](#)
- [How to Enable RADIUS Debug Parameters, page 3](#)
- [Configuration Examples for RADIUS Debug Enhancements, page 4](#)
- [Additional References, page 6](#)
- [Command Reference, page 7](#)
- [Feature Information for RADIUS Debug Enhancements, page 8](#)
- [Glossary, page 9](#)



---

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

## Prerequisites for RADIUS Debug Enhancements

- Establish a working IP network. For more information about configuring IP refer to the [Configuring IPv4 Addresses](#) module.
- Configure the gateway as a RADIUS client. Refer to the section “Configuring the Voice Gateway as a RADIUS Client ” section in the [CDR Accounting for Cisco IOS Voice Gateways document](#).
- Be familiar with IETF RFC 2138.

## Restrictions for RADIUS Debug Enhancements

Only Internet Engineering Task Force (IETF) attributes and Cisco vendor-specific attributes (VSAs) used in voice applications are supported. For unsupported attributes, “undebuggable” is displayed.

## Information About RADIUS Debug Enhancements

To enable RADIUS Debug parameters, you should understand the following concepts:

- [RADIUS Overview](#), page 2
- [Benefits of RADIUS Debug Enhancements](#), page 3

## RADIUS Overview

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.

## Benefits of RADIUS Debug Enhancements

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 VSAs.

This 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.
- Allows a compact debugging output option that is useful for high-traffic, operational environments.

# How to Enable RADIUS Debug Parameters

This section contains the following procedures:

- [Enabling RADIUS Debug Parameters, page 3](#) (optional)
- [Verifying RADIUS Debug Parameters](#) (optional)

## Enabling RADIUS Debug Parameters

Perform this task to enable RADIUS debug parameters. By default, event logging is enabled.



### Note

Prior to Cisco IOS Release 12.2(11)T, the **debug radius** command enabled truncated debugging output in hexadecimal notation, rather than ASCII.

### SUMMARY STEPS

1. **enable**
2. **debug radius** [**accounting** | **authentication** | **brief** | **elog** | **failover** | **retransmit** | **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 radius</b> [ <b>accounting</b>   <b>authentication</b>   <b>brief</b>   <b>elog</b>   <b>failover</b>   <b>retransmit</b>   <b>verbose</b> ]  <b>Example:</b> Router# debug radius accounting	Enables debugging for the specified parameters associated with RADIUS configuration.

## Verifying RADIUS Debug Parameters

Perform this task to verify RADIUS debug parameters.

### SUMMARY STEPS

1. **enable**
2. **show debug**

## 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 debug</b>  <b>Example:</b> Router# show debug	Displays debug information.

## Configuration Examples for RADIUS Debug Enhancements

This section provides the following configuration examples:

- [Enabling RADIUS Debug Parameters: Example, page 4](#)
- [Verifying RADIUS Debug Parameters: Example, page 4](#)

### Enabling RADIUS Debug Parameters: Example

The following example shows how to enable debugging of RADIUS accounting collection.

```
Router> enable
Router# debug radius accounting
```

```
Radius protocol debugging is on
Radius protocol brief debugging is off
Radius protocol verbose debugging is off
Radius packet hex dump debugging is off
Radius packet protocol (authentication) debugging is off
Radius packet protocol (accounting) debugging is on
Radius packet retransmission debugging is off
Radius server fail-over debugging is off
Radius elog debugging is off
```


**Note**

The sample output above displays information that is found inside a RADIUS protocol message. For more information about RADIUS protocol messages, see IETF RFC 2138.

### Verifying RADIUS Debug Parameters: Example

The following example shows how to verify RADIUS debug parameters.

```
Router> enable
Router# show debug
```

```
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-tme=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-tme=*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

```

## Additional References

The following sections provide references related to the RADIUS Debug Enhancements feature.

## Related Documents

Related Topic	Document Title
Configuring RADIUS	“Configuring RADIUS Accounting” module of the <i>CDR Accounting for Cisco IOS Voice Gateways</i> document.
Debug commands: complete command syntax, defaults, command mode, command history, usage guidelines, and examples	<i>Cisco IOS Debug 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: <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, and support for existing RFCs has not been modified.	—

## 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 Debug Command Reference* at [http://www.cisco.com/en/US/docs/ios/debug/command/reference/db\\_book.html](http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_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 radius**
- **show debug**

# Feature Information for RADIUS Debug Enhancements

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 Debug Enhancements

Feature Name	Releases	Feature Information
RADIUS Debug Enhancements	12.2(11)T	<p>This feature provides enhancements to the existing functionality of RADIUS debug parameters.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li><a href="#">Information About RADIUS Debug Enhancements, page 2</a></li> </ul> <p>The following commands were introduced or modified: <b>debug radius</b> and <b>show debug</b>.</p>

# 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.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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

© 2002-2009 Cisco Systems, Inc. All rights reserved.





# RADIUS Logical Line ID

---

**First Published: November 25, 2002**

**Last Updated: July 7, 2009**

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

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 RADIUS Logical Line ID” section on page 9](#).

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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. 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](#)
- [Feature Information for RADIUS Logical Line ID, page 9](#)
- [Glossary, page 11](#)



---

**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.

## 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	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
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 Loopback1	Specifies the IP address portion of the username for the preauthorization request.
Step 4	<b>subscriber access</b> {pppoe   pppoa} <b>pre-authorize nas-port-id</b> [default   <i>list-name</i> ][ <b>send username</b> ]  <b>Example:</b> 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 <b>send username</b> 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"> <li>• String—One or more octets, containing the phone number from which the user placed the call.</li> </ul>

## 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>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>debug radius</code>  <b>Example:</b> <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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## 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><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

# 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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. 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 <b>send username</b> keyword was added to the <b>subscriber access</b> 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 <b>subscriber access</b> 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**

<b>Feature Name</b>	<b>Releases</b>	<b>Feature Information</b>
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, 2005–2009 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.

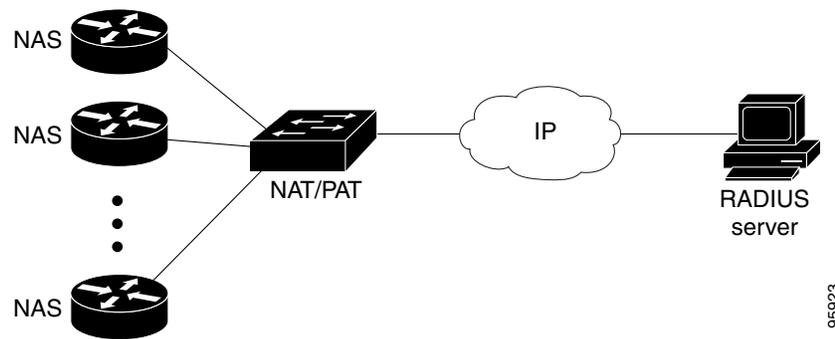
## Information About RADIUS NAS-IP-Address Attribute Configurability

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	<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>radius-server attribute 4 ip-address</b>  <b>Example:</b> 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	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
Step 2	<b>debug radius</b>  <b>Example:</b> Router# debug radius	Displays information associated with 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	“ <a href="#">Configuring RADIUS</a> ” chapter of <i>Cisco IOS Security Configuration Guide</i>
RADIUS 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.

- **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](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 12.3(7)T 12.2(28)SB 12.2(33)SRC Cisco IOS XE Release 2.1	<p>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.</p> <p>This feature was introduced into Cisco IOS Release 12.3(3)B.</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 <b>radius-server attribute 4</b> command was introduced 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.

© 2003–2004, 2006–2007 Cisco Systems, Inc. All rights reserved.





# RADIUS Route Download

---

**First Published: February 25, 2002**  
**Last Updated: September 22, 2008**

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

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 RADIUS Route Download”](#) section on page 6.

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.



---

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

© 2002–2008 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.

## 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)# <b>aaa authorization configuration</b> <i>method-name</i> [ <b>radius</b>   <b>tacacs+</b>   <b>group</b> <i>group-name</i> ]	Downloads static route configuration information from the AAA server using RADIUS.
Step 2	Router(config)# <b>aaa route download</b> [ <i>time</i> ] [ <b>authorization</b> <i>method-list</i> ]	Enables the static route download feature. Use the <b>authorization</b> <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
Configuring Large-Scale Dial-Out	“Configuring Large-Scale Dial-Out” chapter in the <i>Cisco IOS Dial Technologies Configuration Guide</i> ,
Cisco IOS Dial Technologies	<a href="#">Cisco IOS Dial Technologies Command Reference</a>

### 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### 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><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 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 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 Cisco IOS XE Release 2.2	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.  In Cisco IOS XE Release 2.2, this feature was introduced on Cisco ASR 1000 Series Routers  The <b>aaa route download</b> command was introduced by this feature.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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 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	<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>radius-server unique-ident <i>id</i></code>  <b>Example:</b> Router(config)# <code>radius-server unique-ident 5</code>	Enables the acct-session-id-count variable containing the unique identifier variable. <ul style="list-style-type: none"> <li>• 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.</li> </ul>

# 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: <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 <sup>1</sup>	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.	<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*.

- **radius-server unique-iden**

---

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 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.

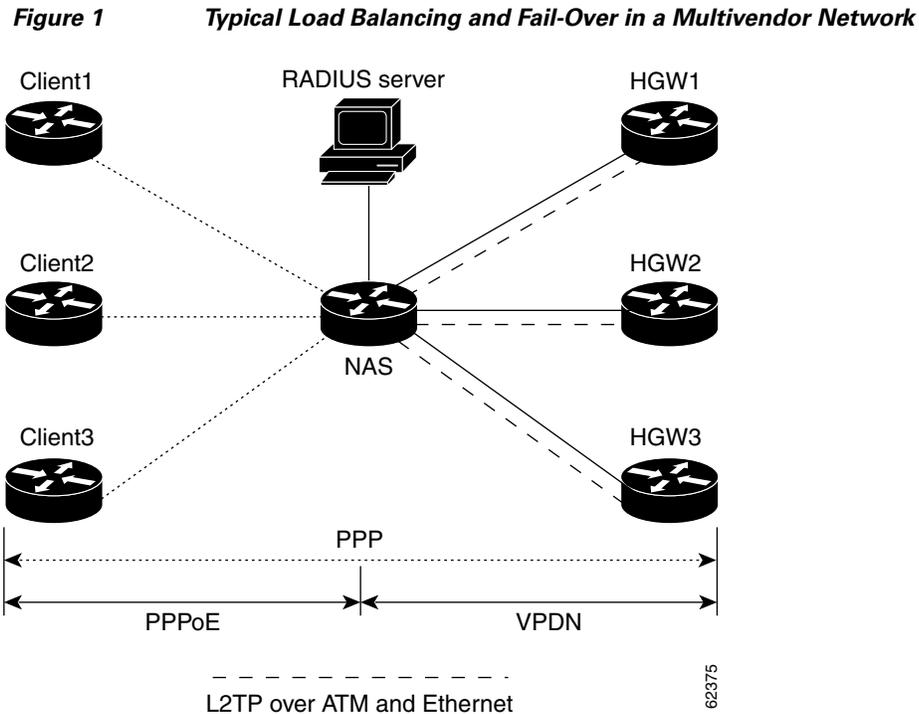
A consensus regarding the tunnel attributes that are to be used in a multivendor network environment is defined in RFC 2868. In RFC 2868, Tunnel-Server-Endpoint, in conjunction with the Tunnel-Medium-Type, specifies the address to which the NAS should initiate a new session. If multiple Tunnel-Server-Endpoint 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](#).



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](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](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](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 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.

---

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 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	<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>radius-server retry method reorder</b>  <b>Example:</b> Router (config)# radius-server retry method reorder	Specifies the reordering of RADIUS traffic retries among a server group.
Step 5	<b>radius-server retransmit</b> <i>{retries}</i>  <b>Example:</b> 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	<p><b>radius-server transaction max-tries</b> <i>{number}</i></p> <p><b>Example:</b> Router (config)# radius-server transaction max-tries 3</p>	<p>Specifies the maximum number of transmissions per transaction that may be retried on a RADIUS server.</p> <p>The <i>number</i> argument is the total number of transmissions per transaction. If this command is not configured, the default is eight transmissions.</p> <p><b>Note</b> This command is global across all RADIUS servers for a given transaction.</p>
Step 7	<p><b>radius-server host</b> <i>{hostname   ip-address}</i> [<b>key string</b>]</p> <p><b>Example:</b> Router (config)# radius-server host 10.2.3.4 key radi23</p>	<p>Specifies a RADIUS server host.</p> <p><b>Note</b> You can also configure a global key for all RADIUS servers that do not have a per-server key configured by issuing the <b>radius-server key</b> command.</p>
Step 8	<p><b>radius-server host</b> <i>{hostname   ip-address}</i> [<b>key string</b>]</p> <p><b>Example:</b> Router (config)# radius-server host 10.5.6.7 key rad234</p>	<p>Specifies a RADIUS server host.</p> <p><b>Note</b> At least two servers must be configured.</p>

## 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	<code>enable</code>  <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	<code>debug aaa sg-server selection</code>  <b>Example:</b> 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	<code>debug radius</code>  <b>Example:</b> 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:~8:59: 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 “ <a href="#">Configuring RADIUS</a> ” in the <i>Cisco IOS Security Configuration Guide</i>
AAA and RADIUS commands	<a href="#">Cisco IOS Security Command Reference</a>
Enabling AAA	“ <a href="#">AAA Overview</a> ” 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: <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 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 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	<p>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.</p> <p>This feature was introduced in 12.3(1).</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: <b>debug aaa sg-server selection, radius-server retry method reorder, radius-server transaction max-tries.</b></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.



# Tunnel Authentication via RADIUS on Tunnel Terminator

---

**First Published: November 3, 2003**  
**Last Updated: July 9, 2009**

The Tunnel Authentication via RADIUS on Tunnel Terminator feature allows tunnel authentication and authorization to occur through a remote RADIUS server instead of local configuration on the tunnel terminator. Thus, users no longer have to configure L2TP access concentrator (LAC) or Layer 2 Tunneling Protocol (L2TP) network server (LNS) data in a virtual private dialup network (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.

## 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 Tunnel Authentication via RADIUS on Tunnel Terminator” section on page 9](#).

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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for Tunnel Authentication via RADIUS on Tunnel Terminator, page 2](#)
- [Restrictions for Tunnel Authentication via RADIUS on Tunnel Terminator, page 2](#)
- [Information About Tunnel Authentication via RADIUS on Tunnel Terminator, page 2](#)
- [How to Configure Tunnel Authentication via RADIUS on Tunnel Terminator, page 4](#)



---

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

- [Configuration Examples for Tunnel Authentication via RADIUS on Tunnel Terminator](#), page 6
- [Additional References](#), page 7
- [Feature Information for Tunnel Authentication via RADIUS on Tunnel Terminator](#), page 9
- [Glossary](#), page 9

## Prerequisites for Tunnel Authentication via RADIUS on Tunnel Terminator

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: Securing User Services*.

**Note**

---

The service-type in the RADIUS user’s profile for the tunnel initiator should always be set to “Outbound.”

---

## Restrictions for Tunnel Authentication via RADIUS on Tunnel Terminator

The Tunnel Authentication via RADIUS on Tunnel Terminator feature is applicable only to L2TP; that is, protocols such as (Layer 2 Forwarding) L2F and Point-to-Point Tunneling Protocol (PPTP) are not supported.

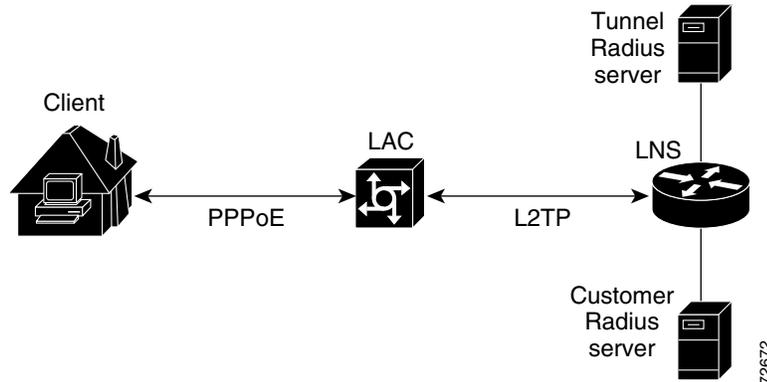
## Information About Tunnel Authentication via RADIUS on Tunnel Terminator

The Tunnel Authentication via RADIUS on Tunnel Terminator feature allows the LNS to perform remote authentication and authorization with RADIUS on incoming 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 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 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.)

## How to Configure Tunnel Authentication via RADIUS on Tunnel Terminator

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

The following task is used to configure an LNS or LAC for incoming dialin or dialout L2TP tunnel termination.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authorization network {default | list-name} method1 [method2...]**
4. **vpdn tunnel authorization network {method-list-name | default}**
5. **vpdn tunnel authorization virtual-template vtemplate-number**
6. **vpdn tunnel authorization password password**

	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 authorization network {default   list-name} method1 [method2...]</b>  <b>Example:</b> Router(config)# aaa authorization network mymethodlist group VPDN-Group	Defines an AAA authorization method list for network services.

	Command	Purpose
Step 4	<b>vpdn tunnel authorization network</b> <i>{method-list-name   default}</i>  <b>Example:</b> Router(config)# vpdn tunnel authorization network mymethodlist	Specifies the AAA authorization method list that will be used for remote tunnel hostname-based authorization. <ul style="list-style-type: none"> <li>If the <i>list-name</i> argument was specified in the <b>aaa authorization</b> command, you use that list name here.</li> <li>If the default keyword was specified in the <b>aaa authorization</b> command, you must choose that keyword, which specifies the default authorization methods that are listed with the <b>aaa authorization</b> command here.</li> </ul>
Step 5	<b>vpdn tunnel authorization virtual-template</b> <i>vtemplate-number</i>  <b>Example:</b> Router(config)# vpdn tunnel authorization virtual-template 10	(Optional) Selects the default virtual template from which to clone virtual access interfaces.
Step 6	<b>vpdn tunnel authorization password</b> <i>password</i>  <b>Example:</b> Router(config)# vpdn tunnel authorization password cisco	(Optional) Configures a “dummy” password for the RADIUS authorization request to retrieve the tunnel configuration that is based on the remote tunnel hostname.  <b>Note</b> If this command is not enabled, the password will always be “cisco.”

## 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:"csidtw13"
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 for Tunnel Authentication via RADIUS on Tunnel Terminator

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"
```

## Additional References

The following sections provide references related to the Tunnel Authentication via RADIUS on Tunnel Terminator feature.

## Related Documents

Related Topic	Document Title
VPNs	The chapter "Configuring Virtual Private Networks" in the <a href="#">Cisco IOS Dial Technologies Configuration Guide</a> .
RADIUS Attributes	<a href="#">Cisco IOS Security Configuration Guide: Securing User Services</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 standards are supported by this feature, and support for existing standards 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

RFC	Title
RFC 2868	<i>RADIUS Attributes for Tunnel Protocol Support</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>

# Feature Information for Tunnel Authentication via RADIUS on Tunnel Terminator

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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. 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 Tunnel Authentication via RADIUS on Tunnel Terminator

Feature Name	Releases	Feature Information
Tunnel Authentication via RADIUS on Tunnel Terminator	12.2(15)B 12.3(4)T	<p>The Tunnel Authentication via RADIUS on Tunnel Terminator feature allows tunnel authentication and authorization to occur through a remote RADIUS server instead of local configuration on the tunnel terminator.</p> <p>In 12.2(15)B, this feature was introduced on the Cisco 6400 series, Cisco 7200 series, and Cisco 7400 series.</p> <p>In 12.3(4)T, this feature was integrated into the Cisco IOS.</p> <p>The following commands were introduced or modified:  <b>vpdn tunnel authorization network, vpdn tunnel authorization password, vpdn tunnel authorization virtual-template.</b></p>

## 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.

---

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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

© 2003–2009 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 implemented on the 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, see the *Cisco IOS Security Command Reference*. To locate documentation of other commands that appear in this chapter, use 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).

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.

## 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

© 2007–2009 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 the 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)# <b>tacacs-server host</b> <i>hostname</i> [ <b>single-connection</b> ] [ <b>port</b> <i>integer</i> ] [ <b>timeout</b> <i>integer</i> ] [ <b>key</b> <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)# <b>tacacs-server key</b> <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)# <b>tacacs-server host</b> <i>name</i> [ <b>single-connection</b> ] [ <b>port</b> <i>integer</i> ] [ <b>timeout</b> <i>integer</i> ] [ <b>key</b> <i>string</i> ]	Specifies and defines the IP address of the server host before configuring the AAA server-group. Refer to the “ <a href="#">Identifying the TACACS+ Server Host</a> ” section of this chapter for more information on the <b>tacacs-server host</b> command.
Step 2	Router(config-if)# <b>aaa group server</b> { <b>radius</b>   <b>tacacs+</b> } <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)# <b>server</b> <i>ip-address</i> [ <b>auth-port</b> <i>port-number</i> ] [ <b>acct-port</b> <i>port-number</i> ]	Associates a particular TACACS+ server with the defined server group. Use the <b>auth-port</b> <i>port-number</i> option to configure a specific UDP port solely for authentication. Use the <b>acct-port</b> <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.  <b>Note</b> Each server in the group must be defined previously using the <b>tacacs-server host</b> 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:

	<b>Command</b>	<b>Purpose</b>
<b>Step 1</b>	Router(config)# <b>aaa dnis map enable</b>	Enables DNIS mapping.
<b>Step 2</b>	Router(config)# <b>aaa dnis map</b> <i>dnis-number</i> <b>authentication ppp group</b> <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.
<b>Step 3</b>	Router(config)# <b>aaa dnis map</b> <i>dnis-number</i> <b>accounting</b> <b>network</b> [ <b>none</b>   <b>start-stop</b>   <b>stop-only</b> ] <b>group</b> <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 sg3. 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"
  }
}
```

---

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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.

© 2007–2009 Cisco Systems, Inc. All rights reserved.





# Per VRF for TACACS+ Servers

---

**First Published: March 1, 2004**

**Last Updated: May 4, 2009**

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

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 Per VRF for TACACS+ Servers”](#) section on page 8.

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 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**

## 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***

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	<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 cisco	Configures a VRF table and enters VRF configuration mode.
Step 4	<b>rd</b> <i>route-distinguisher</i>  <b>Example:</b> Router (config-vrf)# rd 100:1	Creates routing and forwarding tables for a VRF instance.
Step 5	<b>exit</b>  <b>Example:</b> Router (config-vrf)# exit	Exits VRF configuration mode.
Step 6	<b>interface</b> <i>interface-name</i>  <b>Example:</b> Router (config)# interface Loopback0	Configures an interface and enters interface configuration mode.
Step 7	<b>ip vrf forwarding</b> <i>vrf-name</i>  <b>Example:</b> Router (config-if)# ip vrf forwarding cisco	Configures a VRF for the interface.
Step 8	<b>ip address</b> <i>ip-address mask</i> [ <b>secondary</b> ]  <b>Example:</b> Router (config-if)# ip address 10.0.0.2 255.0.0.0	Sets a primary or secondary IP address for an interface.

	Command or Action	Purpose
Step 9	<b>exit</b>  <b>Example:</b> Router (config-if)# exit	Exits interface configuration mode.
Step 10	<b>aaa group server tacacs+ group-name</b>  <b>Example:</b> 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	<b>server-private {ip-address   name} [nat] [single-connection] [port port-number] [timeout seconds] [key [0   7] string]</b>  <b>Example:</b> 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	<b>ip vrf forwarding vrf-name</b>  <b>Example:</b> Router (config-sg-tacacs)# ip vrf forwarding cisco	Configures the VRF reference of a AAA TACACS+ server group.
Step 13	<b>ip tacacs source-interface subinterface-name</b>  <b>Example:</b> Router (config-sg-tacacs)# ip tacacs source-interface Loopback0	Uses the IP address of a specified interface for all outgoing TACACS+ packets.
Step 14	<b>exit</b>  <b>Example:</b> 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**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <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	<code>debug tacacs authentication</code>  <b>Example:</b> Router# debug tacacs authentication	Displays information about AAA/TACACS+ authentication.
Step 3	<code>debug tacacs authorization</code>  <b>Example:</b> Router# debug tacacs authorization	Displays information about AAA/TACACS+ authorization.
Step 4	<code>debug tacacs accounting</code>  <b>Example:</b> Router# debug tacacs accounting	Displays information about accountable events as they occur.
Step 5	<code>debug tacacs packets</code>  <b>Example:</b> 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
```

## Additional References

The following sections provide references related to Per VRF for TACACS+ Servers..

### Related Documents

Related Topic	Document Title
Configuring TACACS+	“ <a href="#">Configuring TACACS+</a> ” chapter of the “Security Server Protocols” section of the <i>Cisco IOS Security Configuration Guide</i>
Per VRF AAA	<a href="#">Per VRF AAA</a>
Cisco IOS commands	<a href="#">Cisco IOS Master Command List, All Releases</a>
Security commands	<a href="#">Cisco IOS Security Command Reference</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: <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>	<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 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).

- **ip tacacs source-interface**
- **ip vrf forwarding (server-group)**
- **server-private (TACACS+)**

# 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, Catalyst OS, and Cisco IOS XE 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	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.
	12.2(33)SRA1	
	12.2(33)SXI	
	12.2(33)SXH4	
Cisco IOS XE Release 2.1		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.
		This feature was integrated into Cisco IOS Release 12.2(33)SXH4.
		This feature was integrated into Cisco IOS XE Release 2.1.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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

© 2004-2009 Cisco Systems, Inc. All rights reserved.



## **RADIUS and TACACS+ Attributes**





## **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.

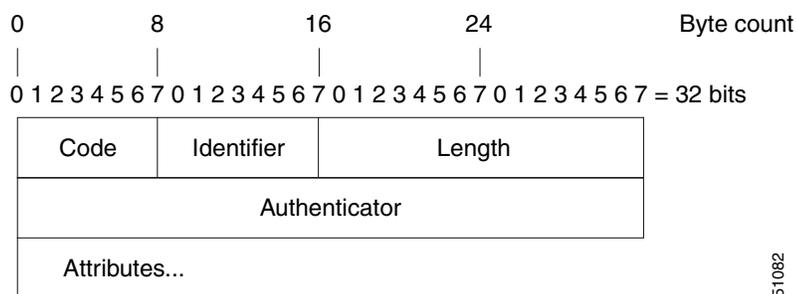
[Figure 125](#) shows the fields within a RADIUS packet.



### 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:
  - abinary—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 <sup>1</sup>	no	no	no	no	no	no	yes	yes
65	Tunnel-Medium-Type <sup>1</sup>	no	no	no	no	no	no	yes	yes
66	Tunnel-Client-Endpoint	no	no	no	no	no	no	yes	yes
67	Tunnel-Server-Endpoint <sup>1</sup>	no	no	no	no	no	no	yes	yes
68	Acct-Tunnel-Connection-ID	no	no	no	no	no	no	yes	yes
69	Tunnel-Password <sup>1</sup>	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 <sup>1</sup>	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 <sup>2</sup>	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 <b>radius-server extended-portnames</b> 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 <b>00ttt</b>, where <b>ttt</b> is the line number or async interface unit number.</p> <p>For ordinary synchronous network interface, the value is <b>10xxx</b>.</p> <p>For channels on a primary rate ISDN interface, the value is <b>2ppcc</b>.</p> <p>For channels on a basic rate ISDN interface, the value is <b>3bb0c</b>.</p> <p>For other types of interfaces, the value is <b>6nnss</b>.</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"> <li>In a request: <ul style="list-style-type: none"> <li>Framed for known PPP or SLIP connection.</li> <li>Administrative-user for <b>enable</b> command.</li> </ul> </li> <li>In response: <ul style="list-style-type: none"> <li>Login—Make a connection.</li> <li>Framed—Start SLIP or PPP.</li> <li>Administrative User—Start an EXEC or <b>enable ok</b>.</li> <li>Exec User—Start an EXEC session.</li> </ul> </li> </ul> <p>Service type is indicated by a particular numeric value as follows:</p> <ul style="list-style-type: none"> <li>1: Login</li> <li>2: Framed</li> <li>3: Callback-Login</li> <li>4: Callback-Framed</li> <li>5: Outbound</li> <li>6: Administrative</li> <li>7: NAS-Prompt</li> <li>8: Authenticate Only</li> <li>9: Callback-NAS-Prompt</li> </ul>
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"> <li>1: PPP</li> <li>2: SLIP</li> <li>3: ARA</li> <li>4: Gandalf-proprietary single-link/multilink protocol</li> <li>5: Xylogics-proprietary IPX/SLIP</li> </ul>
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 <b>radius-server attribute 8 include-in-access-req</b> 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"> <li>• 0: None</li> <li>• 1: Send routing packets</li> <li>• 2: Listen for routing packets</li> <li>• 3: Send routing packets and listen for routing packets</li> </ul>
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"> <li>• 0: None</li> <li>• 1: VJ-TCP/IP header compression</li> <li>• 2: IPX header compression</li> </ul>
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"> <li>• 0: Telnet</li> <li>• 1: Rlogin</li> <li>• 2: TCP-Clear</li> <li>• 3: PortMaster</li> <li>• 4: LAT</li> </ul>
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><a href="#">Table 71</a> 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	Termination is indicated by a numeric value as follows: <ul style="list-style-type: none"> <li>• 0: Default</li> <li>• 1: RADIUS request</li> </ul>
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 <b>radius-server attribute 32 include-in-access-req</b> 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 <b>radius-server attribute 44 include-in-access-req</b> 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"> <li>1. User request</li> <li>2. Lost carrier</li> <li>3. Lost service</li> <li>4. Idle timeout</li> <li>5. Session timeout</li> <li>6. Admin reset</li> <li>7. Admin reboot</li> <li>8. Port error</li> <li>9. NAS error</li> <li>10. NAS request</li> <li>11. NAS reboot</li> <li>12. Port unneeded</li> <li>13. Port pre-empted</li> <li>14. Port suspended</li> <li>15. Service unavailable</li> <li>16. Callback</li> <li>17. User error</li> <li>18. Host request</li> </ol> <p><b>Note</b> 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 <b>radius-server attribute 55 include-in-acct-req</b> command.</p> <p><b>Note</b> 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 <b>clock calendar-valid</b> 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"> <li>• 0: Asynchronous</li> <li>• 1: Synchronous</li> <li>• 2: ISDN-Synchronous</li> <li>• 3: ISDN-Asynchronous (V.120)</li> <li>• 4: ISDN-Asynchronous (V.110)</li> <li>• 5: Virtual</li> </ul>
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 <sup>1</sup>	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 <sup>1</sup>	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> <p style="padding-left: 40px;">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> <p>for the actual tunnel client endpoint IP address. This enhancement adds scalability across multiple network access servers.</p>
67	Tunnel-Server-Endpoint <sup>1</sup>	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 <sup>1</sup>	<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 <b>radius-server attribute 69 clear</b> 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 <sup>1</sup>	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	Determines how RADIUS treats passwords received from login-users when their file entry specifies a hand-held security card server.  The value for this attribute is indicated by a numeric value as follows: <ul style="list-style-type: none"> <li>• 0: No, meaning that the password is ignored.</li> <li>• 1: Yes, meaning that the password is used for authentication.</li> </ul>

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*.

---

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 Vendor-Proprietary Attributes

---

**First Published: May 15, 2001**

**Last Updated: September 25, 2008**

The IETF draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the network access server and the RADIUS server. However, some vendors have extended the RADIUS attribute set for specific applications. This document provides Cisco IOS support information for these vendor-proprietary RADIUS attributes.

## 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 RADIUS Vendor-Proprietary Attributes” section on page 13](#).

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

- [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.



---

**Americas Headquarters:**

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

**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	12.3	12.4
17	Change-Password	no	no	yes	yes	yes	yes	yes	yes	no	no
21	Password-Expiration	no	no	yes	yes	yes	yes	yes	yes	no	no
68	Tunnel-ID	no	no	no	no	no	no	no	yes	yes	yes
108	My-Endpoint-Disc-Alias	no	no	no	no	no	no	no	no	no	no
109	My-Name-Alias	no	no	no	no	no	no	no	no	no	no
110	Remote-FW	no	no	no	no	no	no	no	no	no	no
111	Multicast-GLeave-Delay	no	no	no	no	no	no	no	no	no	no
112	CBCP-Enable	no	no	no	no	no	no	no	no	no	no
113	CBCP-Mode	no	no	no	no	no	no	no	no	no	no
114	CBCP-Delay	no	no	no	no	no	no	no	no	no	no
115	CBCP-Trunk-Group	no	no	no	no	no	no	no	no	no	no
116	Appletalk-Route	no	no	no	no	no	no	no	no	no	no
117	Appletalk-Peer-Mode	no	no	no	no	no	no	no	no	no	no
118	Route-Appletalk	no	no	no	no	no	no	no	no	no	no
119	FCP-Parameter	no	no	no	no	no	no	no	no	no	no
120	Modem-PortNo	no	no	no	no	no	no	no	no	no	no
121	Modem-SlotNo	no	no	no	no	no	no	no	no	no	no
122	Modem-ShelfNo	no	no	no	no	no	no	no	no	no	no
123	Call-Attempt-Limit	no	no	no	no	no	no	no	no	no	no
124	Call-Block-Duration	no	no	no	no	no	no	no	no	no	no
125	Maximum-Call-Duration	no	no	no	no	no	no	no	no	no	no
126	Router-Preference	no	no	no	no	no	no	no	no	no	no
127	Tunneling-Protocol	no	no	no	no	no	no	no	no	no	no
128	Shared-Profile-Enable	no	no	no	no	no	no	no	no	yes	yes
129	Primary-Home-Agent	no	no	no	no	no	no	no	no	no	no
130	Secondary-Home-Agent	no	no	no	no	no	no	no	no	no	no
131	Dialout-Allowed	no	no	no	no	no	no	no	no	no	no
133	BACP-Enable	no	no	no	no	no	no	no	no	no	no
134	DHCP-Maximum-Leases	no	no	no	no	no	no	no	no	no	no
135	Primary-DNS-Server	no	no	no	no	yes	yes	yes	yes	yes	yes
136	Secondary-DNS-Server	no	no	no	no	yes	yes	yes	yes	yes	yes
137	Ascend-Client-Assign-DNS	no	no	no	no	no	no	no	no	yes	yes

**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	12.3	12.4
138	User-Acct-Type	no	no	no	no	no	no	no	no	no	no
139	User-Acct-Host	no	no	no	no	no	no	no	no	no	no
140	User-Acct-Port	no	no	no	no	no	no	no	no	no	no
141	User-Acct-Key	no	no	no	no	no	no	no	no	no	no
142	User-Acct-Base	no	no	no	no	no	no	no	no	no	no
143	User-Acct-Time	no	no	no	no	no	no	no	no	no	no
144	Assign-IP-Client	no	no	no	no	no	no	no	no	no	no
145	Assign-IP-Server	no	no	no	no	no	no	no	no	no	no
146	Assign-IP-Global-Pool	no	no	no	no	no	no	no	no	no	no
147	DHCP-Reply	no	no	no	no	no	no	no	no	no	no
148	DHCP-Pool-Number	no	no	no	no	no	no	no	no	no	no
149	Expect-Callback	no	no	no	no	no	no	no	no	no	no
150	Event-Type	no	no	no	no	no	no	no	no	no	no
151	Ascend-Session-Svr-Key	no	no	no	yes	no	no	yes	yes	yes	yes
152	Ascend-Multicast-Rate-Limit	no	no	no	yes	no	no	yes	yes	yes	yes
153	IF-Netmask	no	no	no	no	no	no	no	no	no	no
154	h323-Remote-Address	no	no	no	no	no	no	no	no	yes	yes
155	Ascend-Multicast-Client	no	no	no	yes	no	no	yes	yes	yes	yes
156	FR-Circuit-Name	no	no	no	no	no	no	no	no	no	no
157	FR-LinkUp	no	no	no	no	no	no	no	no	no	no
158	FR-Nailed-Grp	no	no	no	no	no	no	no	no	no	no
159	FR-Type	no	no	no	no	no	no	no	no	no	no
160	FR-Link-Mgt	no	no	no	no	no	no	no	no	no	no
161	FR-N391	no	no	no	no	no	no	no	no	no	no
162	FR-DCE-N392	no	no	no	no	no	no	no	no	no	no
163	FR-DTE-N392	no	no	no	no	no	no	no	no	no	no
164	FR-DCE-N393	no	no	no	no	no	no	no	no	no	no
165	FR-DTE-N393	no	no	no	no	no	no	no	no	no	no
166	FR-T391	no	no	no	no	no	no	no	no	no	no
167	FR-T392	no	no	no	no	no	no	no	no	no	no
168	Bridge-Address	no	no	no	no	no	no	no	no	no	no
169	TS-Idle-Limit	no	no	no	no	no	no	no	no	no	no
170	TS-Idle-Mode	no	no	no	no	no	no	no	no	no	no
171	DBA-Monitor	no	no	no	no	no	no	no	no	no	no
172	Base-Channel-Count	no	no	no	no	no	no	no	no	no	no
173	Minimum-Channels	no	no	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	12.3	12.4
174	IPX-Route	no	no	no	no	no	no	no	no	no	no
175	FT1-Caller	no	no	no	no	no	no	no	no	no	no
176	Ipssec-Backup-Gateway	no	no	no	no	no	no	no	no	yes	yes
177	rm-Call-Type	no	no	no	no	no	no	no	no	yes	yes
178	Group	no	no	no	no	no	no	no	no	no	no
179	FR-DLCI	no	no	no	no	no	no	no	no	no	no
180	FR-Profile-Name	no	no	no	no	no	no	no	no	no	no
181	Ara-PW	no	no	no	no	no	no	no	no	no	no
182	IPX-Node-Addr	no	no	no	no	no	no	no	no	no	no
183	Home-Agent-IP-Addr	no	no	no	no	no	no	no	no	no	no
184	Home-Agent-Password	no	no	no	no	no	no	no	no	no	no
185	Home-Network-Name	no	no	no	no	no	no	no	no	no	no
186	Home-Agent-UDP-Port	no	no	no	no	no	no	no	no	no	no
187	Multilink-ID	no	no	no	yes	yes	yes	yes	yes	yes	yes
188	Ascend-Num-In-Multilink	no	no	no	yes	yes	yes	yes	yes	yes	yes
189	First-Dest	no	no	no	no	no	no	no	no	no	no
190	Pre-Input-Octets	no	no	no	yes	yes	yes	yes	yes	no	no
191	Pre-Output-Octets	no	no	no	yes	yes	yes	yes	yes	no	no
192	Pre-Input-Packets	no	no	no	yes	yes	yes	yes	yes	no	no
193	Pre-Output-Packets	no	no	no	yes	yes	yes	yes	yes	no	no
194	Maximum-Time	no	no	yes	yes	yes	yes	yes	yes	no	no
195	Disconnect-Cause	no	no	yes	yes	yes	yes	yes	yes	yes	yes
196	Connect-Progress	no	no	no	no	no	no	yes	yes	yes	yes
197	Data-Rate	no	no	no	no	yes	yes	yes	yes	yes	yes
198	PreSession-Time	no	no	no	yes	yes	yes	yes	yes	yes	yes
199	Token-Idle	no	no	no	no	no	no	no	no	yes	yes
201	Require-Auth	no	no	no	no	no	no	no	no	yes	yes
202	Number-Sessions	no	no	no	no	no	no	no	no	no	no
203	Authen-Alias	no	no	no	no	no	no	no	no	no	no
204	Token-Expiry	no	no	no	no	no	no	no	no	no	no
205	Menu-Selector	no	no	no	no	no	no	no	no	no	no
206	Menu-Item	no	no	no	no	no	no	no	no	no	no
207	PW-Warntime	no	no	no	no	no	no	no	no	no	no
208	PW-Lifetime	no	no	yes	yes	yes	yes	yes	yes	yes	yes
209	IP-Direct	no	no	no	no	yes	yes	yes	yes	yes	yes
210	PPP-VJ-Slot-Compression	no	no	yes	yes	yes	yes	yes	yes	yes	yes

**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	12.3	12.4
211	PPP-VJ-1172	no	no	no	no	no	no	no	no	no	no
212	PPP-Async-Map	no	no	no	no	no	no	no	no	no	no
213	Third-Prompt	no	no	no	no	no	no	no	no	no	no
214	Send-Secret	no	no	no	no	no	no	yes	yes	yes	yes
215	Receive-Secret	no	no	no	no	no	no	no	no	no	no
216	IPX-Peer-Mode	no	no	no	no	no	no	no	no	no	no
217	IP-Pool	no	no	yes	yes	yes	yes	yes	yes	yes	yes
218	Static-Addr-Pool	no	no	yes	yes	yes	yes	yes	yes	yes	yes
219	FR-Direct	no	no	no	no	no	no	no	no	no	no
220	FR-Direct-Profile	no	no	no	no	no	no	no	no	no	no
221	FR-Direct-DLCI	no	no	no	no	no	no	no	no	no	no
222	Handle-IPX	no	no	no	no	no	no	no	no	no	no
223	Netware-Timeout	no	no	no	no	no	no	no	no	no	no
224	IPX-Alias	no	no	no	no	no	no	no	no	no	no
225	Metric	no	no	no	no	no	no	no	no	no	no
226	PRI-Number-Type	no	no	no	no	no	no	no	no	no	no
227	Dial-Number	no	no	no	no	no	no	yes	yes	yes	yes
228	Route-IP	no	no	yes	yes	yes	yes	yes	yes	yes	yes
229	Route-IPX	no	no	no	no	no	no	no	no	no	no
230	Bridge	no	no	no	no	no	no	no	no	no	no
231	Send-Auth	no	no	no	no	no	no	yes	yes	yes	yes
232	Send-Passwd	no	no	no	no	no	no	no	no	no	no
233	Link-Compression	no	no	yes	yes	yes	yes	yes	yes	yes	yes
234	Target-Util	no	no	no	yes	no	yes	yes	yes	yes	yes
235	Maximum-Channels	no	no	yes	yes	yes	yes	yes	yes	yes	yes
236	Inc-Channel-Count	no	no	no	no	no	no	no	no	no	no
237	Dec-Channel-Count	no	no	no	no	no	no	no	no	no	no
238	Seconds-of-History	no	no	no	no	no	no	no	no	no	no
239	History-Weigh-Type	no	no	no	no	no	no	no	no	no	no
240	Add-Seconds	no	no	no	no	no	no	no	no	no	no
241	Remove-Seconds	no	no	no	no	no	no	no	no	no	no
242	Data-Filter	no	no	yes	yes	yes	yes	yes	yes	yes	yes
243	Call-Filter	no	no	no	no	no	no	no	no	yes	yes
244	Idle-Limit	no	no	yes	yes	yes	yes	yes	yes	yes	yes
245	Preempt-Limit	no	no	no	no	no	no	no	no	no	no
246	Callback	no	no	no	no	no	no	no	no	yes	yes

**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	12.3	12.4
247	Data-Service	no	no	no	no	no	no	yes	yes	yes	yes
248	Force-56	no	no	no	no	no	no	yes	yes	yes	yes
249	Billing Number	no	no	no	no	no	no	no	no	no	no
250	Call-By-Call	no	no	no	no	no	no	no	no	no	no
251	Transit-Number	no	no	no	no	no	no	no	no	no	no
252	Host-Info	no	no	no	no	no	no	no	no	no	no
253	PPP-Address	no	no	no	no	no	no	no	no	no	no
254	MPP-Idle-Percent	no	no	no	no	no	no	no	no	no	no
255	Xmit-Rate	no	no	no	yes	yes	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.

**Table 74 Vendor-Proprietary RADIUS Attributes (continued)**

<b>Number</b>	<b>Vendor-Proprietary Attribute</b>	<b>Description</b>
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.
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.

**Table 74** Vendor-Proprietary RADIUS Attributes (continued)

<b>Number</b>	<b>Vendor-Proprietary Attribute</b>	<b>Description</b>
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.
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.

Table 74 Vendor-Proprietary RADIUS Attributes (continued)

Number	Vendor-Proprietary Attribute	Description
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.
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 <a href="#">Disconnect-Cause Attribute Values</a> 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.

Table 74 Vendor-Proprietary RADIUS Attributes (continued)

Number	Vendor-Proprietary Attribute	Description
202	Number-Sessions	Specifies the number of active sessions (per class) reported to the RADIUS accounting server.
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><b>Note</b> 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.

**Table 74 Vendor-Proprietary RADIUS Attributes (continued)**

<b>Number</b>	<b>Vendor-Proprietary Attribute</b>	<b>Description</b>
219	FR-Direct	Defines whether the connection profile operates in Frame Relay redirect mode.
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	Defines whether to turn on or turn off "stac" compression over a PPP link.  Link compression is defined as a numeric value as follows: <ul style="list-style-type: none"> <li>• 0: None</li> <li>• 1: Stac</li> <li>• 2: Stac-Draft-9</li> <li>• 3: MS-Stac</li> </ul>
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](#).”

# Feature Information for RADIUS Vendor-Proprietary Attributes

Table 75 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 75 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 75** Feature Information for RADIUS Vendor-Proprietary Attributes

Feature Name	Releases	Feature Information
RADIUS Vendor-Proprietary Attributes	12.2(1)XE	The IETF draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the network access server and the RADIUS server. However, some vendors have extended the RADIUS attribute set for specific applications. This document provides Cisco IOS support information for these vendor-proprietary RADIUS attributes.  In 12.2(1) XE, this feature was introduced.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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.





# RADIUS Vendor-Specific Attributes (VSA) and RADIUS Disconnect-Cause Attribute Values

---

**First Published: September 23, 2005**

**Last Updated: September 26, 2008**

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:

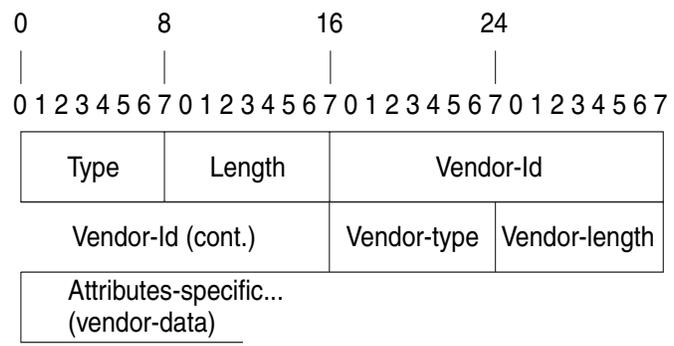
```
cisco-avpair= "shell:priv-lvl=15"
```

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**



51325



**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
<b>MS-CHAP Attributes</b>				
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)
<b>VPDN Attributes</b>				
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	tunnel-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.
<b>Store and Forward Fax Attributes</b>				
26	9	3	Fax-Account-Id-Origin	Indicates the account ID origin as defined by system administrator for the <b>mmoip aaa receive-id</b> or the <b>mmoip aaa send-id</b> 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.
<b>H323 Attributes</b>				
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 <b>telephony</b> and <b>VoIP</b> .
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 <b>ppp pap sent-name password</b> 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><b>Note</b> 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>
<b>Miscellaneous Attributes</b>				
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 <b>radius-server vsa send</b> global configuration command.</p> <p><b>Note</b> 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 <b>ip mobile secure host &lt;addr&gt;</b> 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)**

<b>Cause Code</b>	<b>Value</b>	<b>Description</b>
10	No-Carrier	No carrier detected. <b>Note</b> 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. <b>Note</b> 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 connection has ended.
31	Exit-Rlogin	User exits Rlogin.
32	Invalid-Rlogin-Option	Invalid Rlogin option selected.
33	Insufficient-Resources	Insufficient resources.
40	Timeout-PPP-LCP	PPP LCP negotiation timed out. <b>Note</b> 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. <b>Note</b> 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 in 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. <b>Note</b> VPN-Tunnel-Shut will be sent if there are active sessions in the tunnel.

**Table 3**      **Disconnect-Cause Attribute Values (continued)**

<b>Cause Code</b>	<b>Value</b>	<b>Description</b>
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 <b>clear vpdn tunnel</b> 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. <b>Note</b> 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	<a href="#">Cisco IOS Security Configuration Guide, Release 12.4</a>
Security Server Protocols	<a href="#">Part 2: Security Server Protocols in the Cisco IOS Security Configuration Guide, Release 12.4</a>
RADIUS Configuration	<a href="#">Configuring RADIUS</a>

## Standards

Standard	Title
Internet Engineering Task Force (IETF) Internet Draft: Network Access Servers Requirements	<a href="#">Network Access Servers Requirements: Extended RADIUS Practices</a>

## 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
RFC 2865	<a href="#">Remote Authentication Dial In User Service (RADIUS)</a>

## 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 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, 2008 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	<a href="#">“Configuring and Managing Cisco Access Servers and Dial Shelves”</a> chapter of the <i>Cisco IOS Dial Technologies Configuration Guide</i>
	<a href="#">Cisco IOS Dial Technologies Command Reference</a>
RADIUS and security related information	<a href="#">Cisco IOS Security Command Reference</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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
RFC 2869	<a href="#">RADIUS Extensions</a>

## 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

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](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"> <li>• Cisco AS5300 series</li> <li>• Cisco AS5400 series</li> <li>• Cisco AS5800 series</li> <li>• Cisco AS5850 series</li> </ul>

---

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: July 7, 2009**

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

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 Encrypted Vendor-Specific Attributes” section on page 7](#).

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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. An account on Cisco.com is not required.



---

**Americas Headquarters:**

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

# 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](#)
- [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

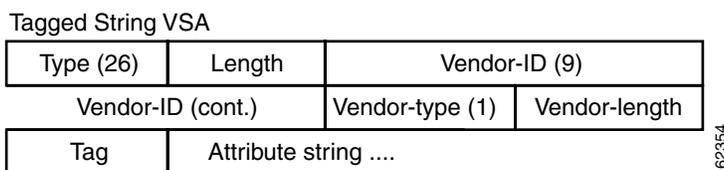
The following sections describe packet encryption formats for the different VSAs:

- [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**



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# <code>debug radius</code>	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 = "password1"
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	<a href="#">Cisco IOS Security Configuration Guide: Securing User Services, Release 12.4T</a>

## 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## 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><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

# 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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. 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 Cisco IOS XE Release 2.3	<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> <p>In Cisco IOS XE Release 2.3, this feature was implemented on the Cisco ASR 1000 series routers.</p>

---

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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

© 2007–2009 Cisco Systems, Inc. All rights reserved.



# Local AAA Server

---

**First Published: March 28, 2005**

**Last Updated: May 4, 2009**

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

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 Local AAA Server” section on page 12](#).

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 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 8](#)
- [Additional References, page 10](#)
- [Command Reference, page 11](#)
- [Feature Information for Local AAA Server, page 12](#)



---

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

# 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 5](#) (required)
- [Monitoring and Troubleshooting a Local AAA Server, page 6](#) (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	<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 attribute list</b> <i>list-name</i>  <b>Example:</b> Router (config)# aaa attribute list TEST	Defines a AAA attribute list.
Step 4	<b>attribute type</b> { <i>name</i> } { <i>value</i> } [ <b>service</b> <i>service</i> ] [ <b>protocol</b> <i>protocol</i> ]  <b>Example:</b> Router (config-attr-list)# attribute type addr-pool poolname service ppp protocol ip	Defines an IP address pool to use.
Step 5	<b>attribute type</b> { <i>name</i> } { <i>value</i> } [ <b>service</b> <i>service</i> ] [ <b>protocol</b> <i>protocol</i> ]  <b>Example:</b> Router (config-attr-list)# attribute type ip-unnumbered loopbacknumber service ppp protocol ip	Defines the loopback interface to use.
Step 6	<b>attribute type</b> { <i>name</i> } { <i>value</i> } [ <b>service</b> <i>service</i> ] [ <b>protocol</b> <i>protocol</i> ]  <b>Example:</b> Router (config-attr-list)# attribute type vrf-id vrfname service ppp protocol ip	Defines the virtual route forwarding (VRF) to use.
Step 7	<b>attribute type</b> { <i>name</i> } { <i>value</i> }  <b>Example:</b> Router (config-attr-list)# attribute type ppp-authen-list aalistname	Defines the AAA authentication list to use.

	Command or Action	Purpose
Step 8	<b>attribute type</b> {name} {value}  <b>Example:</b> Router (config-attr-list)# attribute type ppp-author-list aaalistname	Defines the AAA authorization list to use.
Step 9	<b>attribute type</b> {name} {value}  <b>Example:</b> Router (config-attr-list)# 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 9.](#)”

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **subscriber authorization enable**
4. `policy-map type service example.com`
5. **policy-map type service** *domain-name*
6. **service local**
7. **exit**
8. **aaa attribute list** *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>subscriber authorization enable</b>  <b>Example:</b> Router (config)# subscriber authorization enable	Enables subscriber authorization.
Step 4	<b>policy-map type service domain-name</b>  <b>Example:</b> Router (config)# policy-map type example.com	Specifies the username domain that has to be matched and enters subscriber profile configuration mode.
Step 5	<b>service local</b>  <b>Example:</b> Router (subscriber-profile)# service local	Specifies that local subscriber authorization should be performed.
Step 6	<b>exit</b>  <b>Example:</b> Router (subscriber-profile)# exit	Exits subscriber profile configuration mode.
Step 7	<b>aaa attribute list list-name</b>  <b>Example:</b> 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

- enable
- debug aaa authentication
- debug aaa authorization
- 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	<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 aaa authentication</b>  <b>Example:</b> Router# debug aaa authentication	Displays the methods of authentication being used and the results of these methods.
Step 3	<b>debug aaa authorization</b>  <b>Example:</b> Router# debug aaa authorization	Displays the methods of authorization being used and the results of these methods.
Step 4	<b>debug aaa per-user</b>  <b>Example:</b> Router# debug aaa per-user	Displays information about PPP session per-user activities.
Step 5	<b>debug ppp authentication</b>  <b>Example:</b> Router# debug ppp authentication	Indicates whether a client is passing authentication.
Step 6	<b>debug ppp error</b>  <b>Example:</b> Router (config)# debug ppp error	Displays protocol errors and error statistics that are associated with PPP connection negotiation and operation.
Step 7	<b>debug ppp forward</b>  <b>Example:</b> Router# debug ppp forward	Displays who is taking control of a session.
Step 8	<b>debug ppp negotiation</b>  <b>Example:</b> Router# debug ppp negotiation	Displays PPP packets sent during PPP startup, where PPP options are negotiated.

	Command or Action	Purpose
Step 9	<code>debug radius</code>  <b>Example:</b> Router# debug radius	Displays information about the RADIUS server.
Step 10	<code>debug sss error</code>  <b>Example:</b> 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 8](#)
- [Mapping from the RADIUS Version of a Particular Attribute to the Cisco IOS AAA Version: Example, page 9](#)

### 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
!
policy-map type service example.com
  service local
  aaa attribute list TEST
!
bba-group pppoe grp1
  virtual-template 1
  service profile example.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 “ <a href="#">Configuring Local AAA Server, User Database—Domain to VRF</a> ” in <i>Cisco 10000 Series Broadband Aggregation and Leased-Line Configuration Guide</i>
Cisco IOS security commands	<a href="#">Cisco IOS Security Command Reference</a>

### 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### 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><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 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 attribute list**
- **attribute type**

# Feature Information for Local AAA Server

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, Catalyst OS, and Cisco IOS XE 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 the Cisco ASR 1000 series routers.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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

© 2005–2009 Cisco Systems, Inc. All rights reserved.



# Per-User QoS via AAA Policy Name

---

**First Published: March 31, 2000**

**Last Updated: May 4, 2009**

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

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 Per-User QoS via AAA Policy Name” section on page 6](#).

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 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 Example for Per-User QoS via AAA Policy Name, page 3](#)
- [Additional References, page 4](#)
- [Command Reference, page 5](#)
- [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**

# 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	<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 aaa authorization</b>  <b>Example:</b> Router# debug aaa authorization	Displays information about AAA/TACACS+ authorization.
Step 3	<b>debug aaa per-user</b>  <b>Example:</b> Router# debug aaa per-user	Displays information about per-user QoS parameters.

## Configuration Example for Per-User QoS via AAA Policy Name

The following example shows per-user QoS being configured using the AAA policy name “policy\_class\_1\_2”:

```

!NAS configuration
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

!RADIUS Profile Configuration
peruser_qos_1 Password = "password1"
  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 = "password1"
  Service-Type = Framed,
  Framed-Protocol = PPP,
  Cisco:Cisco-avpair = "ip:sub-policy-Out=ssspolicy"

```

# Additional References

The following sections provide references related to the Per-User QoS via AAA Policy Name.

## Related Documents

Related Topic	Document Title
<ul style="list-style-type: none"> <li>AAA per-user and QoS configurations and information about the <b>policy-map</b> command</li> </ul>	<ul style="list-style-type: none"> <li><a href="#">Configuring Per-User Configuration</a></li> <li><a href="#">Cisco IOS Security Command Reference</a></li> </ul>

## 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 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><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

## Command Reference

No commands were introduced or modified by this feature. For information about security 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).

# 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, Catalyst OS, and Cisco IOS XE 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 Cisco IOS XE Release 2.1	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.  In Cisco IOS XE Release 2.1, this feature was implemented on the Cisco ASR 1000 series routers.

# 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.

---

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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

© 2000–2009 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	<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 group server radius group-name</b>  <b>Example:</b> 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	<b>server ip-address [auth-port port-number] [acct-port port-number]</b>  <b>Example:</b> 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	<b>attribute nas-port format format-type [string]</b>  <b>Example:</b> 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"><li>The service types can be set to use their own respective server groups.</li></ul>

## 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	<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 aaa sg-server selection</b>  <b>Example:</b> 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	<b>debug radius</b>  <b>Example:</b> 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	“ <i>Authentication, Authorization, and Accounting (AAA)</i> ” section of <i>Cisco IOS Security 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: <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
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 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](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	<code>enable</code>  <b>Example:</b> Router> <code>enable</code>	Enables privileged EXEC mode.  • Enter your password if prompted.
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# <code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>radius-server attribute 8 include-in-access-req</code>  <b>Example:</b> Router(config)# <code>radius-server attribute 8 include-in-access-req</code>	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>  <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>more system:running-config</code>  <b>Example:</b> Router# <code>more system:running-config</code>	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>  <b>Example:</b> Router# <code>debug radius</code>	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:  <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, 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	The following sections provide information about this feature: <ul style="list-style-type: none"> <li>• <a href="#">Information About RADIUS Attribute 8 (Framed-IP-Address) in Access Requests, page 2</a></li> <li>• <a href="#">How to Configure RADIUS Attribute 8 (Framed-IP-Address) in Access Requests, page 3</a></li> <li>• <a href="#">Configuration Examples for RADIUS Attribute 8 (Framed-IP-Address) in Access Requests, page 4</a></li> </ul> The following commands were introduced or modified: <b>radius-server attribute 8 include-in-access-req.</b>
Sticky IP	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

---

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

---

**First Published: October 15, 2001**  
**Last Updated: July 7, 2009**

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.

This 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.

## 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 RADIUS Attribute 82: Tunnel Assignment ID” section on page 7](#).

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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for RADIUS Attribute 82: Tunnel Assignment ID, page 2](#)
- [Restrictions for RADIUS Attribute 82: Tunnel Assignment ID, page 2](#)
- [Information About RADIUS Attribute 82: Tunnel Assignment ID, page 2](#)
- [How to Verify if RADIUS Attribute 82 is Being Used by the LAC, page 2](#)



---

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

- [Configuration Examples for RADIUS Attribute 82: Tunnel Assignment ID, page 3](#)
- [Additional References, page 5](#)
- [Feature Information for RADIUS Attribute 82: Tunnel Assignment ID, page 7](#)

## Prerequisites for RADIUS Attribute 82: Tunnel Assignment ID

You must be using a Cisco platform that supports VPDN to use this feature.

## Restrictions for RADIUS Attribute 82: Tunnel Assignment ID

This feature is designed only for VPDN dial-in applications. It does not support VPDN dial-out.

## Information About RADIUS Attribute 82: Tunnel Assignment ID

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.

## How to Verify if RADIUS Attribute 82 is Being Used by the LAC

There are no configuration steps for the RADIUS Attribute 82: Tunnel Assignment ID feature. This task verifies the RADIUS attribute 82 used by the LAC during tunnel authorization.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `debug radius`

## 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>configure terminal</code>  <b>Example:</b> Router# <code>configure terminal</code>	Enters global configuration mode.
Step 3	Router# <code>debug radius</code>  <b>Example:</b> Router# <code>debug radius</code>	Displays information associated with RADIUS. The output of this command shows whether attribute 82 is being sent in access requests.

## Configuration Examples for RADIUS Attribute 82: Tunnel Assignment ID

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 Serial12/0:23
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"
```

# Additional References

The following sections provide references related to the RADIUS Attribute 82: Tunnel Assignment ID feature.

## Related Documents

Related Topic	Document Title
Dial Technologies	<i>Cisco IOS Dial Technologies Configuration Guide</i> , Release 12.4T
Wide Area Networks	<i>Cisco IOS Wide-Area Networking Configuration Guide</i> , Release 12.4T

## 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: <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.	—

## 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 RADIUS Attribute 82: Tunnel Assignment ID

Table 78 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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. An account on Cisco.com is not required.



## Note

Table 78 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 78** Feature Information for RADIUS Attribute 82: Tunnel Assignment ID

Feature Name	Releases	Feature Information
RADIUS Attribute 82: Tunnel Assignment ID	12.2(4)T 12.2(4)T3 12.2(11)T 12.2(27)SB Cisco IOS XE Release 2.1	In 12.2(4)T, this feature was introduced.  In 12.2(4)T3, support for the Cisco 7500 series routers was added.  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.  This feature was integrated into Cisco IOS Release 12.2(27)SB.  In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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

© 2001–2009 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.	Ascend-Private-Route="dest_addr/netmask next_hop"  The destination network address of the router is "dest_addr/netmask", and the address of the next-hop router is "next_hop."

### 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	<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 ip policy</b>  <b>Example:</b> Router# show ip policy	Displays the route map that is used for policy routing.
Step 3	<b>show route-map</b> [ <i>map-name</i>   <b>dynamic</b> [ <i>dynamic-map-name</i>   <b>application</b> [ <i>application-name</i> ]]   <b>all</b> ]  <b>Example:</b> 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	<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 radius</b>  <b>Example:</b> Router# debug radius	Displays information associated with RADIUS.
Step 3	<b>debug aaa per-user</b>  <b>Example:</b> Router# debug aaa per-user	Displays the attributes that are applied to each user as the user authenticates.
Step 4	<b>debug ip policy</b>  <b>Example:</b> 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 gateway10.1.1.1
  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"> <li>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</li> <li><i>IP Access List Entry Sequence Numbering</i>, Release 12.3(2)T</li> </ul>
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	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
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.	<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

- **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](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.





## 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	<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 aaa accounting</b>  <b>Example:</b> Router# debug aaa accounting	Displays information on accountable events as they occur.
Step 3	<b>show radius statistics</b>  <b>Example:</b> 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	<i>Cisco IOS Security Command Reference</i>
Configuring Accounting	“ <a href="#">Configuring Accounting</a> ” chapter in the <i>Cisco IOS Security Configuration Guide</i>
Radius Attributes	“ <a href="#">RADIUS Attributes</a> ” 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### 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><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></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](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: <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

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](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	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.  This feature was introduced in Cisco IOS Release 12.2(15)T.  This feature was integrated into Cisco IOS Release 12.2(28)SB.

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"> <li>Layer 2 Forwarding (L2F)</li> <li>Layer 2 Tunneling Protocol (L2TP)</li> </ul>	Specifies the name used by the tunnel initiator (also known as the NAS <sup>1</sup> ) when authenticating tunnel setup with the tunnel terminator.
91	Tunnel-Server-Auth-ID	gw-name	<ul style="list-style-type: none"> <li>Layer 2 Forwarding (L2F)</li> <li>Layer 2 Tunneling Protocol (L2TP)</li> </ul>	Specifies the name used by the tunnel terminator (also known as the Home Gateway <sup>2</sup> ) 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](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**

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](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**

- 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# <code>debug radius</code>	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](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).

---

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

---

© 2007 Cisco Systems, Inc. All rights reserved.



## 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	<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 aaa accounting</b>  <b>Example:</b> Router# debug aaa accounting	Displays information about accountable events as they occur.
Step 3	<b>debug aaa authentication</b>  <b>Example:</b> Router# debug aaa authentication	Displays information about AAA authentication.
Step 4	<b>debug aaa authorization</b>  <b>Example:</b> Router# debug aaa authorization	Displays information about AAA and TACACS+ authorization.
Step 5	<b>debug isdn event</b>  <b>Example:</b> Router# debug isdn event	Displays ISDN events occurring on the user side (on the router) of the ISDN interface.
Step 6	<b>debug modem csm [slot/port   group group-number]</b>  <b>Example:</b> Router# debug modem csm 1/0 group 1	Displays call switching module (CSM) modem call information.
Step 7	<b>debug ppp {negotiation   authentication}</b>  <b>Example:</b> Router# debug ppp authentication	Displays information on traffic and exchanges in an internetwork that is implementing the PPP.
Step 8	<b>debug radius</b>  <b>Example:</b> 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, ds1=6, t3=0, slot=7, ds0=117465109
01:39:19: AAA/ACCT/DS0: channel=21, ds1=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 8F
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/IPCP: FSM authorization not needed
01:39:54: As1/05 AAA/AUTHOR/FSM: We can start IPCP
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

```



```

01:39:54: As1/05 AAA/AUTHOR/IPCP: no author-info for primary dns
01:39:54: As1/05 AAA/AUTHOR/IPCP: no author-info for primary wins
01:39:54: As1/05 AAA/AUTHOR/IPCP: no author-info for seconday dns
01:39:54: As1/05 AAA/AUTHOR/IPCP: no author-info for seconday wins
01:39:54: As1/05 IPCP: O CONFREJ [REQsent] id 5 len 28
01:39:54: As1/05 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000)
01:39:54: As1/05 IPCP: PrimaryWINS 0.0.0.0 (0x820600000000)
01:39:54: As1/05 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000)
01:39:54: As1/05 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000)
01:39:54: As1/05 IPCP: I CONFACK [REQsent] id 1 len 10
01:39:54: As1/05 IPCP: Address 70.1.1.2 (0x030646010102)
01:39:54: As1/05 IPCP: I CONFREQ [ACKrcvd] id 6 len 10
01:39:54: As1/05 IPCP: Address 0.0.0.0 (0x030600000000)
01:39:54: As1/05 IPCP: O CONFNAK [ACKrcvd] id 6 len 10
01:39:54: As1/05 IPCP: Address 70.2.2.6 (0x030646020206)
01:39:55: As1/05 IPCP: I CONFREQ [ACKrcvd] id 7 len 10
01:39:55: As1/05 IPCP: Address 70.2.2.6 (0x030646020206)
01:39:55: As1/05 IPCP: O CONFACK [ACKrcvd] id 7 len 10
01:39:55: As1/05 IPCP: Address 70.2.2.6 (0x030646020206)
01:39:55: As1/05 IPCP: State is Open
01:39:55: AAA/ACCT/EVENT/(00000007): IPCP_PASS
01:39:55: As1/05 IPCP: Install route to 10.2.2.6
01:39:55: As1/05 IPCP: 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

```

```

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) reccnt 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	<b>show modem</b> [ <i>slot/port</i>   <i>group number</i> ]  <b>Example:</b> 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	<b>show port modem log</b> [ <i>reverse slot/port</i> ] [ <i>slot</i>   <i>slot/port</i> ]  <b>Example:</b> Router# show port modem log	Displays the events generated by the modem sessions.
Step 3	<b>show users</b> [ <i>all</i> ]  <b>Example:</b> 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 msec
  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 msec
      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 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: <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
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. 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](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.



## **TACACS+ Attributes**





## 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:

- [TACACS+ Authentication and Authorization AV Pairs](#)
- [TACACS+ Accounting AV Pairs](#)

The first section lists and describes the supported TACACS+ authentication and authorization AV pairs, 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						
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						



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

© 2007 Cisco Systems, Inc. All rights reserved.

Table 80 Supported TACACS+ Authentication and Authorization AV Pairs (continued)

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
addr-pool=x	<p>Specifies the name of a local pool from which to get the address of the remote host. Used with service=ppp and protocol=ip.</p> <p>Note that <b>addr-pool</b> 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 <b>ip-local pool</b> command to declare local pools. For example:</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 addr-pool=boo or addr-pool=moo to indicate the address pool from which you want to get this remote node's address.</p>	yes						
autocmd=x	Specifies an autocommand to be executed at EXEC startup (for example, autocmd=telnet example.com). Used only with service=shell.	yes						
callback-dialstring	Sets the telephone number for a callback (for example: callback-dialstring=408-555-1212). 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 service=arap, service=slip, service=ppp, service=shell. 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: callback-line=4). Used with service=arap, service=slip, service=ppp, service=shell. 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: callback-rotary=34). Used with service=arap, service=slip, service=ppp, service=shell. 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 cmd-arg attributes can be specified, and they are order dependent.</p> <p><b>Note</b> This TACACS+ AV pair cannot be used with RADIUS attribute 26.</p>	yes						

**Table 80** Supported TACACS+ Authentication and Authorization AV Pairs (continued)

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
cmd=x	A shell (EXEC) command. This indicates the command name for a shell command that is to be run. This attribute must be specified if service equals "shell." A NULL value indicates that the shell itself is being referred to.  <b>Note</b> This TACACS+ AV pair cannot be used with RADIUS attribute 26.	yes						
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
inacl#<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=ppp and protocol=ipx. Per-user access lists do not currently work with ISDN interfaces.	no	no	no	yes	yes	yes	yes
inacl=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						

Table 80 Supported TACACS+ Authentication and Authorization AV Pairs (continued)

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
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. <b>Note</b> 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

**Table 80** Supported TACACS+ Authentication and Authorization AV Pairs (continued)

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
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: <ul style="list-style-type: none"> <li>• 0: None</li> <li>• 1: Stac</li> <li>• 2: Stac-Draft-9</li> <li>• 3: MS-Stac</li> </ul>	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

Table 80 Supported TACACS+ Authentication and Authorization AV Pairs (continued)

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
nas-password	Specifies the password for the network access server during the L2F tunnel authentication. Used with service=ppp and protocol=vpdn.	no	no	yes	yes	yes	yes	yes
nocallback-verify	Indicates that no callback verification is required. The only valid value for this parameter is 1 (for example, nocallback-verify=1). Used with service=arap, service=slip, service=ppp, service=shell. There is no authentication on callback. Not valid for ISDN.	no	yes	yes	yes	yes	yes	yes
noescape=x	Prevents user from using an escape character. Used with service=shell. Can be either true or false (for example, noescape=true).	yes	yes	yes	yes	yes	yes	yes
nohangup=x	Used with service=shell. Specifies the nohangup option, which means that after an EXEC shell is terminated, the user is presented with another login (username) prompt. Can be either true or false (for example, nohangup=false).	yes	yes	yes	yes	yes	yes	yes
old-prompts	Allows providers to make the prompts in TACACS+ appear identical to those of earlier systems (TACACS and Extended TACACS). This allows administrators to upgrade from TACACS or Extended TACACS to TACACS+ transparently to users.	yes	yes	yes	yes	yes	yes	yes
outacl#<n>	ASCII access list identifier for an interface output access list to be installed and applied to an interface for the duration of the current condition. 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
outacl=x	ASCII identifier for an interface output access list. Used with service=ppp and protocol=ip, and service service=ppp and protocol=ipx. Contains an IP output access list for SLIP or PPP/IP (for example, outacl=4). The access list itself must be preconfigured on the router. Per-user access lists do not currently work with ISDN interfaces.	yes (PPP /IP only )	yes	yes	yes	yes	yes	yes
pool-def#<n>	Defines IP address pools on the network access server. Used with service=ppp and protocol=ip.	no	no	no	yes	yes	yes	yes

Table 80 Supported TACACS+ Authentication and Authorization AV Pairs (continued)

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
pool-timeout=	Defines (in conjunction with pool-def) IP address pools on the network access server. During IPCP address negotiation, if an IP pool name is specified for a user (see the addr-pool attribute), a check is made to see if the named pool is defined on the network access server. If it is, the pool is consulted for an IP address. Used with service=ppp and protocol=ip.	no	no	yes	yes	yes	yes	yes
port-type	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: <ul style="list-style-type: none"> <li>• 0: Asynchronous</li> <li>• 1: Synchronous</li> <li>• 2: ISDN-Synchronous</li> <li>• 3: ISDN-Asynchronous (V.120)</li> <li>• 4: ISDN- Asynchronous (V.110)</li> <li>• 5: Virtual</li> </ul> Used with service=any and protocol=aaa.	no	no	no	no	no	yes	yes
ppp-vj-slot-compression	Instructs the Cisco router not to use slot 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						
protocol=x	A protocol that is a subset of a service. An example would be any PPP NCP. Currently known values are <b>lcp, ip, ipx, atalk, vines, lat, xremote, tn3270, telnet, rlogin, pad, vpdn, osicp, deccp, ccp, cdp, bridging, xns, nbf, bap, multilink, and unknown.</b>	yes						
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. Used with the service=shell and protocol=exec.	no	no	no	no	no	yes	yes

Table 80 Supported TACACS+ Authentication and Authorization AV Pairs (continued)

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
route	<p>Specifies a route to be applied to an interface. Used with service=slip, service=ppp, and protocol=ip.</p> <p>During network authorization, the route attribute can be used to specify a per-user static route, to be installed by TACACS+ as follows:</p> <pre>route="dst_address mask [gateway]"</pre> <p>This indicates a temporary static route that is to be applied. The <i>dst_address</i>, <i>mask</i>, and <i>gateway</i> are expected to be in the usual dotted-decimal notation, with the same meanings as in the familiar <b>ip route</b> configuration command on a network access server.</p> <p>If <i>gateway</i> is omitted, the peer's address is the gateway. The route is expunged when the connection terminates.</p>	no	yes	yes	yes	yes	yes	yes
route#<n>	Like the route AV pair, this specifies a route to be applied to an interface, but these routes are numbered, allowing multiple routes to be applied. Used with service=ppp and protocol=ip, and service=ppp and protocol=ipx.	no	no	no	yes	yes	yes	yes
routing=x	Specifies whether routing information is to be propagated to and accepted from this interface. Used with service=slip, service=ppp, and protocol=ip. Equivalent in function to the /routing flag in SLIP and PPP commands. Can either be true or false (for example, routing=true).	yes						
rte-fltr-in#<n>	Specifies an input access list definition to be installed and applied to routing updates on the current interface for the duration of the current connection. Used with service=ppp and protocol=ip, and with service=ppp and protocol=ipx.	no	no	no	yes	yes	yes	yes
rte-fltr-out#<n>	Specifies an output access list definition to be installed and applied to routing updates on the current interface for the duration of the current connection. Used with service=ppp and protocol=ip, and with service=ppp and protocol=ipx.	no	no	no	yes	yes	yes	yes
sap#<n>	Specifies static Service Advertising Protocol (SAP) entries to be installed for the duration of a connection. Used with service=ppp and protocol=ipx.	no	no	no	yes	yes	yes	yes

Table 80 Supported TACACS+ Authentication and Authorization AV Pairs (continued)

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
sap-fltr-in#<n>	Specifies an input SAP filter access list definition to be installed and applied on the current interface for the duration of the current connection. Used with service=ppp and protocol=ipx.	no	no	no	yes	yes	yes	yes
sap-fltr-out#<n>	Specifies an output SAP filter access list definition to be installed and applied on the current interface for the duration of the current connection. Used with service=ppp and protocol=ipx.	no	no	no	yes	yes	yes	yes
send-auth	Defines the protocol to use (PAP or CHAP) for username-password authentication following CLID authentication. Used with service=any and protocol=aaa.	no	no	no	no	no	yes	yes
send-secret	Specifies the password that the NAS needs to respond to a chap/pap request from the remote end of a connection on an outgoing call. Used with service=ppp and protocol=ip.	no	no	no	no	no	yes	yes
service=x	The primary service. Specifying a service attribute indicates that this is a request for authorization or accounting of that service. Current values are <b>slip</b> , <b>ppp</b> , <b>arap</b> , <b>shell</b> , <b>tty-daemon</b> , <b>connection</b> , and <b>system</b> . This attribute must always be included.	yes						
source-ip=x	Used as the source IP address of all VPDN packets generated as part of a VPDN tunnel. This is equivalent to the Cisco <b>vpdn outgoing</b> global configuration command.	no	no	yes	yes	yes	yes	yes
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 <b>ip mobile secure host &lt;addr&gt;</b> 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.	no	no	no	no	no	yes	yes
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						
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> in the <b>vpdn outgoing</b> command. Used with service=ppp and protocol=vpdn.	no	no	yes	yes	yes	yes	yes

**Table 80** Supported TACACS+ Authentication and Authorization AV Pairs (continued)

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
wins-servers=	Identifies a Windows NT server 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 Windows NT server is entered in dotted decimal format.	no	no	no	yes	yes	yes	yes
zonelist=x	A numeric zonelist value. Used with service=arap. Specifies an AppleTalk zonelist for ARA (for example, zonelist=5).	yes						

For more information about configuring TACACS+, refer to the chapter “Configuring TACACS+.” For more information about configuring TACACS+ authentication and authorization, refer to the chapters “Configuring Authentication” and “Configuring Authorization.”

## TACACS+ Accounting AV Pairs

[Table 81](#) lists and describes the supported TACACS+ accounting AV pairs and specifies the Cisco IOS release in which they are implemented.

**Table 81** Supported TACACS+ Accounting AV Pairs

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
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.	no	no	no	no	no	yes	yes
bytes_in	The number of input bytes transferred during this connection.	yes						
bytes_out	The number of output bytes transferred during this connection.	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						
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 <a href="#">Table 82</a> for a list of Disconnect-Cause values and their meanings.	no	no	no	yes	yes	yes	yes

Table 81 Supported TACACS+ Accounting AV Pairs (continued)

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
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						
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						
Fax-Account-Id-Origin	Indicates the account ID origin as defined by system administrator for the <b>mmoip aaa receive-id</b> or the <b>mmoip aaa send-id</b> 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

**Table 81** Supported TACACS+ Accounting AV Pairs (continued)

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
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						
paks_out	The number of output packets transferred during this connection.	yes						
port	The port the user was logged in to.	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)

Attribute	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2
pre-paks-out	Records the number of output packets before authentication. The Pre-Output-Packets attribute is sent in accounting-stop records.	no	no	no	yes	yes	yes	yes
pre-session-time	Specifies the length of time, in seconds, from when a call first connects to when it completes authentication.	no	no	no	yes	yes	yes	yes
priv_level	The privilege level associated with the action.	yes						
protocol	The protocol associated with the action.	yes						
reason	Information included in the accounting packet that describes the event that caused a system change. Events described are system reload, system shutdown, or when accounting is reconfigured (turned on or off).	yes						
service	The service the user used.	yes						
start_time	The time the action started (in seconds since the epoch, 12:00 a.m. Jan 1 1970). The clock must be configured to receive this information.	yes						
stop_time	The time the action stopped (in seconds since the epoch.) The clock must be configured to receive this information.	yes						
task_id	Start and stop records for the same event must have matching (unique) task_id numbers.	yes						
timezone	The time zone abbreviation for all timestamps included in this packet.	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

Cause Codes	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
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

Cause Codes	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
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	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	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	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	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	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	yes						

Cause Codes	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
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	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	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	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	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	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	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	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	yes						
1831 – Q850 Unspecified Cause	No other code applies. This code applies to ISDN or modem calls that came in over ISDN.	no	yes						

Cause Codes	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
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	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	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	yes						
1842 – Q850 Network Congestion	The network is congested. This code applies to ISDN or modem calls that came in over ISDN.	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	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	yes						
1845 – Q850 Call Pre-empted	The call was preempted. This code applies to ISDN or modem calls that came in over ISDN.	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	yes						
1850 – Q850 Facility Not Subscribed	Not a subscribed facility. This code applies to ISDN or modem calls that came in over ISDN.	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	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	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	yes						

Cause Codes	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
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	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	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	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	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	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	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	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	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	yes						

Cause Codes	Description	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
1898 – Q850 Invalid Message	This code is used to report an invalid message when no other code in the invalid message class applies. This code applies to ISDN or modem calls that have come in over ISDN.	no	yes						
1899 – Q850 Bad Info Element	The information element not recognized. This code applies to ISDN or modem calls that have come in over ISDN.	no	yes						
1900 – Q850 Invalid Element Contents	The equipment that is sending this code has received an information element that it has implemented; however, one or more fields in the information element are coded in such a way that has not been implemented by the equipment that is sending this code. This code applies to ISDN or modem calls that have come in over ISDN.	no	yes						
1901 – Q850 Wrong Message for State	The message that was received is incompatible with the call state. This code applies to ISDN or modem calls that have come in over ISDN.	no	yes						
1902 – Q850 Recovery on Timer Expiration	A procedure has been initiated by the expiration of a timer in association with error-handling procedures. This code applies to ISDN or modem calls that have come in over ISDN.	no	yes						
1903 – Q850 Info Element Error	The equipment that is sending this code has received a message that includes information elements or parameters that are not recognized because the information element identifiers or parameter names are not defined or are 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	yes						
1911 – Q850 Protocol Error	This code is used to report a protocol error event only when no other code in the protocol error class applies. This code applies to ISDN or modem calls that have come in over ISDN.	no	yes						
1927 – Q850 Unspecified Internetworking Event	There has been an error when interworking with a network that does not provide codes for actions that it takes. This code applies to ISDN or modem calls that have come in over ISDN.	no	yes						

For more information about configuring TACACS+ accounting, refer to the chapter “[Configuring Accounting](#).”

---

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 (SSH)**





# 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, see 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.

## 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**

© 2008 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

The 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 [Configuring Authentication](#), [Configuring Authorization](#), and [Configuring Accounting](#) chapters earlier in the book. See also [Enabling AAA](#).

## 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 default values will be used.

To configure SSH server, use the following command in global configuration mode:

Command	Purpose
<pre>Router(config)# ip ssh {[timeout seconds]   [authentication-retries integer]}</pre>	<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 vty 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 AAA is disabled on the console for user authentication. AAA authorization is disabled on the console by default. If AAA authorization is enabled on the console, disable it by configuring the **no aaa authorization console** command during the AAA configuration stage.

## 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 username1 password 0 password1
username username2 password 0 password2
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 username1 password 0 password1
username username2 password 0 password2
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 username1 password 0 password1
username username2 password 0 password2
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 sge-registers
no exception linecard slot 1 sge-registers
no exception linecard slot 2 sge-registers
no exception linecard slot 3 sge-registers
no exception linecard slot 4 sge-registers
no exception linecard slot 5 sge-registers
no exception linecard slot 6 sge-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	<code>transport input ssh</code>  <b>Example:</b> Router (config-line)# <code>transport input ssh</code>	Defines which protocols to use to connect to a specific line of the router. <ul style="list-style-type: none"> <li>The <code>ssh</code> keyword must be used for the Reverse SSH Enhancements feature.</li> </ul>
Step 7	<code>exit</code>  <b>Example:</b> Router (config-line)# <code>exit</code>	Exits line configuration mode.
Step 8	<code>exit</code>  <b>Example:</b> Router (config)# <code>exit</code>	Exits global configuration mode.
Step 9	<code>ssh -l userid:{number} {ip-address}</code>  <b>Example:</b> Router# <code>ssh -l lab:1 router.example.com</code>	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><code>userid</code>—User ID.</li> <li><code>:</code>—Signifies that a port number and terminal IP address will follow the <code>userid</code> argument.</li> <li><code>number</code>—Terminal or auxiliary line number.</li> <li><code>ip-address</code>—Terminal server IP address.</li> </ul> <p><b>Note</b> The <code>userid</code> argument and <code>:rotary{number}{ip-address}</code> delimiter and arguments are mandatory when configuring the alternative method of Reverse SSH for modem access.</p>

## 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

- `enable`
- `configure terminal`
- `line line-number [ending-line-number]`
- `no exec`
- `login authentication listname`
- `rotary group`
- `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 <i>line-number</i> [<i>ending-line-number</i>]</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 <i>listname</i></b>  <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.
Step 6	<b>rotary <i>group</i></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
<p><b>Step 10</b> <code>ssh -l userid:rotary{number} {ip-address}</code></p> <p><b>Example:</b> Router# <code>ssh -l lab:rotary1 router.example.com</code></p>	<p>Specifies the user ID to use when logging in on the remote networking device that is running the SSH server.</p> <ul style="list-style-type: none"> <li>• <i>userid</i>—User ID.</li> <li>• <code>:</code>—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> <p><b>Note</b> The <i>userid</i> argument and <code>:rotary{number}{ip-address}</code> delimiter and arguments are mandatory when configuring the alternative method of Reverse SSH for modem access.</p>

## 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
<p><b>Step 1</b> <code>enable</code></p> <p><b>Example:</b> Router&gt; <code>enable</code></p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<p><b>Step 2</b> <code>debug ip ssh client</code></p> <p><b>Example:</b> Router# <code>debug ip ssh client</code></p>	<p>Displays debugging messages for the SSH client.</p>

## 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 (rcp), 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</b> {default   list-name} method1 [method2...]  <b>Example:</b> Router (config)# aaa authentication login default group tacacs+	Enables the AAA access control system.
Step 5	<b>aaa authorization</b> {network   exec   commands level   reverse-access   configuration} {default   list-name} [method1 [method2...]]  <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</b> [privilege level] {password encryption-type encrypted-password}  <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	<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>show running-config</code>  <b>Example:</b> Router# <code>show running-config</code>	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	<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 scp</code>  <b>Example:</b> Router# <code>debug ip scp</code>	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.	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
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.

---

---

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 Version 2 Support

---

**First Published: November 3, 2003**  
**Last Updated: June 19, 2009**

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

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 Secure Shell Version 2 Support”](#) section on page 23.

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 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 15](#)
- [Where to Go Next, page 20](#)



---

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

- [Additional References, page 20](#)
- [Command Reference, page 22](#)
- [Feature Information for Secure Shell Version 2 Support, page 23](#)

## 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

- 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.
- Rivest, Shamir, and Adelman (RSA) key generation is an SSH server side requirement. Routers that act as SSH clients do not need to generate RSA keys.
- The RSA key-pair size must be greater than or equal to 768.
- The following functionality is not supported:
  - RSA user authentication (in the SSH server or SSH client for Cisco IOS software)
  - Public key authentication
  - SSH server strict host key check
  - Port forwarding
  - Compression

## Information About Secure Shell Version 2 Support

To configure SSH Version 2, you should understand the following concepts:

- [Secure Shell Version 2, page 3](#)
- [SNMP Trap Generation, page 4](#)
- [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 5](#) (required)
- [Configuring a Router for SSH Version 2 Using RSA Key Pairs, page 6](#) (optional)
- [Starting an Encrypted Session with a Remote Device, page 7](#) (optional)
- [Enabling Secure Copy Protocol on the SSH Server, page 8](#) (optional)
- [Verifying the Status of the Secure Shell Connection Using the show ssh Command, page 10](#) (optional)
- [Verifying the Secure Shell Status Using the show ip ssh Command, page 11](#) (optional)
- [Monitoring and Maintaining Secure Shell Version 2, page 12](#) (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** [**time-out** *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</b> <i>hostname</i>  <b>Example:</b> Router (config)# hostname cisco 7200	Configures a host name for your router.
Step 4	<b>ip domain-name</b> <i>name</i>  <b>Example:</b> Router (config)# ip domain-name example.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.

	Command or Action	Purpose
Step 6	<pre>ip ssh [time-out seconds   authentication-retries integer]</pre> <p><b>Example:</b> Router (config)# ip ssh time-out 120</p>	(Optional) Configures SSH control variables on your router.
Step 7	<pre>ip ssh version [1   2]</pre> <p><b>Example:</b> Router (config)# ip ssh version 1</p>	(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 [time-out seconds | authentication-retries integer]**
6. **ip ssh version 2**

### DETAILED STEPS

Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal</p>	Enters global configuration mode.
Step 3	<pre>ip ssh rsa keypair-name keypair-name</pre> <p><b>Example:</b> Router (config)# ip ssh rsa keypair-name sshkeys</p>	Specifies which RSA keypair to use for SSH usage. <p><b>Note</b> A Cisco IOS router can have many RSA key pairs.</p>

<b>Step 4</b>	<pre>crypto key generate rsa usage-keys label key-label modulus modulus-size</pre> <p><b>Example:</b> Router (config)# crypto key generate rsa usage-keys label sshkeys modulus 768</p>	<p>Enables the SSH server for local and remote authentication on the router.</p> <p>For SSH Version 2, the modulus size must be at least 768 bits.</p> <p><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.</p>
<b>Step 5</b>	<pre>ip ssh [time-out seconds   authentication-retries integer]</pre> <p><b>Example:</b> Router (config)# ip ssh time-out 120</p>	<p>Configures SSH control variables on your router.</p>
<b>Step 6</b>	<pre>ip ssh version 2</pre> <p><b>Example:</b> Router (config)# ip ssh version 2</p>	<p>Specifies the version of SSH to be run on a router.</p>

## 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

<p><b>Step 1</b></p> <pre>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]</pre> <p><b>Example:</b></p> <pre>Router# ssh -v 2 -c aes256-cbc -m hmac-sha1-96 -l user2 10.76.82.24</pre> <p>Or</p> <p>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:</p> <pre>Router# ssh -v 2 -c aes256-cbc -m hmac-sha1-96 user2@10.76.82.24</pre>	<p>Starts an encrypted session with a remote networking device.</p>
---	---

## 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.

## Enabling Secure Copy Protocol on the SSH Server

To configure server-side functionality for SCP, perform the following steps. This example shows a typical configuration that allows the router to securely copy files from a remote workstation.

### Prerequisites

SCP relies on AAA authentication and authorization to function correctly. Therefore AAA must be configured on the router.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login default local**
5. **aaa authorization exec default local**

6. **username** *name* **privilege** *privilege-level* **password** *password*
7. **ip ssh time-out** *seconds*
8. **ip ssh authentication-retries** *integer*
9. **ip scp server enable**

## DETAILED STEPS

<b>Step 1</b>	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
<b>Step 3</b>	<p><b>aaa new-model</b></p> <p><b>Example:</b> Router(config)# aaa new-model</p>	<p>Enables the authentication, authorization, and accounting (AAA) access control model.</p>
<b>Step 4</b>	<p><b>aaa authentication login default local</b></p> <p><b>Example:</b> Router(config)# aaa authentication login default local</p>	<p>Sets authentication, authorization, and accounting (AAA) authentication at login to use the local username database for authentication.</p>
<b>Step 5</b>	<p><b>aaa authorization exec default local</b></p> <p><b>Example:</b> Router(config)# aaa authorization exec default local</p>	<p>Sets the parameters that restrict user access to a network; runs the authorization to determine if the user ID allowed to run an EXEC shell; and specifies that the system uses the local database for authorization.</p>
<b>Step 6</b>	<p><b>username</b> <i>name</i> <b>privilege</b> <i>privilege-level</i> <b>password</b> <i>password</i></p> <p><b>Example:</b> Router(config)# username samplename privilege 15 password password1</p>	<p>Establishes a username-based authentication system, specifies the username, the privilege level, and an unencrypted password.</p>
<b>Step 7</b>	<p><b>ip ssh time-out</b> <i>seconds</i></p> <p><b>Example:</b> Router(config)# ip ssh time-out 120</p>	<p>Sets the time interval (in seconds) that the router waits for the SSH client to respond.</p>

<b>Step 8</b>	<p><code>ip ssh authentication-retries <i>integer</i></code></p> <p><b>Example:</b> Router(config)# ip ssh authentication-retries 3</p>	Sets the number of authentication attempts after which the interface is reset.
<b>Step 9</b>	<p><code>ip scp server enable</code></p> <p><b>Example:</b> Router (config)# ip scp server enable</p>	Enables the router to securely copy files from a remote workstation.

## Troubleshooting Tips

To troubleshoot SCP authentication problems, use the **debug ip scp** command.

## 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

<b>Step 1</b>	<p><code>enable</code></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<p><code>show ssh</code></p> <p><b>Example:</b> Router# show ssh</p>	Displays the status of SSH server connections.

## 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

<b>Step 1</b>	<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>
<b>Step 2</b>	<b>show ip ssh</b>  <b>Example:</b> Router# show ip ssh	Displays the version and configuration data for 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

<b>Step 1</b>	<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>
<b>Step 2</b>	<b>debug ip ssh</b>  <b>Example:</b> Router# debug ip ssh	Displays debugging messages for SSH.
<b>Step 3</b>	<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 15](#)
- [Configuring Secure Shell Version 2: Example, page 15](#)
- [Configuring Secure Shell Versions 1 and 2: Example, page 16](#)
- [Starting an Encrypted Session with a Remote Device: Example, page 16](#)
- [Configuring Server-Side SCP: Example, page 16](#)
- [Setting an SNMP Trap: Example, page 16](#)
- [SSH Keyboard Interactive Authentication: Examples, page 16](#)
- [SNMP Debugging: Example, page 18](#)
- [SSH Debugging Enhancements: Examples, page 19](#)

### Configuring Secure Shell Version 1: Example

```
Router# configure terminal
Router (config)# ip ssh version 1
Router (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
```

## Configuring Server-Side SCP: Example

The following example shows how to configure server-side functionality for SCP. This example also configures AAA authentication and Authorization on the router. This example uses a locally defined username and password.

```
Router# configure terminal
Router (config)# aaa new-model
Router (config)# aaa authentication login default local
Router (config)# aaa authorization exec default local
Router (config)# username samplename privilege 15 password password1
Router (config)# ip ssh time-out 120
Router (config)# ip ssh authentication-retries 3
Router (config)# ip scp server enable
Router (config)# end
```

## 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>
Configuring Secure Shell	<a href="#">“Configuring Secure Shell”</a> chapter of the <i>Cisco IOS Security Configuration Guide</i>
Debugging commands	<a href="#">Cisco IOS Debug Command Reference</a>
Downloading a Cisco software image	<a href="#">Cisco IOS Configuration Fundamentals and Network Management Configuration Guide</a>
IOS configuration fundamentals	<a href="#">Cisco IOS Configuration Fundamentals and Network Management Configuration Guide</a> and <a href="#">Cisco IOS Configuration Fundamentals and Network Management Command Reference</a>
IPSec	<a href="#">“IP Security and Encryption”</a> section of the <i>Cisco IOS Security Configuration Guide</i>

Related Topic	Document Title
Security commands	<i>Cisco IOS Security Command Reference</i>
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>	<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 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, Catalyst OS, and Cisco IOS XE 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 4</li> <li>“SNMP Debugging: Example” section on page 18</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 16</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 the Cisco ASR 1000 series routers.
Secure Shell Version 2 Enhancements	12.4(20)T Cisco IOS XE Release 2.4	<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>This feature was implemented on the Cisco ASR 1000 series routers.</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> <li>• <a href="#">“Configuring Server-Side SCP: Example” section on page 16</a></li> </ul>

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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

© 2003 – 2009 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
<b>Step 1</b>	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.
<b>Step 2</b>	Router(config-line)# <b>no exec</b>	Disables exec processing on each of the lines.
<b>Step 3</b>	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.
<b>Step 4</b>	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.
<b>Step 5</b>	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.
<b>Step 6</b>	Router(config-line)# <b>exit</b>	Exits line configuration mode.
<b>Step 7</b>	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 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 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.



---

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

© 2007 Cisco Systems, Inc. All rights reserved.

# Contents

- [Information About Cisco IOS Login Enhancements, page 2](#)
- [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	<p><code>enable</code></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<p><code>configure terminal</code></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><code>login block-for seconds attempts tries within seconds</code></p> <p><b>Example:</b> Router(config)# login block-for 100 attempts 2 within 100</p>	<p>Configures your Cisco IOS device for login parameters that help provide DoS detection.</p> <p><b>Note</b> This command must be issued before any other login command can be used.</p>
Step 4	<p><code>login quiet-mode access-class {acl-name   acl-number}</code></p> <p><b>Example:</b> Router(config)# login quiet-mode access-class myacl</p>	<p>(Optional) Specifies an ACL that is to be applied to the router when it switches to quiet mode.</p> <p>If this command is not enabled, all login requests will be denied during quiet mode.</p>
Step 5	<p><code>login delay seconds</code></p> <p><b>Example:</b> Router(config)# login delay 10</p>	<p>(Optional) Configures a delay between successive login attempts.</p>
Step 6	<p><code>login on-failure log [every login]</code></p> <p><b>Example:</b> Router(config)# login on-failure log</p>	<p>(Optional) Generates logging messages for failed login attempts.</p>
Step 7	<p><code>login on-success log [every login]</code></p> <p><b>Example:</b> Router(config)# login on-success log every 5</p>	<p>(Optional) Generates logging messages for successful login attempts.</p>

## 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	<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 login [failures]</b>  <b>Example:</b> Router# show login	Displays login parameters. <ul style="list-style-type: none"> <li>• <b>failures</b>—Displays information related only to failed login attempts.</li> </ul>

### 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"> <li>• <i>AutoSecure</i> (Cisco IOS Release 12.3(1) feature module)</li> <li>• Cisco IOS Security Configuration Guides, Release 12.4.</li> </ul>
Secure Management/Administrative Access	Role-Based CLI Access

### 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><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

### RFCs

RFCs	Title
None	—

### Technical Assistance

Description	Link
<p>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.</p>	<p><a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a></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](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**

---

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 Resilient Configuration

---

**First Published: May 17, 2004**  
**Last Updated: July 8, 2009**

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).

## 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 Cisco IOS Resilient Configuration” section on page 9](#).

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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. An account on Cisco.com is not required.

## 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 7](#)
- [Feature Information for Cisco IOS Resilient Configuration, page 9](#)



---

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

## 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	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>secure boot-image</b>  <b>Example:</b> Router(config)# secure boot-image	Enables Cisco IOS image resilience.
Step 4	<b>secure boot-config</b>  <b>Example:</b> Router(config)# secure boot-config	Stores a secure copy of the primary bootset in persistent storage.

	Command or Action	Purpose
Step 5	<code>end</code>	Exits to privileged EXEC mode.
	<b>Example:</b> <code>Router(config)# end</code>	
Step 6	<code>show secure bootset</code>	(Optional) Displays the status of configuration resilience and the primary bootset filename.
	<b>Example:</b> <code>Router# show secure bootset</code>	

## 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	<b>reload</b>  <b>Example:</b> Router# reload	(Optional) Enters ROM monitor mode, if necessary.
Step 2	<b>dir</b> [ <i>filesystem:</i> ]  <b>Example:</b> rommon 1 > dir slot0:	Lists the contents of the device that contains the secure bootset file. <ul style="list-style-type: none"> <li>The device name can be found in the output of the <b>show secure bootset</b> command.</li> </ul>
Step 3	<b>boot</b> [ <i>partition-number:</i> ][ <i>filename</i> ]  <b>Example:</b> rommon 2 > boot slot0:c3745-js2-mz	Boots up the router using the secure bootset image.
Step 4	<b>no</b>  <b>Example:</b> --- 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"> <li>If the NVRAM was erased, the router enters setup mode and prompts the user to initiate an interactive configuration session.</li> </ul>
Step 5	<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 6	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 7	<b>secure boot-config</b> [restore <i>filename</i> ]  <b>Example:</b> Router(config)# secure boot-config restore slot0:rescue-cfg	Restores the secure configuration to the supplied filename.

	Command or Action	Purpose
Step 8	<b>end</b>  <b>Example:</b> Router(config)# end	Exits to privileged EXEC mode.
Step 9	<b>copy filename running-config</b>  <b>Example:</b> 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 12.4T</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 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><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

# Feature Information for Cisco IOS Resilient Configuration

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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. 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 Resilient Configuration

Feature Name	Releases	Feature Information
Cisco IOS Resilient Configuration	12.3(8)T Cisco IOS XE Release 2.1	<p>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).</p> <p>In 12.3(8)T this feature was introduced.</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: <b>secure boot-config, secure boot-image, show secure bootset.</b></p>

---

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

---

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

© 2004–2009 Cisco Systems, Inc. All rights reserved.



# Image Verification

---

**First Published: September 11, 2007**  
**Last Updated: February 6, 2009**

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.

## 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 Image Verification”](#) section on page 9.

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 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](#)
- [Feature Information for Image Verification, page 9](#)



---

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

# 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.



### Note

---

The Image Verification feature can only be used to check the integrity of a Cisco IOS software image that is stored on a Cisco IOS device. It cannot be used to check the integrity of an image on a remote file system or an image running in memory.

---

# 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	<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>file verify auto</b>  <b>Example:</b> Router(config)# file verify auto	Enables automatic image verification.
Step 4	<b>exit</b>  <b>Example:</b> 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	<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>copy</b> [/erase] [/verify   /noverify] <i>source-url destination-url</i>  <b>Example:</b> 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"> <li>• <b>/verify</b>—Verifies the signature of the destination file. If verification fails, the file will be deleted.</li> <li>• <b>/noverify</b>—Does not verify the signature of the destination file before the image is copied.</li> </ul> <p><b>Note</b> <b>/noverify</b> is often issued if the <b>file verify auto</b> command is enabled, which automatically verifies the signature of all images that are copied.</p>
Step 3	<b>verify</b> [/md5 [md5-value]] <i>filesystem:[file-url]</i>  <b>Example:</b> 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	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre>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]</pre> <p><b>Example:</b> Router# reload /verify</p>	Reloads the operating system. <ul style="list-style-type: none"> <li>• <b>/verify</b>—Verifies the signature of the destination file. If verification fails, the file will be deleted.</li> <li>• <b>/noverify</b>—Does not verify the signature of the destination file before the image is reloaded.</li> </ul> <p><b>Note</b> <b>/noverify</b> is often issued if the <b>file verify auto</b> command is enabled, which automatically verifies the signature of all images that are copied.</p>

## 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 the Image Verification feature.

### 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

Standard	Title
None	—

### MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> <li>None</li> </ul>	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

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><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 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).

### New Command

- **file verify auto**

### Modified Commands

- **copy**
- **reload**
- **verify**

# Feature Information for Image Verification

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, Catalyst OS, and Cisco IOS XE 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 Image Verification

Feature Name	Releases	Feature Information
Image Verification	12.2(25)S 12.0(26)S 12.3(4)T Cisco IOS XE Release 2.1	The Image Verification feature allows users to automatically verify the integrity of Cisco IOS images.  The following commands were introduced or modified: <b>copy, file verify auto, reload, verify.</b>

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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.

© 2007–2009 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.

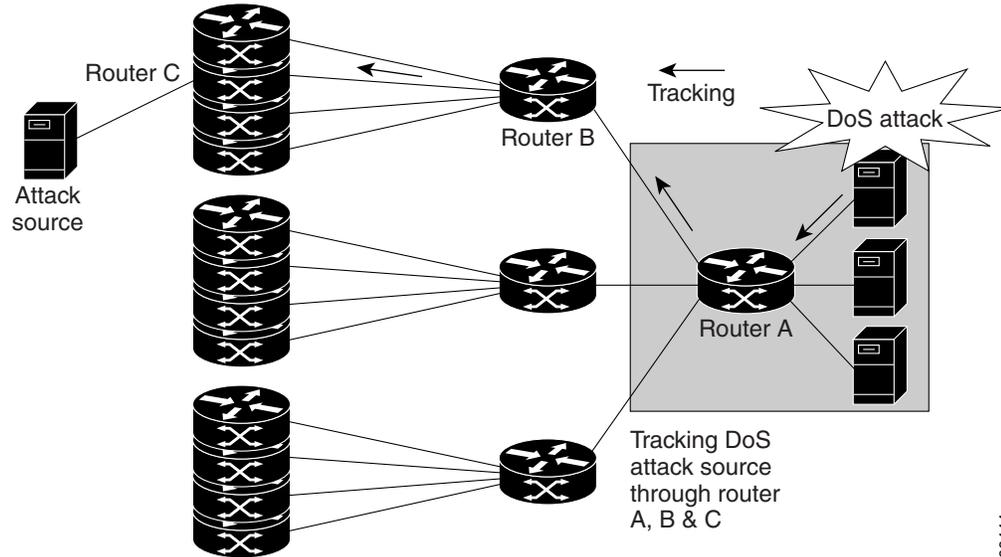
To trace attacks, NetFlow and access control lists (ACLs) have been used. To block attacks, committed access rate (CAR) and ACLs have been used. Support for these features on the Cisco 12000 series Internet router has depended on the type of line card used. Support for these features on the Cisco 7500 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	<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 source-track ip-address</b>  <b>Example:</b> Router(config)# ip source-track 100.10.0.1	Enables IP source tracking for a specified host.
Step 4	<b>ip source-track address-limit number</b>  <b>Example:</b> Router(config)# ip source-track address-limit 10	(Optional) Limits the number of hosts that can be simultaneously tracked at any given time.  <b>Note</b> If this command is not enabled, there is no limit to the number of hosts that be can tracked.
Step 5	<b>ip source-track syslog-interval number</b>  <b>Example:</b> 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.  <b>Note</b> If this command is not enabled, system log messages are not generated.
Step 6	<b>ip source-track export-interval number</b>  <b>Example:</b> 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).  <b>Note</b> 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	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<p><b>show ip source-track</b> [<i>ip-address</i>] [summary   cache]</p> <p><b>Example:</b> Router# show ip source-track summary</p>	<p>Displays traffic flow statistics for tracked IP host addresses</p>
Step 3	<p><b>show ip source-track export flows</b></p> <p><b>Example:</b> Router# show ip source-track export flows</p>	<p>Displays the last 10 packet flows that were exported from the line card to the route processor.</p> <p><b>Note</b> This command can be issued only on distributed platforms, such as the GRP and the RSP.</p>

## 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 ager 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
None	—

## Techn

ical 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 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](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.



## 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.

## 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 Role-Based CLI Access” section on page 14](#).

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 Role-Based CLI Access, page 2](#)
- [Restrictions for Role-Based CLI Access, page 2](#)
- [Information About Role-Based CLI Access, page 2](#)
- [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](#)



---

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

© 2004, 2007-2008 Cisco Systems, Inc. All rights reserved.

# 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 2](#)
- [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.
- 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	<p><code>enable view</code></p> <p><b>Example:</b> Router&gt; enable view</p>	<p>Enables root view.</p> <ul style="list-style-type: none"> <li>Enter your privilege level 15 password (for example, root password) if prompted.</li> </ul>
Step 2	<p><code>configure terminal</code></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><code>parser view view-name</code></p> <p><b>Example:</b> Router(config)# parser view first</p>	<p>Creates a view and enters view configuration mode.</p>
Step 4	<p><code>secret 5 encrypted-password</code></p> <p><b>Example:</b> Router(config-view)# secret 5 secret</p>	<p>Associates a command-line interface (CLI) view or superview with a password.</p> <p><b>Note</b> You must issue this command before you can configure additional attributes for the view.</p>
Step 5	<p><code>commands parser-mode {include   include-exclusive   exclude} [all] [interface interface-name   command]</code></p> <p><b>Example:</b> Router(config-view)# commands exec include show version</p>	<p>Adds commands or interfaces to a view.</p> <ul style="list-style-type: none"> <li><i>parser-mode</i>—The mode in which the specified command exists.</li> <li><b>include</b>—Adds a command or an interface to the view and allows the same command or interface to be added to an additional view.</li> <li><b>include-exclusive</b>—Adds a command or an interface to the view and excludes the same command or interface from being added to all other views.</li> <li><b>exclude</b>—Excludes a command or an interface from the view; that is, customers cannot access a command or an interface.</li> <li><b>all</b>—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.</li> <li><b>interface interface-name</b>—Interface that is added to the view.</li> <li><i>command</i>—Command that is added to the view.</li> </ul>
Step 6	<p><code>exit</code></p> <p><b>Example:</b> Router(config-view)# exit</p>	<p>Exits view configuration mode.</p>

	Command or Action	Purpose
Step 7	<code>exit</code>  <b>Example:</b> Router(config)# <code>exit</code>	Exits global configuration mode.
Step 8	<code>enable [privilege-level] [view view-name]</code>  <b>Example:</b> Router# <code>enable view first</code>	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	<code>show parser view [all]</code>  <b>Example:</b> Router# <code>show parser view</code>	(Optional) Displays information about the view that the user is currently in.  <ul style="list-style-type: none"> <li><b>all</b>—Displays information for all views that are configured on the router.</li> </ul> <p><b>Note</b> Although this command is available for both root and lawful intercept users, the <b>all</b> keyword is available only to root users. However, the <b>all</b> keyword can be configured by a user in root view to be available for users in lawful intercept view and CLI view.</p>

## 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	<b>enable view</b>  <b>Example:</b> Router> enable view	Enables root view.  <ul style="list-style-type: none"> <li>• Enter your privilege level 15 password (for example, root password) if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>li-view</b> <i>li-password</i> <b>user</b> <i>username</i> <b>password</b> <i>password</i>  <b>Example:</b> 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 <b>user</b> <i>username</i> <b>password</b> <i>password</i> options.
Step 4	<b>username</b> [ <b>lawful-intercept</b> ] [ <i>name</i> ] [ <b>privilege</b> <i>privilege-level</i>   <b>view</b> <i>view-name</i> ] <b>password</b> <i>password</i>  <b>Example:</b> Router(config)# username lawful-intercept li-user1 password li-user1pass	Configures lawful intercept users on a Cisco device.

	Command or Action	Purpose
Step 5	<b>parser view</b> <i>view-name</i>  <b>Example:</b> 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	<b>secret 5</b> <i>encrypted-password</i>  <b>Example:</b> Router(config-view)# secret 5 secret	(Optional) Changes an existing password for a lawful intercept view.
Step 7	<b>name</b> <i>new-name</i>  <b>Example:</b> 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**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable view</b>  <b>Example:</b> Router> enable view	Enables root view.  <ul style="list-style-type: none"> <li>• Enter your privilege level 15 password (for example, root password) if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>parser view</b> <i>superview-name</i> <b>superview</b>  <b>Example:</b> Router(config)# parser view su_view1 superview	Creates a superview and enters view configuration mode.
<b>Step 4</b>	<b>secret 5</b> <i>encrypted-password</i>  <b>Example:</b> Router(config-view)# secret 5 secret	Associates a CLI view or superview with a password.  <b>Note</b> You must issue this command before you can configure additional attributes for the view.
<b>Step 5</b>	<b>view</b> <i>view-name</i>  <b>Example:</b> 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.
<b>Step 6</b>	<b>exit</b>  <b>Example:</b> Router(config-view)# exit	Exits view configuration mode.

	Command or Action	Purpose
Step 7	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits global configuration mode.
Step 8	<b>show parser view [all]</b>  <b>Example:</b> Router# show parser view	(Optional) Displays information about the view that the user is currently in. <ul style="list-style-type: none"> <li><b>all</b>—Displays information for all views that are configured on the router.</li> </ul> <b>Note</b> Although this command is available for both root and lawful intercept users, the <b>all</b> keyword is available only to root users. However, the <b>all</b> keyword can be configured by a user in root view to be available for users in lawful intercept view and CLI view.

## 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$QuZaU8PIMP1ff9sFCZvgW/
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** 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 “ <a href="#">Configuring SNMP</a> ” in the <i>Cisco IOS Network Management Configuration Guide</i> .
Privilege levels	The chapter “ <a href="#">Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices</a> ” 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: <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/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*.

- **commands (view)**
- **enable**
- **li-view**
- **name (view)**
- **parser view**
- **parser view superview**
- **secret**
- **show parser view**
- **show users**
- **username**
- **view**

# Feature Information for Role-Based CLI Access

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, Catalyst OS, and Cisco IOS XE 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 Role-Based CLI Access

Feature Name	Releases	Feature Information
Role-Based CLI Access	12.3(7)T	This feature enables network administrators to restrict user access to CLI and configuration information.
	12.3(11)T	
	12.2(33)SRB	In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers
	12.2(33)SB	In 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.
	Cisco IOS XE Release 2.1	
12.2(33)SXI		

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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, 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

---

**First Published: May 2, 2005**

**Last Updated: May 4, 2009**

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.

## 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 Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices”](#) section on page 42.

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.



---

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

© 2007 Cisco Systems, Inc. All rights reserved.

# Contents

- [Restrictions for Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices, page 2](#)
- [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 39](#)
- [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
systat         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
<pre>Router&gt; enable Password Router# exit Router&gt;</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• If a privileged EXEC mode password has been configured the system will prompt you for a password after you issue the enable command.</li> <li>• Use the exit command to leave privileged EXEC mode.</li> </ul>



### 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# <b>disable</b>	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# <b>configure terminal</b>	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)# <b>end</b> or Router(config)# ^z	Ends the current configuration session and returns to privileged EXEC mode.
Router(config)# <b>exit</b>	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)# <b>interface</b> <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)# <b>interface</b> <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](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
<b>enable</b>  <b>Example:</b> Router> <b>enable</b> Password Router#	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted. The password will not be shown in the terminal window.</li> <li>• The “&gt;” at the end of the prompt string is changed to a “#” to indicate that you are in privileged EXEC mode.</li> </ul>

## 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 username1 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*.

([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 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	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><b>line vty</b> <i>line-number</i> [<i>ending-line-number</i>]</p> <p><b>Example:</b> Router(config)# line vty 0 4</p>	<p>Enters line configuration mode.</p>
Step 4	<p><b>password</b> <i>password</i></p> <p><b>Example:</b> Router(config-line)# password H7x3U8</p>	<p>The argument <i>password</i> is a character string that specifies the line password. The following rules apply to the <i>password</i> argument:</p> <ul style="list-style-type: none"> <li>The first character cannot be a number.</li> <li>The string can contain any alphanumeric characters, including spaces, up to 80 characters. You cannot specify the password in the format number-space-anything.</li> <li>Passwords are case sensitive.</li> </ul>
Step 5	<p><b>end</b></p> <p><b>Example:</b> Router(config-line)# end</p>	<p>Exits the current configuration mode and returns to privileged EXEC mode.</p>
Step 6	<p><b>telnet</b> <i>ip-address</i></p> <p><b>Example:</b> Router# telnet 172.16.1.1</p>	<p>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).</p> <ul style="list-style-type: none"> <li>Enter the password that you configured in step 4 when prompted.</li> </ul> <p><b>Note</b> This procedure is often referred to as a 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	<p><b>exit</b></p>	<p>Terminates the remote CLI session (recursive Telnet session) with the networking device.</p>

## 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	<code>enable</code>  <b>Example:</b> <code>Router&gt; 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>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>line console 0</code>  <b>Example:</b> <code>Router(config)# line console 0</code>	Enters line configuration mode and selects the console port as the line that you are configuring.
Step 4	<code>password password</code>  <b>Example:</b> <code>Router(config-line)# password Ji8F5Z</code>	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"> <li>The first character cannot be a number.</li> <li>The string can contain any alphanumeric characters, including spaces, up to 80 characters. You cannot specify the password in the format <code>number-space-anything</code>.</li> <li>Passwords are case sensitive.</li> </ul>
Step 5	<code>end</code>  <b>Example:</b> <code>Router(config-line)# end</code>	Exits the current configuration mode and returns to privileged EXEC mode.
Step 6	<code>exit</code>  <b>Example:</b> <code>Router# exit</code>	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"> <li>Enter the password that you configured in step 4 when prompted to verify that it was configured correctly.</li> </ul> <p><b>Note</b> This step can be performed only if you are using a local CLI session to perform this task.</p>

### 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	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><b>enable password password</b></p> <p><b>Example:</b> Router(config)# enable password t6D77CdKq</p>	<p>The argument <i>password</i> is a character string that specifies the enable password. The following rules apply to the <i>password</i> argument:</p> <ul style="list-style-type: none"> <li>Must contain from 1 to 25 uppercase and lowercase alphanumeric characters.</li> <li>Must not have a number as the first character.</li> <li>Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.</li> <li>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"> <li>Enter abc</li> <li>Type Ctrl-v</li> <li>Enter ?123</li> </ul> </li> </ul>
Step 4	<p><b>end</b></p> <p><b>Example:</b> Router(config)# end</p>	<p>Exits the current configuration mode and returns to privileged EXEC mode.</p>
Step 5	<p><b>exit</b></p> <p><b>Example:</b> Router# exit</p>	<p>Exits privileged EXEC mode.</p>
Step 6	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter the password you configured in step 3.</li> </ul>

## 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	<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>service password-encryption</b>  <b>Example:</b> 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	<b>end</b>  <b>Example:</b> 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

- enable**
- configure terminal**
- enable secret** *password*  
or  
**enable secret** *5 previously-encrypted-password*
- end**
- exit
- enable

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><b>enable secret password</b> or <b>enable secret 5 previously-encrypted-password</b></p> <p><b>Example:</b> Router(config)# enable secret t6D77CdKq or</p> <p><b>Example:</b> Router(config)# enable secret 5 \$1\$/x6H\$RhnDI3yLC4GA01aJnHLQ4/</p>	<p>The argument <i>password</i> is a character string that specifies the <b>enable secret</b> password. The following rules apply to the <i>password</i> argument:</p> <ul style="list-style-type: none"> <li>Must contain from 1 to 25 uppercase and lowercase alphanumeric characters.</li> <li>Must not have a number as the first character.</li> <li>Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.</li> <li>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"> <li>Enter abc</li> <li>Type Ctrl-v</li> <li>Enter ?123</li> </ul> </li> </ul> <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 <b>enable secret</b> command to use this method.</p>
Step 4	<p><b>end</b></p> <p><b>Example:</b> Router(config)# end</p>	<p>Exits the current configuration mode and returns to privileged EXEC mode.</p>

	Command or Action	Purpose
Step 5	<code>exit</code>  <b>Example:</b> Router# <code>exit</code>	Exits privileged EXEC mode.
Step 6	<code>enable</code>  <b>Example:</b> Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter the password that you configured in Step 3.</li> </ul>

### 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** *password*  
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** *level password*  
Configures a new enable secret password for privilege level 7.  
Router(config)# **enable secret level** 7 Zy72sKj
- Step 4** **privilege exec level** *level command-string*  
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** *level command-string*  
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 of 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
```

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	<a href="#">Role-Based CLI Access</a>
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	<a href="#">Neighbor Router Authentication: Overview and Guidelines</a>
Assigning privilege levels with TACACS+ and RADIUS	<a href="#">How to Assign Privilege Levels with TACACS+ and RADIUS</a>

## 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: <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 functionality, and support for existing RFCs has not been modified.	—

## 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 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 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, Catalyst OS, and Cisco IOS XE 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 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 Cisco IOS XE Release 2.1	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).  In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 series routers.  The following sections provide information about this feature: <ul style="list-style-type: none"> <li>• <a href="#">Configuring and Verifying the Networking Device to Require a Username for the First-Line Technical Support Staff, page 30</a></li> <li>• <a href="#">Configuring and Verifying the Enable Secret Password, page 23</a></li> </ul>
Privilege Command Enhancement	12.0(22)S 12.2(13)T	The keyword <b>all</b> was added to the <b>privilege</b> command as a wild card to reduce the number of times that the <b>privilege</b> command is entered when you are changing the privilege level of several keywords for the same command.  The following sections provide information about this feature: <ul style="list-style-type: none"> <li>• <a href="#">Privilege Command Enhancement, page 26</a></li> </ul>

---

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, 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, 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. (0903R)

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

© 2005–2009 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	<p><b>reload</b></p> <p><b>Example:</b> Router&gt; reload</p>	<p>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.</p> <p>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.</p> <p><b>Note</b> The default Break key combination is Ctrl-C, but this may be configured differently on your system.</p>
Step 2	<p><b>set tftp-file ip-address ip-subnet-mask default-gateway tftp-server</b></p> <p><b>Example:</b> ROMMON&gt; set tftpabc 10.10.0.0 255.0.0.0 10.1.1.0 10.29.32.0</p>	<p>Displays all the created variables. The arguments are as follows:</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <i>ip-address</i>—IP address on the router to connect to the TFTP server.</li> <li>• <i>ip-subnet-mask</i>—IP subnet mask of the router.</li> <li>• <i>default-gateway</i>—IP address of the gateway of the TFTP server.</li> <li>• <i>tftp-server</i>—IP address of the TFTP server from which the image will be downloaded.</li> </ul> <p><b>Note</b> This command is not supported on the Cisco 800 series routers.</p>
Step 3	<p><b>sync</b></p> <p><b>Example:</b> ROMMON&gt; sync</p>	<p>Saves the changes to the image.</p>
Step 4	<p><b>tftpdnld -u</b></p> <p><b>Example:</b> ROMMON&gt; tftpdnld -u</p>	<p>Downloads the new ROMMON image from the TFTP server. Reset if prompted.</p>
Step 5	<p><b>boot</b></p> <p><b>Example:</b> ROMMON&gt; boot</p>	<p>Boots the router with the Cisco IOS image in flash memory.</p>

## 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	<code>enable</code>  <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	<code>show version</code>  <b>Example:</b> Router# show version	Displays information about the system software, including configuration register settings. The configuration register must be set to autoboot before entering the <b>no service password-recovery</b> command.
Step 3	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 4	<code>config-register value</code>  <b>Example:</b> Router(config)# config-register 0x2012	(Optional) Changes the configuration register setting. <ul style="list-style-type: none"> <li>• If necessary, change the configuration register setting so the router is set to autoboot.</li> </ul>
Step 5	<code>no service password-recovery</code>  <b>Example:</b> Router(config)# no service password-recovery	Disables password-recovery capability at the system console.
Step 6	<code>exit</code>  <b>Example:</b> 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](mailto: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](mailto: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: <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
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*.

- **service password-recovery**

---

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.





## 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	<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 traffic-export profile</b> <i>profile-name</i>  <b>Example:</b> 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	<b>interface</b> <i>interface-name</i>  <b>Example:</b> Router(config-rite)# interface FastEthernet 0/1	Specifies the outgoing (monitored) interface for exported traffic.  <b>Note</b> If you do not issue this command, the profile will not recognize an interface in which to send the captured IP traffic.
Step 5	<b>bidirectional</b>  <b>Example:</b> Router(config-rite)# bidirectional	(Optional) Exports incoming and outgoing IP traffic on the monitored interface.  <b>Note</b> If this command is not enabled, only incoming traffic is exported.
Step 6	<b>mac-address</b> <i>H.H.H</i>  <b>Example:</b> Router(config-rite)# mac-address 00a.8aab.90a0	Specifies the 48-bit address of the destination host that is receiving the exported traffic.  <b>Note</b> If you do not issue this command, the profile will not recognize a destination host in which to send the exported packets.
Step 7	<b>incoming</b> { <b>access-list</b> { <i>standard</i>   <i>extended</i>   <i>named</i> }   <b>sample one-in-every</b> <i>packet-number</i> }  <b>Example:</b> Router(config-rite)# incoming access-list my_acl	(Optional) Configures filtering for incoming traffic. After you have created a profile via the <b>ip traffic-export profile</b> , this functionality is enabled by default.
Step 8	<b>outgoing</b> { <b>access-list</b> { <i>standard</i>   <i>extended</i>   <i>named</i> }   <b>sample one-in-every</b> <i>packet-number</i> }  <b>Example:</b> Router(config-rite)# outgoing sample one-in-every 50	(Optional) Configures filtering for outgoing export traffic.  <b>Note</b> If you issue this command, you must also issue the <b>bidirectional</b> 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	<b>exit</b>	Exits RITE configuration mode.

	Command or Action	Purpose
Step 10	<code>interface type number</code>  <b>Example:</b> Router(config)# interface FastEthernet0/0	Configures an interface type and enters interface configuration mode.
Step 11	<code>ip traffic-export apply profile-name</code>  <b>Example:</b> 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	<code>enable</code>  <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	<code>debug ip traffic-export events</code>  <b>Example:</b> Router# debug ip traffic-export events	Enables debugging messages for exported IP traffic packets events.
Step 3	<code>show ip traffic-export [interface <i>interface-name</i>   profile <i>profile-name</i>]</code>  <b>Example:</b> Router# show ip traffic-export	Displays information related to exported IP traffic events. <ul style="list-style-type: none"> <li>• <b>interface <i>interface-name</i></b>—Only data associated with the monitored ingress interface is shown.</li> <li>• <b>profile <i>profile-name</i></b>—Only flow statistics, such as exported packets and the number of bytes, are shown.</li> </ul>

## 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
```

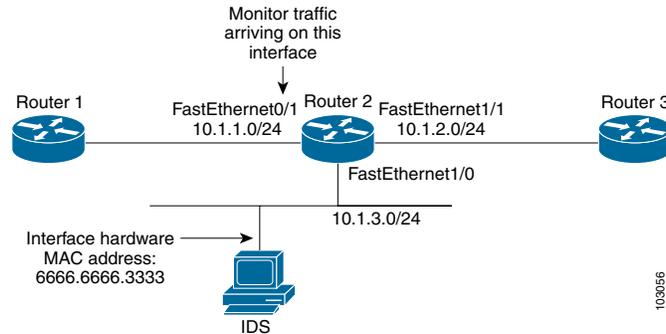
# Configuration Examples for IP Traffic Export

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: <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
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

- **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](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.