



Cisco IOS Security Configuration Guide: Securing User Services

Release 12.2SR

Americas Headquarters

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

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

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

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

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

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

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, 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 Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, 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. (0910R)

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 Software Documentation

Last Updated: October 14, 2009

This document describes the objectives, audience, conventions, and organization used in Cisco IOS software 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 i](#)
- [Documentation Organization, page iii](#)
- [Additional Resources and Documentation Feedback, page xii](#)

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 software 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 contains the following topics:

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

Typographic Conventions

Cisco IOS documentation uses the following typographic conventions:

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

Command Syntax Conventions

Cisco IOS documentation uses the following command syntax conventions:

| Convention | Description |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| bold | Bold text indicates commands and keywords that you enter as shown. |
| <i>italic</i> | Italic text indicates arguments for which you supply values. |
| [x] | Square brackets enclose an optional keyword or argument. |
| ... | 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, that is enclosed within braces or square brackets 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 software uses the following program code conventions:

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

Reader Alert Conventions

Cisco IOS documentation 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. It also lists the configuration guides, command references, and supplementary references and resources that comprise the documentation set. It contains the following topics:

- [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

The Cisco IOS documentation set 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 select severity 3 (moderate) defects in released Cisco IOS software. Review release notes before other documents to learn whether 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 conceptual and task-oriented descriptions of Cisco IOS features.
 - Command references—Compilations of command pages in alphabetical order that provide detailed information about the commands used in the Cisco IOS features and the processes that comprise the related configuration guides. For each technology, there is a single command reference that supports 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 organization of the Cisco IOS documentation set and how to access various document types.

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

New Features List

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

Feature Guides

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

Configuration Guides

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

Command References

Command reference books contain descriptions of Cisco IOS commands that are supported in many different software releases and on many different platforms. The books are organized 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.

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 software configuration guides and command references, including brief descriptions of the contents of the documents. The Cisco IOS command references contain commands for Cisco IOS 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.

[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.

For additional information about configuring and operating specific networking devices, and to access Cisco IOS documentation, go to the Product/Technologies Support area of Cisco.com at the following location:

<http://www.cisco.com/go/techdocs>

Table 1 *Cisco IOS Configuration Guides and Command References*

| Configuration Guide and Command Reference Titles | Features/Protocols/Technologies |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| <ul style="list-style-type: none"> • <i>Cisco IOS AppleTalk Configuration Guide</i> • <i>Cisco IOS AppleTalk Command Reference</i> | AppleTalk protocol. |
| <ul style="list-style-type: none"> • <i>Cisco IOS Asynchronous Transfer Mode Configuration Guide</i> • <i>Cisco IOS Asynchronous Transfer Mode Command Reference</i> | LAN ATM, multiprotocol over ATM (MPoA), and WAN ATM. |

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

| Configuration Guide and Command Reference Titles | Features/Protocols/Technologies |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • <i>Cisco IOS Bridging and IBM Networking Configuration Guide</i> • <i>Cisco IOS Bridging Command Reference</i> • <i>Cisco IOS IBM Networking Command Reference</i> | <p>Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRSM).</p> <p>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.</p> |
| <ul style="list-style-type: none"> • <i>Cisco IOS Broadband Access Aggregation and DSL Configuration Guide</i> • <i>Cisco IOS Broadband Access Aggregation and DSL Command Reference</i> | <p>PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE).</p> |
| <ul style="list-style-type: none"> • <i>Cisco IOS Carrier Ethernet Configuration Guide</i> • <i>Cisco IOS Carrier Ethernet Command Reference</i> | <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 Operation, Administration, and Maintenance (OAM).</p> |
| <ul style="list-style-type: none"> • <i>Cisco IOS Configuration Fundamentals Configuration Guide</i> • <i>Cisco IOS Configuration Fundamentals Command Reference</i> | <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> |
| <ul style="list-style-type: none"> • <i>Cisco IOS DECnet Configuration Guide</i> • <i>Cisco IOS DECnet Command Reference</i> | <p>DECnet protocol.</p> |
| <ul style="list-style-type: none"> • <i>Cisco IOS Dial Technologies Configuration Guide</i> • <i>Cisco IOS Dial Technologies Command Reference</i> | <p>Asynchronous communications, dial backup, dialer technology, dial-in terminal services and AppleTalk remote access (ARA), dial-on-demand routing, dial-out, ISDN, large scale dial-out, modem and resource pooling, Multilink PPP (MLP), PPP, and virtual private dialup network (VPDN).</p> |
| <ul style="list-style-type: none"> • <i>Cisco IOS Flexible NetFlow Configuration Guide</i> • <i>Cisco IOS Flexible NetFlow Command Reference</i> | <p>Flexible NetFlow.</p> |
| <ul style="list-style-type: none"> • <i>Cisco IOS High Availability Configuration Guide</i> • <i>Cisco IOS High Availability Command Reference</i> | <p>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.</p> |
| <ul style="list-style-type: none"> • <i>Cisco IOS Integrated Session Border Controller Command Reference</i> | <p>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).</p> |

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

| Configuration Guide and Command Reference Titles | Features/Protocols/Technologies |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • <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, and session state monitoring. |
| <ul style="list-style-type: none"> • <i>Cisco IOS 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. |
| <ul style="list-style-type: none"> • <i>Cisco IOS IP 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). |
| <ul style="list-style-type: none"> • <i>Cisco IOS 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). |
| <ul style="list-style-type: none"> • <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. |
| <ul style="list-style-type: none"> • <i>Cisco IOS 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). |
| <ul style="list-style-type: none"> • <i>Cisco IOS 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). |
| <ul style="list-style-type: none"> • <i>Cisco IOS IP Routing: BFD Configuration Guide</i> | Bidirectional forwarding detection (BFD). |
| <ul style="list-style-type: none"> • <i>Cisco IOS IP Routing: BGP Configuration Guide</i> • <i>Cisco IOS IP Routing: BGP Command Reference</i> | Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast. |
| <ul style="list-style-type: none"> • <i>Cisco IOS IP Routing: EIGRP Configuration Guide</i> • <i>Cisco IOS IP Routing: EIGRP Command Reference</i> | Enhanced Interior Gateway Routing Protocol (EIGRP). |
| <ul style="list-style-type: none"> • <i>Cisco IOS IP Routing: ISIS Configuration Guide</i> • <i>Cisco IOS IP Routing: ISIS Command Reference</i> | Intermediate System-to-Intermediate System (IS-IS). |
| <ul style="list-style-type: none"> • <i>Cisco IOS IP Routing: ODR Configuration Guide</i> • <i>Cisco IOS IP Routing: ODR Command Reference</i> | On-Demand Routing (ODR). |

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

| Configuration Guide and Command Reference Titles | Features/Protocols/Technologies |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <i>Cisco IOS IP Routing: OSPF Configuration Guide</i> <i>Cisco IOS IP Routing: OSPF Command Reference</i> | Open Shortest Path First (OSPF). |
| <ul style="list-style-type: none"> <i>Cisco IOS IP Routing: Protocol-Independent Configuration Guide</i> <i>Cisco IOS IP Routing: Protocol-Independent Command Reference</i> | IP routing protocol-independent features and commands. Generic policy-based routing (PBR) features and commands are included. |
| <ul style="list-style-type: none"> <i>Cisco IOS IP Routing: RIP Configuration Guide</i> <i>Cisco IOS IP Routing: RIP Command Reference</i> | Routing Information Protocol (RIP). |
| <ul style="list-style-type: none"> <i>Cisco IOS IP SLAs Configuration Guide</i> <i>Cisco IOS IP SLAs Command Reference</i> | Cisco IOS IP Service Level Agreements (IP SLAs). |
| <ul style="list-style-type: none"> <i>Cisco IOS IP Switching Configuration Guide</i> <i>Cisco IOS IP Switching Command Reference</i> | Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS). |
| <ul style="list-style-type: none"> <i>Cisco IOS IPv6 Configuration Guide</i> <i>Cisco IOS IPv6 Command Reference</i> | For IPv6 features, protocols, and technologies, go to the IPv6 “Start Here” document. |
| <ul style="list-style-type: none"> <i>Cisco IOS ISO CLNS Configuration Guide</i> <i>Cisco IOS ISO CLNS Command Reference</i> | ISO Connectionless Network Service (CLNS). |
| <ul style="list-style-type: none"> <i>Cisco IOS 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). |
| <ul style="list-style-type: none"> <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. |
| <ul style="list-style-type: none"> <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. |
| <ul style="list-style-type: none"> <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. |
| <ul style="list-style-type: none"> <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. |
| <ul style="list-style-type: none"> <i>Cisco IOS Multiprotocol Label Switching Configuration Guide</i> <i>Cisco IOS Multiprotocol Label Switching Command Reference</i> | MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS traffic engineering (TE), and MPLS Embedded Management (EM) and MIBs. |

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

| Configuration Guide and Command Reference Titles | Features/Protocols/Technologies |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • <i>Cisco IOS Multi-Topology Routing Configuration Guide</i> • <i>Cisco IOS Multi-Topology Routing Command Reference</i> | Unicast and multicast topology configurations, traffic classification, routing protocol support, and network management support. |
| <ul style="list-style-type: none"> • <i>Cisco IOS NetFlow Configuration Guide</i> • <i>Cisco IOS NetFlow Command Reference</i> | Network traffic data analysis, aggregation caches, and export features. |
| <ul style="list-style-type: none"> • <i>Cisco IOS Network Management Configuration Guide</i> • <i>Cisco IOS Network Management Command Reference</i> | Basic system management; system monitoring and logging; troubleshooting, logging, and fault management; Cisco Discovery Protocol; Cisco IOS Scripting with Tool Control Language (Tcl); Cisco networking services (CNS); DistributedDirector; Embedded Event Manager (EEM); Embedded Resource Manager (ERM); Embedded Syslog Manager (ESM); HTTP; Remote Monitoring (RMON); SNMP; and VPN Device Manager Client for Cisco IOS software (XSM Configuration). |
| <ul style="list-style-type: none"> • <i>Cisco IOS Novell IPX Configuration Guide</i> • <i>Cisco IOS Novell IPX Command Reference</i> | Novell Internetwork Packet Exchange (IPX) protocol. |
| <ul style="list-style-type: none"> • <i>Cisco IOS Optimized Edge Routing Configuration Guide</i> • <i>Cisco IOS Optimized Edge Routing Command Reference</i> | Optimized edge routing (OER) monitoring; Performance Routing (PfR); and automatic route optimization and load distribution for multiple connections between networks. |
| <ul style="list-style-type: none"> • <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> • <i>Cisco IOS Quality of Service Solutions Command Reference</i> | Traffic queueing, traffic policing, traffic shaping, Modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), Multilink PPP (MLP) for QoS, header compression, AutoQoS, Resource Reservation Protocol (RSVP), and weighted random early detection (WRED). |
| <ul style="list-style-type: none"> • <i>Cisco IOS Security Command Reference</i> | Access control lists (ACLs); authentication, authorization, and accounting (AAA); firewalls; IP security and encryption; neighbor router authentication; network access security; network data encryption with router authentication; public key infrastructure (PKI); RADIUS; TACACS+; terminal access security; and traffic filters. |
| <ul style="list-style-type: none"> • <i>Cisco IOS Security Configuration Guide: Securing the Data Plane</i> | Access Control Lists (ACLs); Firewalls: Context-Based Access Control (CBAC) and Zone-Based Firewall; Cisco IOS Intrusion Prevention System (IPS); Flexible Packet Matching; Unicast Reverse Path Forwarding (uRPF); Threat Information Distribution Protocol (TIDP) and TMS. |
| <ul style="list-style-type: none"> • <i>Cisco IOS Security Configuration Guide: Securing the Control Plane</i> | Control Plane Policing, Neighborhood Router Authentication. |
| <ul style="list-style-type: none"> • <i>Cisco IOS Security Configuration Guide: Securing User Services</i> | AAA (includes 802.1x authentication and Network Admission Control [NAC]); Security Server Protocols (RADIUS and TACACS+); Secure Shell (SSH); Secure Access for Networking Devices (includes Autosecure and Role-Based CLI access); Lawful Intercept. |

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

| Configuration Guide and Command Reference Titles | Features/Protocols/Technologies |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i> | Internet Key Exchange (IKE) for IPsec VPNs; IPsec Data Plane features; IPsec Management features; Public Key Infrastructure (PKI); Dynamic Multipoint VPN (DMVPN); Easy VPN; Cisco Group Encrypted Transport VPN (GETVPN); SSL VPN. |
| <ul style="list-style-type: none"> • <i>Cisco IOS Service Advertisement Framework Configuration Guide</i> • <i>Cisco IOS Service Advertisement Framework Command Reference</i> | Cisco Service Advertisement Framework. |
| <ul style="list-style-type: none"> • <i>Cisco IOS Service Selection Gateway Configuration Guide</i> • <i>Cisco IOS Service Selection Gateway Command Reference</i> | Subscriber authentication, service access, and accounting. |
| <ul style="list-style-type: none"> • <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. |
| <ul style="list-style-type: none"> • <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. |
| <ul style="list-style-type: none"> • <i>Cisco IOS Terminal Services Configuration Guide</i> • <i>Cisco IOS Terminal Services Command Reference</i> | DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD). |
| <ul style="list-style-type: none"> • <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). Note For information about virtual switch configuration, see the product-specific software configuration information for the Cisco Catalyst 6500 series switch or for the Metro Ethernet 6500 series switch. |
| <ul style="list-style-type: none"> • <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. |
| <ul style="list-style-type: none"> • <i>Cisco IOS 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. |

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

| Configuration Guide and Command Reference Titles | Features/Protocols/Technologies |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • <i>Cisco IOS Wide-Area Networking Configuration Guide</i> • <i>Cisco IOS Wide-Area Networking Command Reference</i> | Frame Relay; Layer 2 Tunnel Protocol Version 3 (L2TPv3); L2VPN Pseudowire Redundancy; L2VPN Interworking; Layer 2 Local Switching; Link Access Procedure, Balanced (LAPB); and X.25. |
| <ul style="list-style-type: none"> • <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 lists documents and resources that supplement the Cisco IOS software configuration guides and command references.

Table 2 Cisco IOS Supplementary Documents and Resources

| Document Title or Resource | 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, may be informational only, or may help diagnose problems with communications lines, internal hardware, or system software. |
| <i>Cisco IOS Debug Command Reference</i> | Alphabetical list of debug commands including brief descriptions of use, command syntax, and usage guidelines. |
| Release Notes and Caveats | Information about new and changed features, system requirements, and other useful information about specific software releases; information about defects in specific Cisco IOS software releases. |
| MIBs | Files used for network monitoring. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator . |
| RFCs | Standards documents maintained by the Internet Engineering Task Force (IETF) that Cisco IOS documentation references where applicable. The full text of referenced RFCs may be obtained at the following URL: http://www.rfc-editor.org/ |

Additional Resources and Documentation Feedback

What's New in Cisco Product Documentation is released 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, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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 Software

Last Updated: October 14, 2009

This document provides basic information about the command-line interface (CLI) in Cisco IOS 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 xi](#)
- [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 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/Technologies Support area of Cisco.com at <http://www.cisco.com/go/techdocs>.

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 ASR 1000 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 vii](#)
- [Using the Command History Feature, page viii](#)
- [Abbreviating Commands, page ix](#)
- [Using Aliases for CLI Commands, page ix](#)
- [Using the no and default Forms of Commands, page x](#)
- [Using the debug Command, page x](#)
- [Filtering Output Using Output Modifiers, page x](#)
- [Understanding CLI Error Messages, page xi](#)

Understanding Command Modes

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

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

Table 1 CLI Command Modes

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

Table 1 CLI Command Modes (continued)

| Command Mode | Access Method | Prompt | Exit Method | Mode Usage |
|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ROM monitor | From privileged EXEC mode, issue the reload command. Press the Break key during the first 60 seconds while the system is booting. | rommon # > The # symbol represents the line number and increments at each prompt. | Issue the continue command. | <ul style="list-style-type: none"> Run as the default operating mode when a valid image cannot be loaded. Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted. Perform password recovery when a Ctrl-Break sequence is issued within 60 seconds of a power-on or reload event. |
| Diagnostic (available only on Cisco ASR 1000 series routers) | <p>The router boots or enters diagnostic mode in the following scenarios. When a Cisco IOS process or processes fail, in most scenarios the router will reload.</p> <ul style="list-style-type: none"> A user-configured access policy was configured using the transport-map command, which directed the user into diagnostic mode. The router was accessed using an RP auxiliary port. A break signal (Ctrl-C, Ctrl-Shift-6, or the send break command) was entered, and the router was configured to enter diagnostic mode when the break signal was received. | Router (diag) # | <p>If a Cisco IOS process failure is the reason for entering diagnostic mode, the failure must be resolved and the router must be rebooted to exit diagnostic mode.</p> <p>If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or use a method that is configured to connect to the Cisco IOS CLI.</p> <p>If the RP auxiliary port was used to access the router, use another port for access. Accessing the router through the auxiliary port is not useful for customer purposes.</p> | <ul style="list-style-type: none"> Inspect various states on the router, including the Cisco IOS state. Replace or roll back the configuration. Provide methods of restarting the Cisco IOS software or other processes. Reboot hardware (such as the entire router, an RP, an ESP, a SIP, a SPA) or other hardware components. Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP. |

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

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

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

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

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



Note

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

Using the Interactive Help Feature

The CLI includes an interactive Help feature. [Table 2](#) describes the purpose of the CLI interactive Help commands.

Table 2 CLI Interactive Help Commands

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

The following examples show how to use the help commands:

help

```
Router> help
```

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

Two styles of help are provided:

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

?

```
Router# ?
```

```
Exec commands:
```

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

```
<snip>
```

partial command?

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

```
zone zone-pair
```

partial command<Tab>

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

command?

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

| | |
|--------------|------------------------|
| enable | Enable pppoe |
| max-sessions | Maximum PPPOE sessions |

command keyword?

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

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

```
<cr>
```

Understanding Command Syntax

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

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

Table 3 CLI Syntax Conventions

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

The following examples show syntax conventions:

```
Router(config)# ethernet cfm domain ?
WORD domain name
Router(config)# ethernet cfm domain dname ?
level
Router(config)# ethernet cfm domain dname level ?
<0-7> maintenance level number
Router(config)# ethernet cfm domain dname level 7 ?
<cr>

Router(config)# snmp-server file-transfer access-group 10 ?
protocol protocol options
<cr>

Router(config)# logging host ?
Hostname or A.B.C.D IP address of the syslog server
ipv6 Configure IPv6 syslog server
```

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 numeral. 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 numeral for the first character of your password followed by a space, the system will read the number as if it were the numeric keyword and not as part of your password.

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

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

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

Using the Command History Feature

The command history feature saves, in a command history buffer, the commands that you enter during a session. The default number of saved commands 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 command history feature is enabled by default. To disable this feature for a terminal session, issue the **terminal no history** command in user EXEC or privileged EXEC mode or the **no history** command in line configuration mode.

Abbreviating Commands

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

Using Aliases for CLI Commands

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

Table 4 shows the default command aliases.

Table 4 Default Command Aliases

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

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

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

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

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

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_a1.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** form is documented in the command pages of command references. The **default** form is generally documented in the command pages only when the **default** form performs a different function than the plain and **no** forms of the command. To see what **default** commands are available on your system, enter **default ?** in the appropriate command mode.

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 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 **undebg all** command.

For more information about **debug** commands, see the *Cisco IOS Debug Command Reference* at http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html.



Caution

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

Filtering Output Using Output Modifiers

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

The following three output modifiers are available:

- **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 document:

- [Cisco IOS Release 12.4T System Message Guide](#)

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
- Cisco Product/Technology Support
<http://www.cisco.com/go/techdocs>
- 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/cgi-bin/Support/OutputInterpreter/home.pl>

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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: October 14, 2009

The AutoSecure feature uses a single CLI command to 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, and simplify and harden the security configuration on the router.

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 15](#).

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 AutoSecure, page 2](#)
- [Information About AutoSecure, page 2](#)
- [How to Configure AutoSecure, page 6](#)
- [Configuration Examples for AutoSecure, page 9](#)
- [Additional References, page 13](#)
- [Feature Information for AutoSecure, page 15](#)



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](#), page 3
- [Disable Per Interface Services](#), page 4
- [Enable Global Services](#), page 4
- [Secure Access to the Router](#), page 4
- [Log for Security](#), page 5

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

Configuring Additional Security

Perform the following task to enable enhanced security access to your router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **security passwords min-length** *length*
4. **enable password** {*password* | [*encryption-type*] *encrypted-password*}
5. **security authentication failure rate** *threshold-rate* **log**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | enable Example: Router> enable | Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | security passwords min-length length Example: Router(config)# security passwords min-length 6 | Ensures that all configured passwords are at least a specified length. <ul style="list-style-type: none"> <i>length</i>—Minimum length of a configured password. |
| Step 4 | enable password {password [encryption-type] encrypted-password} Example: Router(config)# enable password elephant | Sets a local password to control access to various privilege levels. |
| Step 5 | security authentication failure rate threshold-rate log Example: Router(config)# security authentication failure rate 10 log | Configures the number of allowable unsuccessful login attempts. <ul style="list-style-type: none"> <i>threshold-rate</i>—Number of allowable unsuccessful login attempts. log—Syslog authentication failures if the rate exceeds the threshold. |

Verifying AutoSecure

To verify that the AutoSecure feature is working successfully, perform the following optional steps:

SUMMARY STEPS

1. **enable**
2. **show auto secure config**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Step 1 | enable Example: Router> enable | Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted. |
| Step 2 | show auto secure config Example: 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 the AutoSecure feature.

Related Documents

| Related Topic | Document Title |
|-----------------------------------------------------------------------|---------------------------------------------------------------------------------|
| Login functionality (such as login delays and login blocking periods) | “Cisco IOS Login Enhancements” feature module |
| Additional information regarding router configuration | <i>Cisco IOS Configuration Fundamentals Configuration Guide</i> , Release 12.4T |
| Additional router configuration commands | <i>Cisco IOS Configuration Fundamentals Command Reference Guide</i> |

Standards

| Standards | Title |
|-----------|-------|
| None | — |

MIBs

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

RFCs

| RFCs | Title |
|----------|---------------------------------------------------------------------------------------------------------------|
| RFC 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> | <p>http://www.cisco.com/public/support/tac/home.shtml</p> |

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 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 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>The AutoSecure feature uses a single CLI command to 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, and simplify and harden the security configuration on the router.</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>The following commands were introduced or modified: auto secure, security passwords min-length, show auto secure config.</p> |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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.



Authentication, Authorization, and Accounting (AAA)



Authentication



Configuring Authentication

First Published: October 26, 1998

Last Updated: October 14, 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 53](#).

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

- [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.
- If you configure one RADIUS server with the nonstandard option and another RADIUS server without the nonstandard option, the RADIUS-server host with the nonstandard option does not accept a predefined host. If you configure the same RADIUS server host IP address for a different UDP destination port for accounting requests using the `acct-port` keyword and a UDP destination port for authentication requests using the `auth-port` keyword with and without the nonstandard option, the RADIUS server does not accept the nonstandard option.

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:

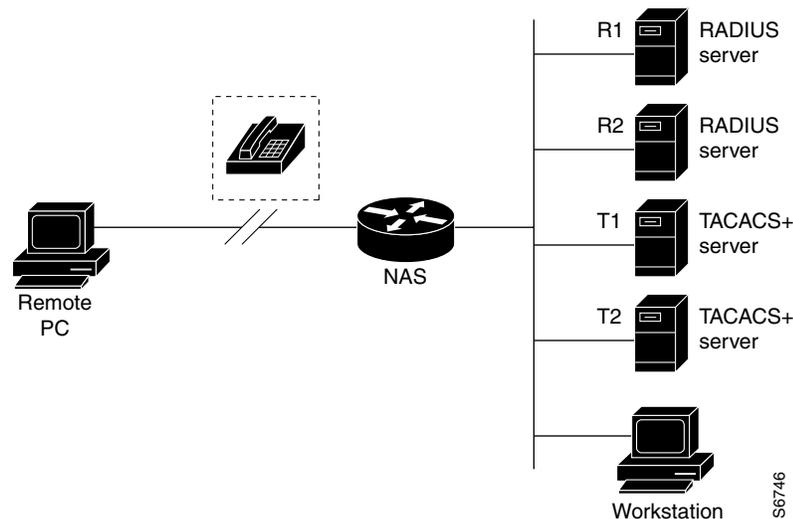
- [Method Lists and Server Groups](#)

- [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)# aaa new-model | Enables AAA globally. |
| Step 2 | Router(config)# aaa authentication login {default list-name} method1 [method2...] | Creates a local authentication list. |
| Step 3 | Router(config)# line [aux console tty vty] line-number [ending-line-number] | Enters line configuration mode for the lines to which you want to apply the authentication list. |
| Step 4 | Router(config-line)# login authentication {default list-name} | Applies the authentication list to a line or set of lines. |

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

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

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



Note

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

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

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

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

Table 4 lists the supported login authentication methods.

Table 4 AAA Authentication Login Methods

| Keyword | Description |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| enable | Uses the enable password for authentication. |
| krb5 | Uses Kerberos 5 for authentication. |
| krb5-telnet | Uses Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router. If selected, this keyword must be listed as the first method in the method list. |

Table 4 AAA Authentication Login Methods (continued)

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

**Note**

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

This section includes the following sections:

- [Preventing an Access Request with an Expired Username from Being Sent to the RADIUS Server](#)
- [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](#)

Preventing an Access Request with an Expired Username from Being Sent to the RADIUS Server

The following task is used to prevent an access request with an expired username from being sent to the RADIUS server. The Easy VPN client is notified by the RADIUS server that its password has expired. The password-expiry feature also provides a generic way for the user to change the password.

**Note**

The **radius-server vsa send authentication** command must be configured to make the password-expiry feature work.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login {default | list-name} passwd-expiry method1 [method2...]**

5. radius-server vsa send authentication

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code> Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted. |
| Step 2 | <code>configure terminal</code> Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | <code>aaa new-model</code> Example: Router(config)# aaa new-model | Enables AAA. |
| Step 4 | <code>aaa authentication login {default list-name} passwd-expiry method1 [method2...]</code> Example: Router(config)# aaa authentication login userauthen passwd-expiry group radius | The default keyword uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in. The <i>list-name</i> argument is a character string used to name the list of authentication methods activated when a user logs in. The password-expiry keyword enables password aging on a local authentication list. The <i>method</i> argument identifies the list of methods that the authentication algorithm tries in the given sequence. You must enter at least one method; you may enter up to four methods. The example configures password aging by using AAA with a crypto client. |
| Step 5 | <code>radius-server vsa send authentication</code> Example: Router(config)# radius-server vsa send authentication | Sends vendor-specific attributes in access requests |

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 29 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 31 in this chapter.

Login Authentication Using Group RADIUS

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

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

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

Configuring RADIUS Attribute 8 in Access Requests

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

Login Authentication Using Group TACACS+

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

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

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

Login Authentication Using group group-name

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

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

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

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

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

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

Configuring PPP Authentication Using AAA

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

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

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

| | Command | Purpose |
|--------|------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# aaa new-model | Enables AAA globally. |
| Step 2 | Router(config)# aaa authentication ppp {default list-name} method1 [method2...] | Creates a local authentication list. |
| Step 3 | Router(config)# interface interface-type interface-number | Enters interface configuration mode for the interface to which you want to apply the authentication list. |
| Step 4 | Router(config-if)# ppp authentication {protocol1 [protocol2...]} [if-needed] {default list-name} [callin] [one-time] [optional] | Applies the authentication list to a line or set of lines. In this command, <i>protocol1</i> and <i>protocol2</i> represent the following protocols: CHAP, MS-CHAP, and PAP. PPP authentication is attempted first using the first authentication method, specified by <i>protocol1</i> . If <i>protocol1</i> is unable to establish authentication, the next configured protocol is used to negotiate authentication. |

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

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

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

```
aaa authentication ppp default local
```

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

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

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



Note

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

Table 5 lists the supported login authentication methods.

Table 5 AAA Authentication PPP Methods

| Keyword | Description |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| if-needed | Does not authenticate if user has already been authenticated on a TTY line. |
| krb5 | Uses Kerberos 5 for authentication (can only be used for PAP authentication). |
| local | Uses the local username database for authentication. |
| local-case | Uses case-sensitive local username authentication. |
| none | Uses no authentication. |
| group radius | Uses the list of all RADIUS servers for authentication. |
| group tacacs+ | Uses the list of all TACACS+ servers for authentication. |
| group <i>group-name</i> | Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the aaa group server radius or aaa group server tacacs+ command. |

This section includes the following sections:

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

PPP Authentication Using Kerberos

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

```
aaa authentication ppp default krb5
```

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



Note

Kerberos login authentication works only with PPP PAP authentication.

PPP Authentication Using Local Password

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

```
aaa authentication ppp default local
```

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

PPP Authentication Using Group RADIUS

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

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

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

Configuring RADIUS Attribute 44 in Access Requests

Once you have used the **aaa authentication ppp** command with the **group radius method** to specify RADIUS as the login authentication method, you can configure your router to send attribute 44 (Acct-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)# aaa processes <i>number</i> | Allocates a specific number of background processes to handle AAA authentication and authorization requests for PPP. |

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



Note

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

Configuring ARAP Authentication Using AAA

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

Use the following commands starting in global configuration mode:

| | Command | Purpose |
|--------|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| Step 1 | Router(config)# aaa new-model | Enables AAA globally. |
| Step 2 | Router(config)# aaa authentication arap { default <i>list-name</i> } <i>method1</i> [<i>method2...</i>] | Enables authentication for ARAP users. |
| Step 3 | Router(config)# line <i>number</i> | (Optional) Changes to line configuration mode. |
| Step 4 | Router(config-line)# autoselect arap | (Optional) Enables autoselection of ARAP. |

| | Command | Purpose |
|--------|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | Router(config-line)# autoselect during-login | (Optional) Starts the ARAP session automatically at user login. |
| Step 6 | Router(config-line)# arap authentication list-name | (Optional—not needed if default is used in the aaa authentication arap command) Enables TACACS+ authentication for ARAP on a line. |

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

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

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

**Note**

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

Table 6 lists the supported login authentication methods.

Table 6 AAA Authentication ARAP Methods

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

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

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

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

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

This section includes the following sections:

- [ARAP Authentication Allowing Authorized Guest Logins](#)
- [ARAP Authentication Allowing Guest Logins](#)
- [ARAP Authentication Using Line Password](#)

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

ARAP Authentication Allowing Authorized Guest Logins

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

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

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



Note

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

ARAP Authentication Allowing Guest Logins

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

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

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

ARAP Authentication Using Line Password

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

```
aaa authentication arap default line
```

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

ARAP Authentication Using Local Password

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

```
aaa authentication arap default local
```

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

ARAP Authentication Using Group RADIUS

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

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

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

ARAP Authentication Using Group TACACS+

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

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

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

ARAP Authentication Using Group group-name

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

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

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

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

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

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

Configuring NASI Authentication Using AAA

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

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

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

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

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

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



Note

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

Table 7 lists the supported NASI authentication methods.

Table 7 AAA Authentication NASI Methods

| Keyword | Description |
|-------------------|------------------------------------------------------|
| enable | Uses the enable password for authentication. |
| line | Uses the line password for authentication. |
| local | Uses the local username database for authentication. |
| local-case | Uses case-sensitive local username authentication. |

Table 7 AAA Authentication NASI Methods (continued)

| Keyword | Description |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| none | Uses no authentication. |
| group radius | Uses the list of all RADIUS servers for authentication. |
| group tacacs+ | Uses the list of all TACACS+ servers for authentication. |
| group <i>group-name</i> | Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the aaa group server radius or aaa group server tacacs+ command. |

This section includes the following sections:

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

NASI Authentication Using Enable Password

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

```
aaa authentication nasi default enable
```

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

NASI Authentication Using Line Password

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

```
aaa authentication nasi default line
```

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

NASI Authentication Using Local Password

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

```
aaa authentication nasi default local
```

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

NASI Authentication Using Group RADIUS

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

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

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

NASI Authentication Using Group TACACS+

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

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

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

NASI Authentication Using group group-name

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

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

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

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

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

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

Specifying the Amount of Time for Login Input

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

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

Enabling Password Protection at the Privileged Level

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

Use the following command in global configuration mode:

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

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

Table 8 AAA Authentication Enable Default Methods

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

Changing the Text Displayed at the Password Prompt

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

```
Password:
```

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

The **aaa authentication password-prompt** command works when RADIUS is used as the login method. You will be able to see the password prompt defined in the command shown even when the RADIUS server is unreachable. The **aaa authentication password-prompt** command does not work with TACACS+. TACACS+ supplies the NAS with the password prompt to display to the users. If the TACACS+ server is reachable, the NAS gets the password prompt from the server and uses that prompt instead of the one defined in the **aaa authentication password-prompt** command. If the TACACS+ server is not reachable, the password prompt defined in the **aaa authentication password-prompt** command may be used.

Use the following command in global configuration mode:

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

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 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | aaa new-model Example: Router(config)# configure terminal | Enables AAA globally. |
| Step 4 | aaa authentication suppress null-username Example: 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)# aaa new-model | Enables AAA. |
| Step 2 | Router(config)# aaa authentication banner <i>delimiter string delimiter</i> | Creates a personalized login banner. |

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

Configuring a Failed-Login Banner

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

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

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

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

Configuring AAA Packet of Disconnect

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

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

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

Enabling Double Authentication

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

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

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

This section includes the following subsections:

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

How Double Authentication Works

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

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



Note

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

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

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



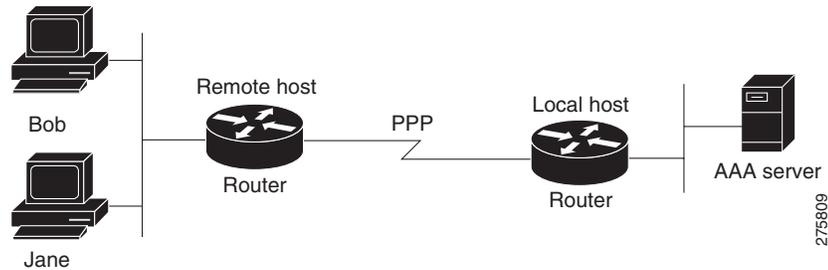
Caution

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

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

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

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



Configuring Double Authentication

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

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



Note

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

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

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

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

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

Accessing the User Profile After Double Authentication

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

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

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

| Command | Purpose |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| <code>Router> access-profile [merge replace] [ignore-sanity-checks]</code> | 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*.

**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 show ip trigger-authentication command.) |
| Step 3 | <code>Router# debug ip trigger-authentication</code> | Displays debug output related to automated double authentication. |

Non-AAA Authentication Methods

This section discusses the following non-AAA authentication tasks:

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

Configuring Line Password Protection

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

| | Command or Action | Purpose |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | line [aux console tty vty] line-number [ending-line-number] Example: Router(config)# line console 0 | Enters line configuration mode. |
| Step 4 | password password Example: 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. |
| Step 5 | login Example: Router(config-line)# login | Enables password checking at login. You can disable line password verification by disabling password checking by using the no version of this command. Note The login command only changes username and privilege level but it does not execute a shell; therefore autocommands will not be executed. To execute autocommands under this circumstance, you need to establish a Telnet session back into the router (loop-back). Make sure that the router has been configured for secure Telnet sessions if you choose to implement autocommands this way. |

Establishing Username Authentication

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

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

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

| | Command | Purpose |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <pre>Router(config)# username name [nopassword password password password encryption-type encrypted password] or Router(config)# username name [access-class number]</pre> | Establishes username authentication with encrypted passwords. or (Optional) Establishes username authentication by access list. |
| Step 2 | <pre>Router(config)# username name [privilege level]</pre> | (Optional) Sets the privilege level for the user. |
| Step 3 | <pre>Router(config)# username name [autocommand command]</pre> | (Optional) Specifies a command to be executed automatically. |
| Step 4 | <pre>Router(config)# username name [noescape] [nohangup]</pre> | (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 {<i>protocol1</i> [<i>protocol2</i>...]} [<i>if-needed</i>] [<i>default</i> <i>list-name</i>] [<i>callin</i>] [<i>one-time</i>]</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 username password password</code> | Enables outbound PAP authentication. |

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

Refusing PAP Authentication Requests

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

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

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

Creating a Common CHAP Password

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

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

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

Refusing CHAP Authentication Requests

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

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

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

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

Delaying CHAP Authentication Until Peer Authenticates

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

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

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

Using MS-CHAP

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

MS-CHAP differs from the standard CHAP as follows:

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

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

Table 9 Vendor-Specific RADIUS Attributes for MS-CHAP

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

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

| | Command | Purpose |
|--------|------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| Step 1 | <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, page 37](#)
- [TACACS+ Authentication Examples, page 39](#)
- [Kerberos Authentication Examples, page 39](#)
- [AAA Scalability Example, page 40](#)
- [Login and Failed Banner Examples, page 41](#)
- [AAA Packet of Disconnect Server Key Example, page 41](#)
- [Double Authentication Examples, page 42](#)
- [Automated Double Authentication Example, page 47](#)
- [MS-CHAP Example, page 49](#)

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"

```

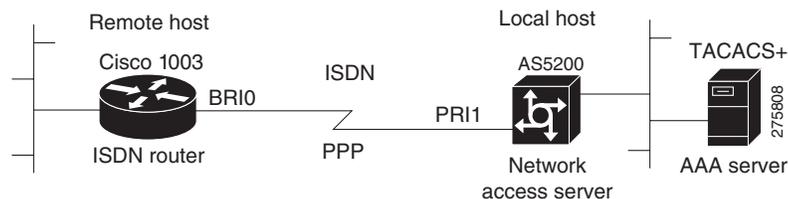
Complete Configuration with TACACS+ Example

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 | “ Configuring Authorization ” module. |
| Accounting | “ Configuring Accounting ” module. |

Standards

| Standard | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | — |

MIBs

| MIB | MIBs Link |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

RFCs

| RFC | Title |
|----------|----------------------------------------------------------|
| RFC 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>http://www.cisco.com/techsupport</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 XE 2.1 | This feature was introduced in the Cisco IOS Release 12.0 software. This feature was introduced in the Cisco IOS Release XE 2.1 software. |
| AAA Per-User Scalability | 12.2(27)SB 12.2(33)SR 15.0(1)M | This feature was introduced in Cisco IOS Release 12.2(27)SB. This feature was integrated into Cisco IOS Release 12.2(33)SR. This feature was integrated into Cisco IOS Release 15.0(1)M. |
| RADIUS - CLI to Prevent Sending of Access Request with a Blank Username | 12.2(33)SRD Cisco IOS XE Release 2.4 | 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. The following section provides information about this feature: <ul style="list-style-type: none"> • Preventing an Access Request with a Blank Username from Being Sent to the RADIUS Server, page 22 The following command was introduced: aaa authentication suppress null-username . |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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.



Login Password Retry Lockout

First Published: March 24, 2005
Last Updated: November 20, 2009

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.

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 Login Password Retry Lockout” 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 Login Password Retry Lockout, page 2](#)
- [Restrictions for Login Password Retry Lockout, page 2](#)
- [Information About Login Password Retry Lockout, page 2](#)
- [How to Configure Login Password Retry Lockout, page 3](#)
- [Configuration Examples for Login Password Retry Lockout, page 6](#)
- [Additional References, page 8](#)
- [Feature Information for Login Password Retry Lockout, page 9](#)
- [Glossary, page 10](#)



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

Prerequisites for Login Password Retry Lockout

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

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:

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

Lock Out of 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. A user that can change to the root privilege (level 15) 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 \(optional\)](#)
- [Unlocking a Login Locked-Out User, page 4 \(optional\)](#)
- [Clearing the Unsuccessful Login Attempts of a User, page 5 \(optional\)](#)
- [Monitoring and Maintaining Login Password Retry Lockout Status, page 5 \(optional\)](#)

Configuring Login Password Retry Lockout

To configure the Login Password Retry Lockout feature, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **username** *name* [**privilege level**] **password** *encryption-type password*
4. **aaa new-model**
5. **aaa local authentication attempts max-fail** *number-of-unsuccessful-attempts*
6. **aaa authentication login default** *method*

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | username name [privilege level] password encryption-type password Example: Router(config)# username user1 privilege 15 password 0 cisco | Establishes a username-based authentication system. |
| Step 4 | aaa new-model Example: Router(config)# aaa new-model | Enables the AAA access control model. |
| Step 5 | aaa local authentication attempts max-fail number-of-unsuccessful-attempts Example: Router(config)# aaa local authentication attempts max-fail 3 | Specifies the maximum number of unsuccessful attempts before a user is locked out. |
| Step 6 | aaa authentication login default method Example: Router(config)# aaa authentication login default local | Sets the authentication, authorization, and accounting (AAA) authentication method at login. For example, aaa authentication login default local specifies the local AAA user database. |

Unlocking a Login Locked-Out User

To unlock a login locked-out user, perform the following steps.

**Note**

This task can be performed only by users having the root privilege (level 15).

SUMMARY STEPS

1. enable
2. clear aaa local user logout {username username | all}

DETAILED STEPS

| | Command or Action | Purpose |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <pre>enable</pre> <p>Example: Router> enable </p> | Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted. |
| Step 2 | <pre>clear aaa local user lockout {username username all}</pre> <p>Example: Router# clear aaa local user lockout username user1 </p> | Unlocks a locked-out user. |

Clearing the Unsuccessful Login Attempts of a User

This task is useful for cases in which the user configuration was changed and the unsuccessful login attempts of a user that are already logged must be cleared.

To clear the unsuccessful login attempts of a user that have already been logged, perform the following steps.

SUMMARY STEPS

- enable
- clear aaa local user fail-attempts {username *username* | all}

DETAILED STEPS

| | Command or Action | Purpose |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <pre>enable</pre> <p>Example: Router> enable </p> | Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted. |
| Step 2 | <pre>clear aaa local user fail-attempts {username username all}</pre> <p>Example: Router# clear aaa local user fail-attempts username user1 </p> | Clears the unsuccessful attempts of the user. <ul style="list-style-type: none"> This command is useful for cases in which the user configuration was changed and the unsuccessful attempts that are already logged must be cleared. |

Monitoring and Maintaining Login Password Retry Lockout Status

To monitor and maintain the status of the Login Password Retry Lockout configuration, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show aaa local user logout**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | show aaa local user logout Example: Router# show aaa local user logout | Displays a list of the locked-out users for the current login password retry lockout configuration. |

Examples

The following output shows that user1 is locked out:

```
Router# show aaa local user logout

                Local-user           Lock time
                user1                 04:28:49 UTC Sat Jun 19 2004
```

Configuration Examples for Login Password Retry Lockout

This section provides the following configuration examples:

- [Displaying the Login Password Retry Lockout Configuration: Example, page 6](#)

Displaying the Login Password Retry Lockout Configuration: Example

The following **show running-config** command output illustrates that the maximum number of failed user attempts has been set for 2 as the login password retry lockout configuration:

```
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
```

Additional References

The following sections provide references related to Login Password Retry Lockout.

Related Documents

| Related Topic | Document Title |
|-----------------------------|------------------------------------------------------|
| Cisco IOS security commands | Cisco IOS Security Command Reference |

Standards

| Standards | Title |
|-----------|-------|
| None | — |

MIBs

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

RFCs

| RFCs | Title |
|------|-------|
| None | — |

Technical Assistance

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

Feature Information for Login Password Retry Lockout

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 Login Password Retry Lockout

| Feature Name | Releases | Feature Information |
|------------------------------|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Login Password Retry Lockout | 12.3(14)T 12.2(33)SRE | <p>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.</p> <p>This feature was introduced in Cisco IOS Release 12.3(14)T.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRE.</p> <p>The following commands were introduced or modified: aaa local authentication attempts max-fail, clear aaa local user fail-attempts, clear aaa local user lockout.</p> |

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, 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 Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, 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. (0910R)

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.



Throttling of AAA (RADIUS) Records

First Published: December 3, 2007

Last Updated: October 9, 2009

The Throttling of AAA (RADIUS) Records feature supports throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server. This feature allows a user to configure the appropriate throttling rate to avoid network congestion and instability; such as when there is insufficient bandwidth to accommodate a sudden burst of records generated from the Cisco IOS router to the RADIUS server.

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 Throttling of AAA \(RADIUS\) Records”](#) 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

- [Information About Throttling of AAA \(RADIUS\) Records, page 2](#)
- [How to Configure Throttling of AAA \(RADIUS\) Records, page 3](#)
- [Configuration Examples for Throttling of AAA \(RADIUS\) Records, page 5](#)
- [Additional References, page 7](#)
- [Feature Information for Throttling of AAA \(RADIUS\) Records, page 9](#)



Americas Headquarters:

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

Information About Throttling of AAA (RADIUS) Records

To configure the Throttling of AAA (RADIUS) Records feature, you should understand the following concepts:

- [Benefits of the Throttling of AAA \(RADIUS\) Records Feature, page 2](#)
- [Throttling Access Requests and Accounting Records, page 2](#)

Benefits of the Throttling of AAA (RADIUS) Records Feature

A Network Access Server (NAS), acting as RADIUS client, can generate a burst of accounting or access requests, causing severe network congestion or causing the RADIUS server to become overloaded with a burst of RADIUS traffic. This problem could be compounded when multiple NASs interact with the RADIUS servers.

The following conditions can trigger a sudden burst of RADIUS traffic:

- An interface flap, which in turn brings down all the subscriber sessions and generates accounting requests for each subscriber.
- The Cisco IOS High Availability (HA) program generating a START record for every session that survived a switchover, such as the scenario described the preceding bullet.

A large number of generated requests can make the network unstable if there is insufficient bandwidth or if the RADIUS server is slow to respond. Neither the User Datagram Protocol (UDP) transport layer nor the RADIUS protocol has a flow control mechanism. The throttling mechanism provided by this feature provides a solution for these issues.

Throttling Access Requests and Accounting Records

The Throttling of AAA (RADIUS) Records feature introduces a mechanism to control packets (flow control) at the NAS level, which improves the RADIUS server performance.

Because of their specific uses, access requests and accounting records must be treated separately. Access request packets are time sensitive, while accounting record packets are not.

- If a response to an access request is not returned to the client in a timely manner, the protocol or the user will time out, impacting the device transmission rates.
- Accounting records packets are not real-time critical.

When configuring threshold values on the same server, it is important to prioritize threshold values for the handling of the time-sensitive access request packets and to place a lesser threshold value on the accounting records packets.

In some cases, when an Internet Service Provider (ISP) is using separate RADIUS servers for access requests and accounting records, only accounting records throttling may be required.

Summary

- The Throttling of AAA (RADIUS) Records is disabled, by default.
- Throttling functionality can be configured globally or at server group level.

How to Configure Throttling of AAA (RADIUS) Records

This section describes how to configure throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server for both, global and server groups.

Server-group configurations are used to enable or disable throttling for a particular server group and to specify the threshold value for that server group.



Note

Server-group configurations override any configured global configurations.

This section includes the following tasks.

- [Throttling Accounting and Access Request Packets Globally, page 3](#)
- [Throttling Accounting and Access Request Packets Per Server Group, page 4](#)

Throttling Accounting and Access Request Packets Globally

To globally configure the throttling of accounting and access request packets, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server throttle** {[*accounting threshold*] [*access threshold*] [*access-timeout number-of-timeouts*]}
4. **exit**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |

| | Command or Action | Purpose |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <p>radius-server throttle {[<i>accounting threshold</i>] [<i>access threshold</i>] [<i>access-timeout number-of-timeouts</i>]}</p> <p>Example: Router(config)# radius-server throttle accounting 100 access 200 access-timeout 2</p> | <p>Configures global throttling for accounting and access request packets.</p> <p>For this example:</p> <ul style="list-style-type: none"> The accounting threshold value (the range is 0-65536) is set to 100, and the access threshold value is set to 200. <p>Note The default threshold value is 0 (throttling disabled).</p> <ul style="list-style-type: none"> The number of timeouts per transaction value (the range is 1-10) is set to 2. |
| Step 4 | <p>exit</p> <p>Example: Router(config)# exit</p> | Exits global configuration mode. |

Throttling Accounting and Access Request Packets Per Server Group

The following server-group configuration can be used to enable or disable throttling for a specified server group and to specify the threshold value for that server group.

To configure throttling of server-group accounting and access request packets, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *server-group-name*
4. **throttle** {[*accounting threshold*] [*access threshold*] [*access-timeout number-of-timeouts*]}
5. **exit**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p>enable</p> <p>Example: Router> enable</p> | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted. |
| Step 2 | <p>configure terminal</p> <p>Example: Router# configure terminal</p> | Enters global configuration mode. |

| | Command or Action | Purpose |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <pre>aaa group server radius server-group-name</pre> <p>Example: Router(config)# aaa group server radius myservergroup</p> | Enters server-group configuration mode. |
| Step 4 | <pre>throttle {[accounting threshold] [access threshold [access-timeout number-of-timeouts]]}</pre> <p>Example: Router(config-sg-radius)# throttle accounting 100 access 200 access-timeout 2</p> | <p>Configures the specified server-group throttling values for accounting and access request packets.</p> <p>For this example:</p> <ul style="list-style-type: none"> The accounting threshold value (the range is 0-65536) is set to 100, and the access threshold value is set to 200. <p>Note The default threshold value is 0 (throttling disabled).</p> <ul style="list-style-type: none"> The number of time-outs per transaction value (the range is 1-10) is set to 2. |
| Step 5 | <pre>exit</pre> <p>Example: Router(config-sg-radius)# exit</p> | Exits server-group configuration mode. |

Configuration Examples for Throttling of AAA (RADIUS) Records

This section provides the following configuration examples:

- [Throttling Accounting and Access Request Packets Globally: Example, page 5](#)
- [Throttling Accounting and Access Request Packets Per Server Group: Example, page 6](#)

Throttling Accounting and Access Request Packets Globally: Example

The following example shows how to limit the number of accounting requests sent to a server to 100:

```
enable
configure terminal
radius-server throttle accounting 100
```

The following example shows how to limit the number of access requests packets sent to a server to 200 and sets the number of time-outs allowed per transactions to 2:

```
enable
configure terminal
radius-server throttle access 200
radius-server throttle access 200 access-timeout 2
```

The following example shows how to throttle both accounting and access request packets:

```
enable
configure terminal
radius-server throttle accounting 100 access 200
```

Throttling Accounting and Access Request Packets Per Server Group: Example

The following example shows how to limit the number of accounting requests sent to server-group-A to 100:

```
enable
configure terminal
aaa group server radius server-group-A
throttle accounting 100
```

The following example shows how to limit the number of access requests packets sent to server-group-A to 200 and sets the number of time-outs allowed per transactions to 2:

```
enable
configure terminal
aaa group server radius server-group-A
throttle access 200 access-timeout 2
```

The following example shows how to throttle both accounting and access request packets for server-group-A:

```
enable
configure terminal
aaa group server radius server-group-A
throttle accounting 100 access 200
```

Additional References

The following sections provide references related to the Throttling of AAA (RADIUS) Records feature.

Related Documents

| Related Topic | Document Title |
|----------------|---------------------------------------------------------------------------------------|
| AAA and RADIUS | <i>Cisco IOS Security Configuration Guide: Securing User Services</i> , Release 15.0. |

Standards

| Standard | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | — |

MIBs

| MIB | MIBs Link |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

RFCs

| RFC | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | — |

Technical Assistance

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

Feature Information for Throttling of AAA (RADIUS) Records

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 Throttling of AAA (RADIUS) Records

| Feature Name | Releases | Feature Information |
|------------------------------------|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Throttling of AAA (RADIUS) Records | 12.2(33)SRC 12.4(20)T Cisco IOS XE Release 2.1 | <p>The Throttling of AAA (RADIUS) Records feature supports throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server. This feature allows a user to configure the appropriate throttling rate to avoid network congestion and instability; such as when there is insufficient bandwidth to accommodate a sudden burst of records generated from the Cisco IOS router to the RADIUS server.</p> <p>In Release 12.2(33)SRC, this feature was introduced on the Cisco 7200 and Cisco 7200 routers.</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: radius-server throttle, throttle</p> |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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

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



AAA Authorization and Authentication Cache

First Published: March 16, 2006

Last Updated: October 02, 2009

The AAA Authorization and Authentication Cache feature allows you to cache authorization and authentication responses for a configured set of users or service profiles, providing performance improvements and an additional level of network reliability because user and service profiles that are returned from authorization and authentication responses can be queried from multiple sources and need not depend solely on an offload server. This feature also provides a failover mechanism so that if a network RADIUS or TACACS+ server is unable to provide authorization and authentication responses network users and administrators can still access the network.

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 Implementing Authorization and Authentication Profile Caching”](#) section on page 13.

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 Implementing Authorization and Authentication Profile Caching](#), page 2
- [Information About Implementing Authorization and Authentication Profile Caching](#), page 2
- [How to Implement Authorization and Authentication Profile Caching](#), page 4
- [Configuration Examples for Implementing Authorization and Authentication Profile Caching](#), page 10
- [Additional References](#), page 11



Americas Headquarters:

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

- [Feature Information for Implementing Authorization and Authentication Profile Caching, page 13](#)

Prerequisites for Implementing Authorization and Authentication Profile Caching

The following prerequisites apply to implementing authorization and authentication profile caching:

- Understand how you would want to implement profile caching, that is, are profiles being cached to improve network performance or as a failover mechanism if your network authentication and authorization (RADIUS and TACACS+) servers become unavailable.
- RADIUS and TACACS+ server groups must already be configured.

Information About Implementing Authorization and Authentication Profile Caching

To implement authorization and authentication profile caching, you should understand the following concepts:

- [Network Performance Optimization Using Authorization and Authentication Profile Caching, page 2](#)
- [Authorization and Authentication Profile Caching as a Failover Mechanism, page 3](#)
- [Method Lists in Authorization and Authentication Profile Caching, page 3](#)
- [Authorization and Authentication Profile Caching Guidelines, page 3](#)
- [General Configuration Procedure for Implementing Authorization and Authentication Profile Caching, page 4](#)

Network Performance Optimization Using Authorization and Authentication Profile Caching

RADIUS and TACACS+ clients run on Cisco routers and send authentication requests to a central RADIUS or TACACS+ server that contains all user authentication and network service access information. The router is required to communicate with an offload RADIUS or TACACS+ server to authenticate a given call and then apply a policy or service to that call. Unlike authentication, authorization, and accounting (AAA) accounting, AAA authentication and authorization is a blocking procedure, which means the call setup may not proceed while the call is being authenticated and authorized. Thus, the time required to process the call setup is directly impacted by the time required to process such an authentication or authorization request from the router to the offload RADIUS or TACACS+ server, and back again. Any communication problems in the transmission, offload server utilization, and numerous other factors cause significant degradation in a router's call setup performance due simply to the AAA authentication and authorization step. The problem is further highlighted when multiple AAA authentications and authorizations are needed for a single call or session.

A solution to this problem is to minimize the impact of such authentication requests by caching the authentication and authorization responses for given users on the router, thereby removing the need to send the requests to an offload server again and again. This profile caching adds significant performance

improvements to call setup times. Profile caching also provides an additional level of network reliability because user and service profiles that are returned from authentication and authorization responses can be queried from multiple sources and need not depend solely on an offload server.

To take advantage of this performance optimization, you need to configure the authentication method list so that the AAA cache profile is queried first when a user attempts to authenticate to the router. See the [“Method Lists in Authorization and Authentication Profile Caching”](#) section for more information.

Authorization and Authentication Profile Caching as a Failover Mechanism

If, for whatever reason, RADIUS or TACACS+ servers are unable to provide authentication and authorization responses, network users and administrators can be locked out of the network. The profile caching feature allows usernames to be authorized without having to complete the authentication phase. For example, a user by the name of user100@example.com with a password secretpassword1 could be stored in a profile cache using the regular expression “.*@example.com”. Another user by the name of user101@example.com with a password of secretpassword2 could also be stored using the same regular expression, and so on. Because the number of users in the “.*@example.com” profile could number in the thousands, it is not feasible to authenticate each user with their personal password. Therefore authentication is disabled and each user simply accesses authorization profiles from a common Access Response stored in cache.

The same reasoning applies in cases where higher end security mechanisms such as Challenge Handshake Authentication Protocol (CHAP), Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), or Extensible Authentication Protocol (EAP), which all use an encrypted password between the client and AAA offload server. To allow these unique, secure username and password profiles to retrieve their authorization profiles, authentication is bypassed.

To take advantage of this failover capability, you need to configure the authentication and authorization method list so that the cache server group is queried last when a user attempts to authenticate to the router. See the [“Method Lists in Authorization and Authentication Profile Caching”](#) section for more information.

Method Lists in Authorization and Authentication Profile Caching

A method list is a sequential list describing the authentication methods to be queried in order to authenticate a user. We support methods such as local (use the local Cisco IOS database), none (do nothing), RADIUS server group, or TACACS+ server group. Typically, more than one method can be configured into a method list. 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 until all methods defined in the method list are exhausted.

To optimize network performance or provide failover capability using the profile caching feature you simply change the order of the authentication and authorization methods in the method list. To optimize network performance, make sure the cache server group appears first in the method list. For failover capability, the cache server group should appear last in the method list.

Authorization and Authentication Profile Caching Guidelines

Because the number of usernames and profiles that can request to be authenticated or authorized at a given router on a given point of presence (POP) can be quite extensive, it would not be feasible to cache all of them. Therefore, only usernames and profiles that are commonly used or that share a common

authentication and authorization response should be configured to use caching. Commonly used usernames such as aolip and aolnet, which are used for America Online (AOL) calls, or preauthentication dialed number identification service (DNIS) numbers used to connect Public Switched Telephone Network (PSTN) calls to a network attached storage device, along with domain-based service profiles, are all examples of usernames and profiles that can benefit from authentication and authorization caching.

General Configuration Procedure for Implementing Authorization and Authentication Profile Caching

To implement authorization and authentication profile caching, you would complete the following procedure:

1. Create cache profile groups and define the rules for what information is cached in each group. Entries that match based on exact username, regular expressions, or specify that all authentication and authorization requests can be cached.
2. Update existing server groups to reference newly defined cache groups.
3. Update authentication or authorization method lists to use the cached information to optimize network performance or provide a failover mechanism.

How to Implement Authorization and Authentication Profile Caching

This section contains the following tasks:

- [Creating Cache Profile Groups and Defining Caching Rules, page 4](#) (required)
- [Defining RADIUS and TACACS+ Server Groups That Use Cache Profile Group Information, page 7](#) (required)
- [Updating Authorization and Authentication Method Lists to Specify How Cache Information is Used, page 8](#) (required)

Creating Cache Profile Groups and Defining Caching Rules

Perform this task to create a cache profile group, define the rules for what information is cached in that group, and verify and manage cache profile entries.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa cache profile** *group-name*
5. **profile** *name* [**no-auth**]
6. Repeat Step 5 for each username you want to add to the profile group in Step 4.

7. **regexp** *matchexpression* {**any** | **only**} [**no-auth**]
8. Repeat Step 7 for each regular expression you want to add to the cache profile group defined in Step 4.
9. **all** [**no-auth**]
10. **end**
11. **show aaa cache group** *name*
12. **clear aaa cache group** *name* {**profile name** | **all**}
13. **debug aaa cache group**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|-------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | aaa new-model Example: Router(config)# aaa new-model | Enables the AAA access control model. |
| Step 4 | aaa cache profile <i>group-name</i> Example: Router(config)# aaa cache profile networkusers@companyname | Defines an authentication and authorization cache profile server group and enters profile map configuration mode. |
| Step 5 | profile <i>name</i> [no-auth] Example: Router(config-profile-map)# profile networkuser1 no-auth | Creates an individual authentication and authorization cache profile based on a username match. <ul style="list-style-type: none"> The <i>name</i> argument must be an exact match to a username being queried by an authentication or authorization service request. Use the no-auth keyword to bypass authentication for this user. |
| Step 6 | Repeat Step 5 for each username you want to add to the profile group in Step 4. | — |

| | Command or Action | Purpose |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7 | <pre>regexp matchexpression {any only} [no-auth]</pre> <p>Example: Router(config-profile-map)# regexp .*@example.com any no-auth</p> | <p>(Optional) Creates an entry in a cache profile group that matches based on a regular expression.</p> <ul style="list-style-type: none"> • If you use the any keyword, all unique usernames matching the regular expression are saved. • If you use the only keyword, only one profile entry is cached for all usernames matching the regular expression. • Use the no-auth keyword to bypass authentication for this user or set of users. • Because the number of entries in a regular expression cache profile group could be in the thousands, and validating each request against a regular expression can be time consuming, we do not recommend using regular expression entries in cache profile groups. |
| Step 8 | Repeat Step 7 for each regular expression you want to add to the cache profile group defined in Step 4. | — |
| Step 9 | <pre>all [no-auth]</pre> <p>Example: Router(config-profile-map)# all no-auth</p> | <p>(Optional) Specifies that all authentication and authorization requests are cached.</p> <ul style="list-style-type: none"> • Use the all command for specific service authorization requests, but it should be avoided when dealing with authentication requests. |
| Step 10 | <pre>end</pre> <p>Example: Router(config-profile-map)# end</p> | Returns to privileged EXEC mode. |
| Step 11 | <pre>show aaa cache group name</pre> <p>Example: Router# show aaa cache group networkusers@companyname</p> | (Optional) Displays all cache entries for a specified group. |
| Step 12 | <pre>clear aaa cache group name {profile name all}</pre> <p>Example: Router# clear aaa cache group networkusers@companyname profile networkuser1</p> | (Optional) Clears an individual entry or all entries in the cache. |
| Step 13 | <pre>debug aaa cache group</pre> <p>Example: Router# debug aaa cache group</p> | (Optional) Displays debug information about cached entries. |

Defining RADIUS and TACACS+ Server Groups That Use Cache Profile Group Information

Perform this task to define how RADIUS and TACACS+ server groups use the information stored in each cache profile group.

Prerequisites

RADIUS and TACACS+ server groups must be created.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server radius** *group-name*
or
aaa group server tacacs+ *group-name*
5. **cache authorization profile** *name*
6. **cache authentication profile** *name*
7. **cache expiry** *hours* [**enforce** | **failover**]
8. **end**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | aaa new-model Example: Router(config)# aaa new-model | Enables the AAA access control model. |
| Step 4 | aaa group server radius <i>group-name</i> or aaa group server tacacs+ <i>group-name</i> Example: Router(config)# aaa group server radius networkusers@companyname | Enters RADIUS server group configuration mode. <ul style="list-style-type: none">• To enter TACACS+ server group configuration mode, use the aaa group server tacacs+ <i>group-name</i> command. |

| | Command or Action | Purpose |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <pre>cache authorization profile name</pre> <p>Example: Router(config-sg-radius)# cache authorization profile networkusers@companyname </p> | <p>Activates the authorization caching rules in the profile networkusers for this RADIUS or TACACS+ server group.</p> <ul style="list-style-type: none"> The <i>name</i> argument in this command is a AAA cache profile group name. |
| Step 6 | <pre>cache authentication profile name</pre> <p>Example: Router(config-sg-radius)# cache authentication profile networkusers@companyname </p> | <p>Activates the authentication caching rules in the profile networkusers for this RADIUS or TACACS+ server group.</p> |
| Step 7 | <pre>cache expiry hours {enforce failover}</pre> <p>Example: Router(config-sg-radius)# cache expiry 240 failover </p> | <p>(Optional) Sets the amount of time before a cache profile entry expires (becomes stale).</p> <p>Use the enforce keyword to specify that once a cache profile entry expires it is not used again.</p> <p>Use the failover keyword to specify that an expired cache profile entry can be used if all other methods to authenticate and authorize the user fail.</p> |
| Step 8 | <pre>end</pre> <p>Example: Router(config-sg-radius)# end </p> | <p>Returns to privileged EXEC mode.</p> |

Updating Authorization and Authentication Method Lists to Specify How Cache Information is Used

Perform this task to update authorization and authentication method lists to use the authorization and authentication cache information.

Prerequisites

Method lists must already be defined.

SUMMARY STEPS

- enable**
- configure terminal**
- aaa new-model**
- aaa authorization {auth-proxy | cache | commands level | config-commands | configuration | console | exec | ipmobile | multicast | network | policy-if | prepaid | radius-proxy | reverse-access | subscriber-service | template} {default | list-name} [method1 [method2...]]**
- aaa authentication ppp {default | list-name} method1 [method2...]**
- aaa authentication login {default | list-name} method1 [method2...]**
- end**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p>enable</p> <p>Example: Router> enable</p> | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted. |
| Step 2 | <p>configure terminal</p> <p>Example: Router# configure terminal</p> | <p>Enters global configuration mode.</p> |
| Step 3 | <p>aaa new-model</p> <p>Example: Router(config)# aaa new-model</p> | <p>Enables the AAA access control model.</p> |
| Step 4 | <p>aaa authorization {auth-proxy cache commands level config-commands configuration console exec ipmobile multicast network policy-if prepaid radius-proxy reverse-access subscriber-service template} {default list-name} [method1 [method2...]]</p> <p>Example: Router(config)# aaa authorization network default cache networkusers@companyname group networkusers@companyname</p> | <p>Enables AAA authorization and creates method lists, which define the authorization methods used when a user accesses a specified function.</p> |
| Step 5 | <p>aaa authentication ppp {default list-name} method1 [method2...]</p> <p>Example: Router(config)# aaa authentication ppp default cache networkusers@companyname group networkusers@companyname</p> | <p>Specifies one or more authentication methods for use on serial interfaces that are running PPP.</p> |
| Step 6 | <p>aaa authentication login {default list-name} method1 [method2...]</p> <p>Example: Router(config)# aaa authentication login default cache adminusers group adminusers</p> | <p>Sets the authentication at login.</p> |
| Step 7 | <p>end</p> <p>Example: Router(config)# end</p> | <p>Returns to privileged EXEC mode.</p> |

Configuration Examples for Implementing Authorization and Authentication Profile Caching

This section contains the following examples:

- [Implementing Authorization and Authentication Profile Caching for Network Optimization: Example, page 10](#)
- [Implementing Authorization and Authentication Profile Caching as a Failover Mechanism: Example, page 10](#)

Implementing Authorization and Authentication Profile Caching for Network Optimization: Example

The following configuration example shows how to:

- Define a cache profile group `adminusers` that contains all administrator names on the network and sets it as the default list that is used for all login and exec sessions.
- Activate the new caching rules for a RADIUS server group.
- Add the new cache profile group in the authentication and authorization method list and change the method order so that the cache profile group is queried first.

```
configure terminal
  aaa new-model
  ! Define aaa cache profile groups and the rules for what information is saved to
  cache.
  aaa cache profile admin_users
  profile adminuser1
  profile adminuser2
  profile adminuser3
  profile adminuser4
  profile adminuser5
  exit
  ! Define server groups that use the cache information in each profile group.
  aaa group server radius admins@companyname.com
  cache authorization profile admin_users
  cache authentication profile admin_users
  ! Update authentication and authorization method lists to specify how profile groups
  and server groups are used.
  aaa authentication login default cache admins@companyname.com group
  admins@companyname.com
  aaa authorization exec default cache admins@companyname.com group
  admins@companyname.com
end
```

Implementing Authorization and Authentication Profile Caching as a Failover Mechanism: Example

The following configuration example shows how to:

- Create a cache profile group `admin_users` that contains all of the administrators on the network so that if the RADIUS or TACACS+ server should become unavailable the administrators can still access the network.

- Create a cache profile group `abc_users` that contains all of the ABC company users on the network so that if the RADIUS or TACACS+ server should become unavailable these users will be authorized to use the network.
- Activate the new caching rules for each profile group on a RADIUS server.
- Add the new cache profile group in the authentication and authorization method list and change the method order so that the cache profile group is queried last.

```

configure terminal
aaa new-model
! Define aaa cache profile groups and the rules for what information is saved to
cache.
aaa cache profile admin_users
profile admin1
profile admin2
profile admin3
exit
aaa cache profile abcusers
profile .*@example.com only no-auth
exit
! Define server groups that use the cache information in each cache profile group.
aaa group server tacacs+ admins@companyname.com
server 10.1.1.1
server 10.20.1.1
cache authentication profile admin_users
cache authorization profile admin_users
exit
aaa group server radius abcusers@example.com
server 172.16.1.1
server 172.20.1.1
cache authentication profile abcusers
cache authorization profile abcusers
exit
! Update authentication and authorization method lists to specify how cache is used.
aaa authentication login default cache admins@companyname.com group
admins@companyname.com
aaa authorization exec default cache admins@companyname.com group
admins@companyname.com
aaa authentication ppp default group abcusers@example.com cache abcusers@example.com
aaa authorization network default group abcusers@example.com cache
abcusers@example.com
end

```

Additional References

The following sections provide references related to implementing authentication and authorization profile caching.

Related Documents

| Related Topic | Document Title |
|-----------------------------------|---------------------------------------------|
| Authentication configuring tasks | “Configuring Authentication” module. |
| Authorization configuration tasks | “Configuring Authorization” module. |
| RADIUS configuration tasks | “Configuring RADIUS” module. |
| Security commands | <i>Cisco IOS Security Command Reference</i> |

Standards

| Standard | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | — |

MIBs

| MIB | MIBs Link |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

RFCs

| RFC | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | — |

Technical Assistance

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

Feature Information for Implementing Authorization and Authentication Profile Caching

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 Implementing Authorization and Authentication Profile Caching

| Feature Name | Releases | Feature Information |
|--------------------------------------------|----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AAA Authorization and Authentication Cache | 12.2(28)SB 12.2(33)SRC 12.2(33)SRC Cisco IOS XE Release 2.3 15.0(1)M | <p>This feature optimizes network performance and provides a failover mechanism in the event a network RADIUS or TACACS+ server becomes unavailable for any reason.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> Information About Implementing Authorization and Authentication Profile Caching How to Implement Authorization and Authentication Profile Caching <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> <p>This feature was integrated into Cisco IOS Release 15.0(1)M.</p> <p>The following commands were introduced or modified: aaa authentication login, aaa authentication ppp, aaa authorization, aaa cache profile, all (profile map configuration), cache authentication profile (server group configuration), cache authorization profile (server group configuration), cache expiry (server group configuration), clear aaa cache group, debug aaa cache group, profile (profile map configuration), regexp (profile map configuration), show aaa cache group.</p> |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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.

© 2006-2009 Cisco Systems, Inc. All rights reserved.



Authorization



Configuring Authorization

First Published: June 12, 1993

Last Updated: September 10, 2009

The AAA authorization feature is used to determine what a user can and cannot do. 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 is granted access to a requested service only if the information in the user profile allows it.

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 Authorization” section on page 15](#).

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, page 2](#)
- [Information About Configuring Authorization, page 2](#)
- [How to Configure Authorization, page 5](#)
- [Authorization Configuration Examples, page 8](#)
- [Additional References, page 13](#)
- [Feature Information for Configuring Authorization, page 15](#)



Americas Headquarters:

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

Prerequisites

Before configuring authorization using named method lists, the following tasks must be performed:

- Enable AAA on your network access server.
- Configure AAA authentication. Authorization generally takes place after authentication and relies on authentication to work properly.
- Define the characteristics of your RADIUS or TACACS+ security server if RADIUS or TACACS+ authorization is issued so that the Cisco network access server can communicate with the RADIUS or TACACS+ security server.
- Define the rights associated with specific users by using the **username** command if local authorization is issued.
- See the “[Related Documents](#)” section on page 13 for more information on documents related to these prerequisites.

Information About Configuring Authorization

The following sections provide information about how the Authorization feature is configured:

- [Named Method Lists for Authorization, page 2](#)
- [AAA Authorization Methods, page 3](#)
- [Method Lists and Server Groups, page 3](#)
- [AAA Authorization Types, page 4](#)
- [Authorization Attribute-Value Pairs, page 5](#)

Named Method Lists for Authorization

Method lists for authorization define the ways that authorization is performed and the sequence in which these methods are 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 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. See “[Related Documents](#)” section on page 13 for more information about where to find authentication proxy configuration documentation.

- **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 a named method list is created, a particular list of authorization methods for the indicated authorization type is defined.

Once defined, 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 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

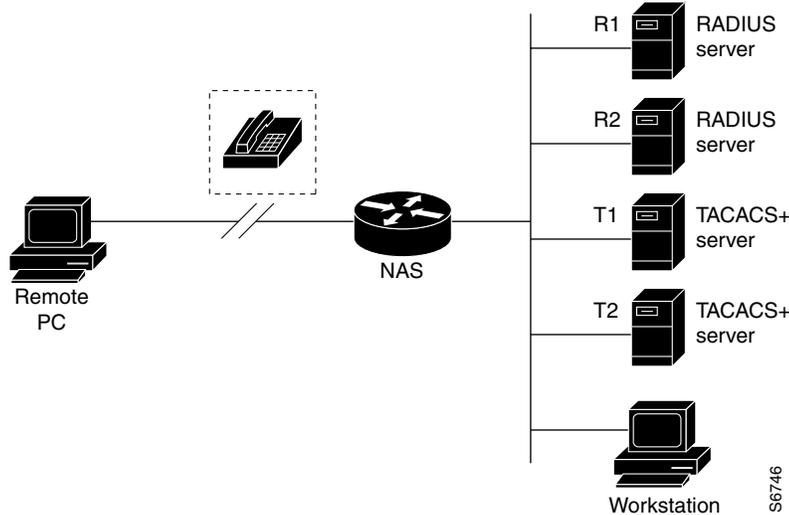
AAA supports five different methods of authorization:

- **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 through 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 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 make up the group of RADIUS servers. T1 and T2 make up the group of TACACS+ servers.

Figure 1 Typical AAA Network Configuration



Using server groups, a subset of the configured server hosts can be specified and use them for a particular service. For example, server groups allows R1 and R2 to be defined as separate server groups, and T1 and T2 as separate server groups. This allows either R1 and T1 to be specified in the method list or R2 and T2 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, 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 tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order they are configured.)

For more information about configuring server groups and about configuring server groups based on DNIS numbers. See the “[Configuring RADIUS](#)” or “[Configuring TACACS+](#)” feature modules.

AAA Authorization Types

Cisco IOS software supports five different types of authorization:

- **Auth-proxy**—Applies specific security policies on a per-user basis. See “[Related Documents](#)” [section on page 13](#) for more information about where to find authentication proxy configuration documentation.
- **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.

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.

See “[Related Documents](#)” section on page 13 for more information about supported RADIUS attributes and TACACS+ attribute-value pair documentation.

How to Configure Authorization

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](#)

See “[Authorization Configuration Examples](#)” section on page 8 for more information.

Configuring AAA Authorization Using Named Method Lists

Perform this task to configure AAA authorization using named method lists:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authorization** { **auth-proxy** | **network** | **exec** | **commands** *level* | **reverse-access** | **configuration** | **ipmobile** } { **default** | *list-name* } [*method1* [*method2*...]]
4. **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
5. **authorization** { **arap** | **commands** *level* | **exec** | **reverse-access** } { **default** | *list-name* }

DETAILED STEPS

| | Command | Purpose |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | Router(config)# aaa authorization { auth-proxy network exec commands <i>level</i> reverse-access configuration ipmobile } { default <i>list-name</i> } [<i>method1</i> [<i>method2</i> ...]] | Creates an authorization method list for a particular authorization type and enable authorization. |
| Step 4 | Router(config)# line [aux console tty vty] <i>line-number</i> [<i>ending-line-number</i>] or Router(config)# interface <i>interface-type</i> <i>interface-number</i> | Enters the line configuration mode for the lines to which the authorization method list is applied. Alternately, enters the interface configuration mode for the interfaces to which the authorization method list is applied. |
| Step 5 | Router(config-line)# authorization { arap commands <i>level</i> exec reverse-access } { default <i>list-name</i> } or Router(config-line)# ppp authorization { default <i>list-name</i> } | Applies the authorization list to a line or set of lines. Alternately, applies the authorization list to an interface or set of interfaces. |

This section includes the following sections:

- [Authorization Types](#)
- [Authorization Methods](#)

Authorization Types

Named authorization method lists are specific to the indicated type of authorization.

To create a method list to enable authorization that applies specific security policies on a per-user basis, use the **auth-proxy** keyword. See “[Related Documents](#)” section on page 13 for more information about where to find authentication proxy configuration documentation.

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 all commands associated with a specified command level from 0 to 15 to be authorized.)

To create a method list to enable authorization for reverse Telnet functions, use the **reverse-access** keyword.

Authorization Methods

To have the network access server request authorization information through 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, see the “[Configuring TACACS+](#)” feature module. For an example of how to enable a TACACS+ server to authorize the use of network services, including PPP and ARA, see the “[TACACS+ Authorization: Examples](#)” section on [page 10](#) for more information.

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 this method is selected, all requested functions are automatically granted to authenticated users.

There may be times when it is not desirable to run authorization from a particular interface or line. To stop authorization activities on designated lines or interfaces, use the **none method** keyword. If this method is selected, 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, see the “[Configuring Authentication](#)” feature module.

To have the network access server request authorization through a RADIUS security server, use the **radius method** keyword. For more specific information about configuring authorization using a RADIUS security server, see the “[Configuring RADIUS](#)” feature module.

To have the network access server request authorization through 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, see the “[Configuring RADIUS](#)” feature module. For an example of how to enable a RADIUS server to authorize services, see the “[RADIUS Authorization: Example](#)” section on [page 11](#) for more information.



Note

Authorization method lists for SLIP follow whatever is configured for PPP on the relevant interface. If no lists are defined and applied to a particular interface (or no PPP settings are configured), the default setting for authorization applies.

Disabling Authorization for Global Configuration Commands

The **aaa authorization** command with the keyword **commands** attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level. Because there are configuration commands that are identical to some EXEC-level commands, there can be some confusion in the authorization process. Using **no aaa authorization config-commands** stops the network access server from attempting configuration command authorization.

To disable AAA authorization for all global configuration commands, use the following command in global configuration mode:

| Command | Purpose |
|-------------------------------------------------------------|---------------------------------------------------------------|
| Router(config)# no aaa authorization config-commands | Disables authorization for all global configuration commands. |

Configuring Authorization for Reverse Telnet

Telnet is a standard terminal emulation protocol used for remote terminal connection. Normally, a network access server is logged into and then Telnet is used 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 |
|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Router(config)# aaa authorization reverse-access <i>method1 [method2 ...]</i> | 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+. The specific reverse Telnet privileges for the user on the security server itself must be configured.

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 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 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 is 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 is used on serial lines using PPP. If the RADIUS server fails to respond, then local network authorization is 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) are 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 through RADIUS. This can be used to govern address assignment, the application of access lists, and various other per-user quantities.



Note

Since no fallback method is specified in this example, authorization fails 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.

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.

Additional References

The following sections provide references related to the Authorization feature.

Related Documents

| Related Topic | Document Title |
|-------------------------------|-------------------------------------------------------------------------------------------|
| Authorization Commands | Cisco IOS Security Command Reference |
| RADIUS | “ Configuring RADIUS ” feature module. |
| RADIUS attributes | “ RADIUS Attributes Overview and RADIUS IETF Attributes ” feature module. |
| TACACS+ | “ Configuring TACACS+ ” feature module. |
| TACACS+ Attribute-Value Pairs | “ TACACS+ Attribute-Value Pairs ” feature module. |
| Authentication | “ Configuring Authentication ” feature module. |
| Authentication Proxy | “ Configuring Authentication Proxy ” feature module. |

Standards

| Standard | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | — |

MIBs

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

RFCs

| RFC | Title |
|--------------------------------------------------------|-------|
| 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>http://www.cisco.com/techsupport</p> |

Feature Information for Configuring Authorization

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 Configuring Authorization

| Feature Name | Releases | Feature Information |
|---------------------------|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuring Authorization | 10.0 Cisco IOS XE Release 2.1 | The AAA authorization feature is used to determine what a user can and cannot do. 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 is granted access to a requested service only if the information in the user profile allows it. This feature was introduced in Cisco IOS Release 10.0. This feature was introduced on Cisco ASR 1000 Series Routers. |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, 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 Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, 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. (0910R)

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.

© 1993–2009 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 32.

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 25](#)
- [Additional References, page 30](#)
- [Feature Information for Configuring Accounting, page 32](#)



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 by using the **aaa new-model** command in global configuration mode.
- 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 “[Configuring RADIUS](#)” module. For more information about configuring the Cisco network access server to communicate with the TACACS+ security server, see the “[Configuring TACACS+](#)” module.

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.

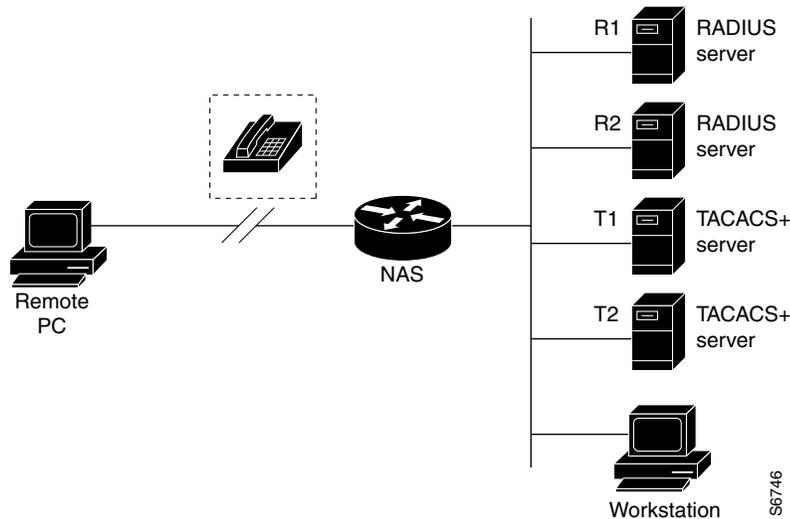
This section includes the following subsections:

- [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: Securing User Services*.

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](#)

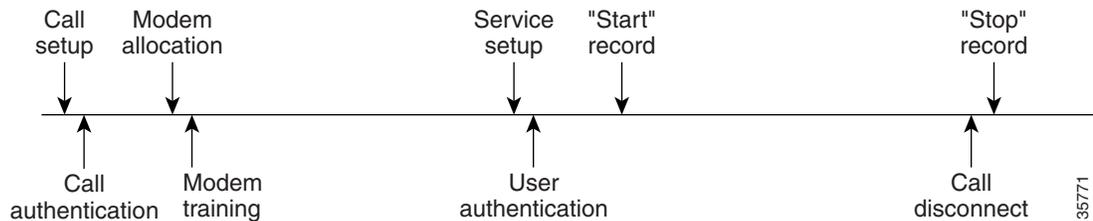
AAA Resource Failure Stop Accounting

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*

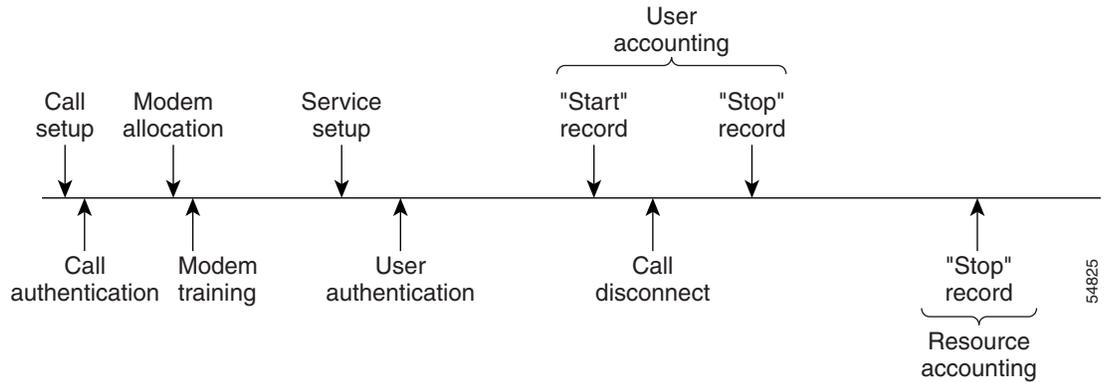


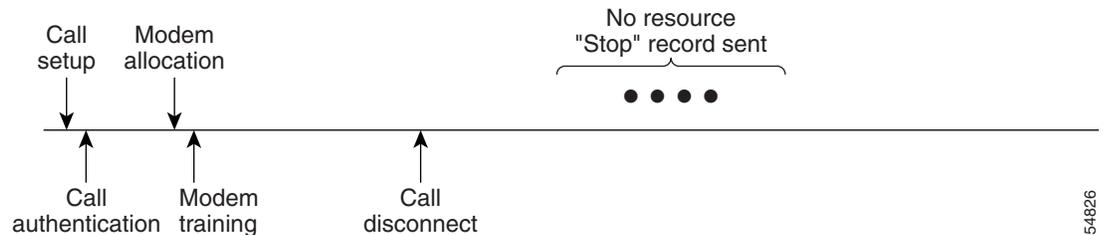
Figure 4 illustrates a call setup sequence with call disconnect occurring before user authentication and with AAA resource failure stop accounting enabled.

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*



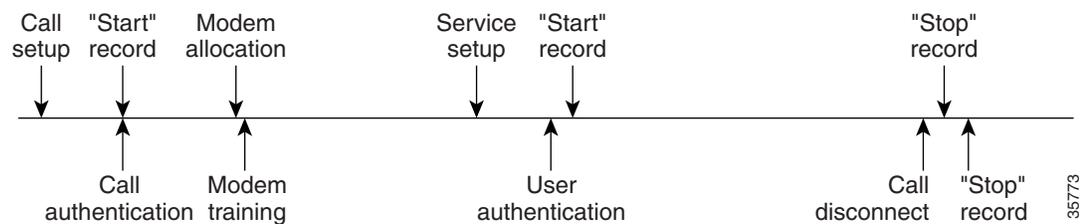
AAA Resource Accounting for Start-Stop Records

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 20](#)
- [Generating Interim Accounting Records, page 20](#)
- [Generating Accounting Records for Failed Login or Session, page 21](#)
- [Specifying Accounting NETWORK-Stop Records Before EXEC-Stop Records, page 21](#)
- [Configuring AAA Resource Failure Stop Accounting, page 21](#)
- [Configuring AAA Resource Accounting for Start-Stop Records, page 23](#)
- [Configuring AAA Broadcast Accounting, page 23](#)
- [Configuring Per-DNIS AAA Broadcast Accounting, page 23](#)
- [Configuring AAA Session MIB, page 24](#)
- [Establishing a Session with a Router if the AAA Server is Unreachable, page 24](#)
- [Monitoring Accounting, page 25](#)
- [Troubleshooting Accounting, page 25](#)

Configuring AAA Accounting Using Named Method Lists

To configure AAA accounting using named method lists, use the following commands beginning in global configuration mode:

| | Command | Purpose |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# aaa accounting { system network exec connection commands level } { default <i>list-name</i> } { start-stop stop-only none } [<i>method1</i> [<i>method2...</i>]] | Creates an accounting method list and enables accounting. The argument <i>list-name</i> is a character string used to name the created list. |
| Step 2 | Router(config)# line [aux console tty vtty] <i>line-number</i> [<i>ending-line-number</i>] or Router(config)# interface <i>interface-type</i> <i>interface-number</i> | Enters the line configuration mode for the lines to which the accounting method list is applied. or Enters the interface configuration mode for the interfaces to which the accounting method list is applied. |
| Step 3 | Router(config-line)# accounting { arap commands level connection exec } { default <i>list-name</i> } or Router(config-if)# ppp accounting { default <i>list-name</i> } | Applies the accounting method list to a line or set of lines. or Applies the accounting method list to an interface or set of interfaces. |



Note

System accounting does not use named method lists. For system accounting, define only the default method list.

This section includes the following sections:

- [Accounting Types, page 17](#)
- [Accounting Record Types, page 17](#)
- [Accounting Methods, page 17](#)
- [Configuring RADIUS System Accounting, page 19](#)

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 |
|--------------------------------|--------------------------------------------------------------------------------------------------------------|
| group radius | Uses the list of all RADIUS servers for accounting. |
| group tacacs+ | Uses the list of all TACACS+ servers for accounting. |
| group <i>group-name</i> | 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.

Configuring RADIUS System Accounting

This task is used to configure RADIUS system accounting on the global RADIUS server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server accounting system host-config**
5. **aaa group server radius *server-name***
6. **server-private {*host-name* | *ip-address*} key {[0 *server-key* | 7 *server-key*] *server-key*}**
7. **accounting system host-config**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | aaa new-model Example: Router(config)# aaa new-model | Enables AAA network security services. |
| Step 4 | radius-server accounting system host-config Example: Router(config)# radius-server accounting system host-config | Enables the router to send a system accounting record for the addition and deletion of a RADIUS server. |
| Step 5 | aaa group server radius <i>server-name</i> Example: Router(config)# aaa group server radius radgroup1 | Adds the RADIUS server and enters server-group (config-sg-radius) configuration mode. <ul style="list-style-type: none"> • The <i>server-name</i> argument specifies the RADIUS server group name. |

| | Command or Action | Purpose |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6 | <p>server-private {<i>host-name</i> <i>ip-address</i>} key {[0 <i>server-key</i> 7 <i>server-key</i>] <i>server-key</i>}</p> <p>Example: Router(config-sg-radius)# server-private 172.16.1.11 key cisco</p> | <p>Enters the hostname or IP address of the RADIUS server and hidden server key.</p> <ul style="list-style-type: none"> (Optional) 0 with the <i>server-key</i> argument specifies that an unencrypted (cleartext) hidden server key follows. (Optional) 7 with the <i>server-key</i> argument specifies that an encrypted hidden server key follows. The <i>server-key</i> argument specifies the hidden server key. If the <i>server-key</i> argument is configured without the 0 or 7 preceding it, it is unencrypted. <p>Note Once the server-private command is configured RADIUS system accounting is enabled.</p> |
| Step 7 | <p>accounting system host-config</p> <p>Example: Router(config-sg-radius)# accounting system host-config</p> | <p>Enables the generation of system accounting records for private server hosts when they are added or deleted.</p> |

Suppressing Generation of Accounting Records for Null Username Sessions

When AAA accounting is activated, the Cisco IOS software issues accounting records for all users on the system, including users whose username string, because of protocol translation, is NULL. An example of this is users who come in on lines where the **aaa authentication login method-list none** command is applied. To prevent accounting records from being generated for sessions that do not have usernames associated with them, use the following command in global configuration mode:

| Command | Purpose |
|--------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| Router(config)# aaa accounting suppress null-username | Prevents accounting records from being generated for users whose username string is NULL. |

Generating Interim Accounting Records

To enable periodic interim accounting records to be sent to the accounting server, use the following command in global configuration mode:

| Command | Purpose |
|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| Router(config)# aaa accounting update {[newinfo] [periodic] number} | Enables periodic interim accounting records to be sent to the accounting server. |

When the **aaa accounting update** command is activated, the Cisco IOS software issues interim accounting records for all users on the system. If the keyword **newinfo** is used, interim accounting records are sent to the accounting server every time there is new accounting information to report. An example of this would be when IPCP completes IP address negotiation with the remote peer. The interim accounting record includes the negotiated IP address used by the remote peer.

When used with the keyword **periodic**, interim accounting records are sent periodically as defined by the argument number. The interim accounting record contains all of the accounting information recorded for that user up to the time the interim accounting record is sent.

**Caution**

Using the **aaa accounting update periodic** command can cause heavy congestion when many users are logged in to the network.

Generating Accounting Records for Failed Login or Session

When AAA accounting is activated, the Cisco IOS software does not generate accounting records for system users who fail login authentication, or who succeed in login authentication but fail PPP negotiation for some reason.

To specify that accounting stop records be generated for users who fail to authenticate at login or during session negotiation, use the following command in global configuration mode:

| Command | Purpose |
|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| Router(config)# aaa accounting send stop-record authentication failure | Generates “stop” records for users who fail to authenticate at login or during session negotiation using PPP. |

Specifying Accounting NETWORK-Stop Records Before EXEC-Stop Records

For PPP users who start EXEC terminal sessions, it can be specified that NETWORK records be generated before EXEC-stop records. In some cases, such as billing customers for specific services, it can be desirable to keep network start and stop records together, essentially “nesting” them within the framework of the EXEC start and stop messages. For example, a user dialing in using PPP can create the following records: EXEC-start, NETWORK-start, EXEC-stop, NETWORK-stop. By nesting the accounting records, NETWORK-stop records follow NETWORK-start messages: EXEC-start, NETWORK-start, NETWORK-stop, EXEC-stop.

To nest accounting records for user sessions, use the following command in global configuration mode:

| Command | Purpose |
|----------------------------------------------|-----------------------------------|
| Router(config)# aaa accounting nested | Nests network accounting records. |

Configuring AAA Resource Failure Stop Accounting

To enable resource failure stop accounting, use the following command in global configuration:

| Command | Purpose |
|------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>Router(config)# aaa accounting resource <i>method-list stop-failure group server-group</i></pre> | <p>Generates a “stop” record for any calls that do not reach user authentication.</p> <p>Note Before configuring this feature, the tasks described in the section “Prerequisites for Configuring Accounting” 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 “Configuring SNMP Support” 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)# aaa accounting resource method-list start-stop group server-group</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>Note Before configuring this feature, the tasks described in the section “Prerequisites for Configuring Accounting” 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 “Configuring SNMP Support” 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)# aaa accounting {system network exec connection commands level} {default list-name} {start-stop stop-only none} [broadcast] method1 [method2...]</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)# aaa dnis map dnis-number accounting network [start-stop stop-only none] [broadcast] method1 [method2...]</pre> | <p>Allows per-DNIS accounting configuration. This command has precedence over the global aaa accounting 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)# aaa session-mib disconnect | Monitors and terminates authenticated client connections using SNMP. To terminate the call, the disconnect keyword must be used. |

Establishing a Session with a Router if the AAA Server is Unreachable

To establish a console or telnet session with a router if the AAA server is unreachable, use the following command in Global Configuration mode:

| Command | Purpose |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router(config)# no aaa accounting system guarantee-first | The aaa accounting system guarantee-first command guarantees system accounting as the first record, which is the default condition. In some situations, users may be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than three minutes. To resolve this problem, the no aaa accounting system guarantee-first command can be used. |



Note

Entering the **no aaa accounting system guarantee-first** command is not the only condition by which the console or telnet session can be started. For example, if the Privileged EXEC session is being authenticated by TACACS and the TACACS server is not reachable, then the session cannot start.

Monitoring Accounting

No specific **show** command exists for either RADIUS or TACACS+ accounting. To obtain accounting records displaying information about users currently logged in, use the following command in privileged EXEC mode:

| Command | Purpose |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Router# show accounting | Allows display of the active accountable events on the network and helps collect information in the event of a data loss on the accounting server. |

Troubleshooting Accounting

To troubleshoot accounting information, use the following command in privileged EXEC mode:

| Command | Purpose |
|-------------------------------------|-----------------------------------------------------------|
| Router# debug aaa accounting | Displays information on accountable events as they occur. |

Configuration Examples for AAA Accounting

This section contains the following examples:

- [Configuring Named Method List: Example, page 26](#)
- [Configuring AAA Resource Accounting: Example, page 28](#)
- [Configuring AAA Broadcast Accounting: Example, page 28](#)
- [Configuring Per-DNIS AAA Broadcast Accounting: Example, page 29](#)
- [AAA Session MIB: Example, page 29](#)

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 | “ Configuring Authorization ” module. |
| Authentication | “ Configuring Authentication ” module. |

Standards

| Standard | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | — |

MIBs

| MIB | MIBs Link |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

RFCs

| RFC | Title |
|----------|----------------------------------------------------------|
| RFC 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>http://www.cisco.com/techsupport</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 Connection Accounting, page 7 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 Configuring AAA Session MIB, page 24 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 Configuring AAA Broadcast Accounting, page 23 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 Generating Interim Accounting Records, page 20 for more information. |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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

First Published: November 27, 2000
Last Updated: August 4, 2009

The Cisco IOS Firewall Authentication Proxy feature provides dynamic, per-user authentication and authorization, authenticating users against industry standard TACACS+ and RADIUS authentication protocols. Authenticating and authorizing connections by users provides more robust protection against network attacks.

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 Authentication Proxy”](#) section on page 35.

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 Configuring Authentication Proxy](#), page 2
- [Restrictions for Configuring Authentication Proxy](#), page 2
- [Information About Configuring Authentication Proxy](#), page 2
- [How to Configure Authentication Proxy](#), page 12
- [Monitoring and Maintaining Authentication Proxy](#), page 19
- [Configuration Examples for Authentication Proxy](#), page 20
- [Additional References](#), page 33
- [Feature Information for Authentication Proxy](#), page 35



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

Prerequisites for 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.”

Restrictions for Configuring Authentication Proxy

- 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.

Information About Configuring 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.

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:

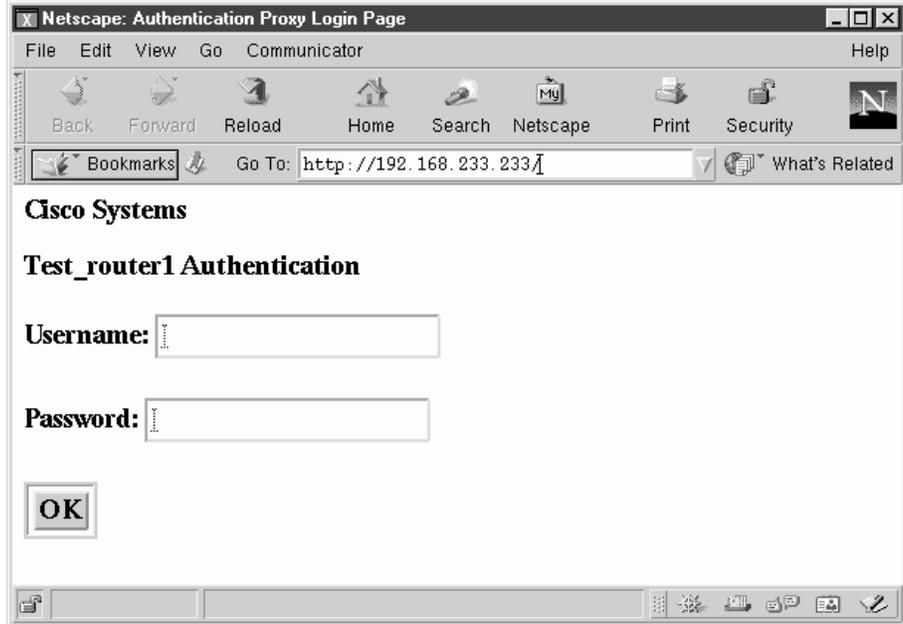
- [How Authentication Proxy Works, page 3](#)
- [Secure Authentication, page 5](#)
- [Using Authentication Proxy, page 6](#)
- [When to Use the Authentication Proxy, page 7](#)
- [Applying Authentication Proxy, page 8](#)
- [Operation with One-Time Passwords, page 9](#)
- [Compatibility with Other Security Features, page 9](#)
- [Compatibility with AAA Accounting, page 10](#)
- [Protection Against Denial-of-Service Attacks, page 11](#)
- [Risk of Spoofing with Authentication Proxy, page 11](#)
- [Comparison with the Lock-and-Key Feature, page 11](#)

How 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 1](#) illustrates the authentication proxy HTML login page.

Figure 1 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.

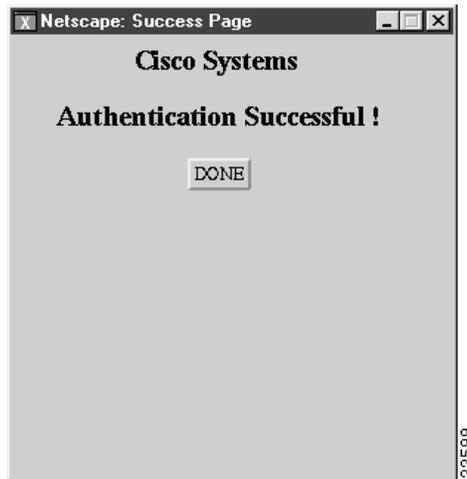
If the authentication fails, the authentication proxy reports the failure to the user and prompts the user with multiple retries. If the user fails to authenticate after five attempts, the user must wait two minutes and initiate another HTTP session to trigger authentication proxy.

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 2](#) illustrates the login status in the HTML page.

Figure 2 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](#)

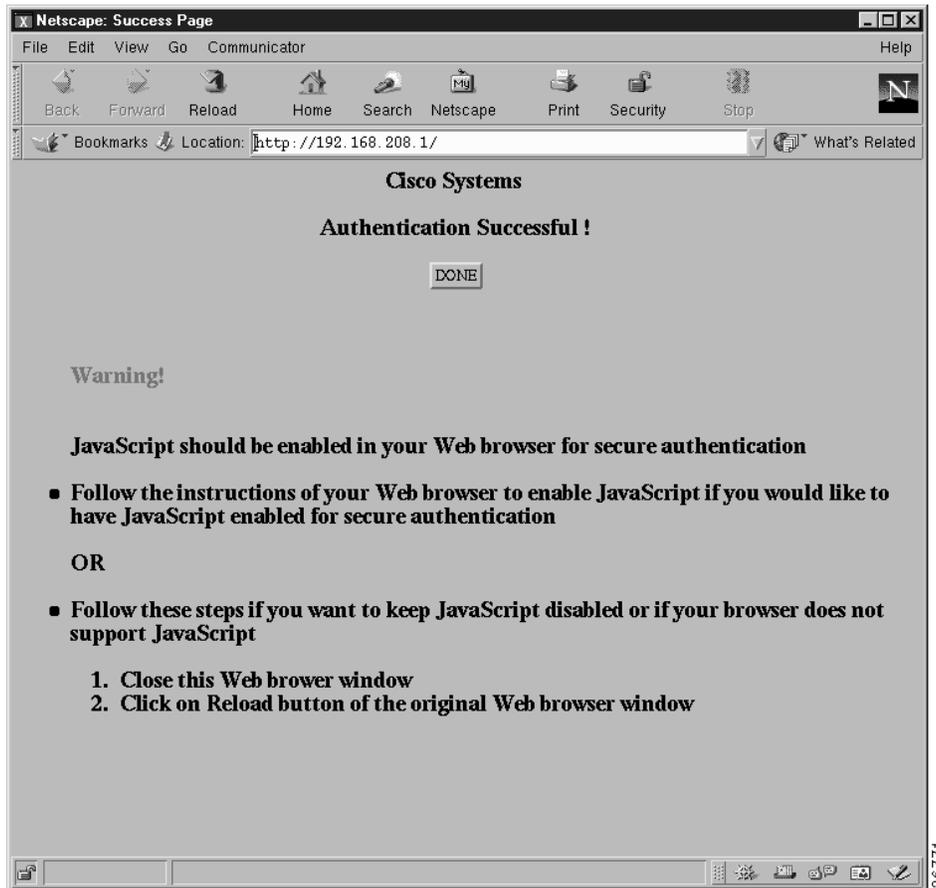
Operation with JavaScript

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 2](#). 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 3](#) illustrates the authentication proxy login status message with JavaScript disabled on the browser.

Figure 3 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 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 1](#) describes the interaction of the authentication proxy with the client host.

Table 1 **Authentication Proxy Interaction with the Client Host**

| Authentication Proxy Action with Client | Description |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Triggering on HTTP connections | If a user is not currently authenticated at the firewall router, any HTTP connection initiated by the user triggers the authentication proxy. If the user is already authenticated, the authentication proxy is transparent to the user. |
| Logging in using the login page | Triggering the authentication proxy generates an HTML-based login page. The user must enter a username and password to be authenticated with the AAA server. Figure 1 illustrates the authentication proxy login page. |
| Authenticating the user at the client | <p>Following the login attempt, the authentication proxy action can vary depending on whether JavaScript is enabled in the browser. If JavaScript is enabled, and authentication is successful, the authentication proxy displays a message indicating the status of the authentication as shown in Figure 2. After the authentication status is displayed, the proxy automatically completes the HTTP connection.</p> <p>If JavaScript is disabled, and authentication is successful, the authentication proxy generates a popup window with additional instructions for completing the connection. See Figure 3.</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 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 4 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 4 Applying the Authentication Proxy at the Local Interface

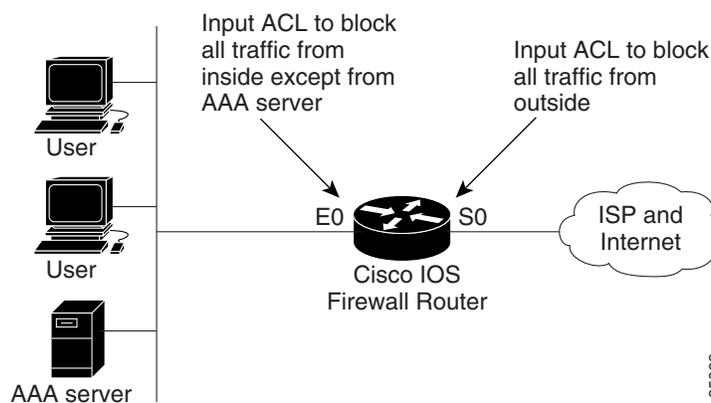
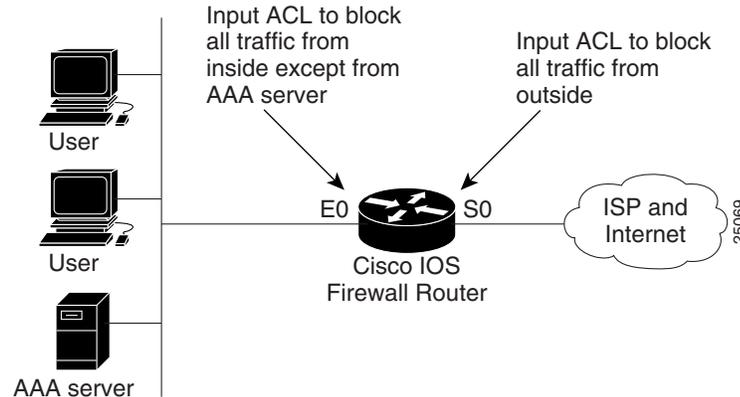


Figure 5 shows the authentication proxy applied at the dial-in interface with all network traffic blocked at each interface.

Figure 5 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 2](#) compares the authentication proxy and lock-and-key features.

Table 2 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.

How to Configure Authentication Proxy

To configure the authentication proxy feature, perform the following tasks:

- [Configuring AAA](#) (Required)
- [Configuring the HTTP Server for Authentication Proxy](#) (Required)
- [Configuring Authentication Proxy](#) (Required)
- [Verifying Authentication Proxy](#) (Optional)

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

Configuring AAA

You must configure the authentication proxy for AAA services. Use the following commands in global configuration mode to enable authorization and to define the authorization methods:

| | Command | Purpose |
|--------|-----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>router(config)# aaa new-model</code> | Enables the AAA functionality on the router. |
| Step 2 | <code>router(config)# aaa authentication login default TACACS+ RADIUS</code> | Defines the list of authentication methods at login. |
| Step 3 | <code>router(config)# aaa authorization auth-proxy default [method1 [method2...]]</code> | Uses the auth-proxy keyword to enable authentication proxy for AAA methods. |
| Step 4 | <code>router(config)# aaa accounting auth-proxy default start-stop group tacacs+</code> | Uses the auth-proxy keyword to set up the authorization policy as dynamic ACLs that can be downloaded. This command activates authentication proxy accounting. |
| Step 5 | <code>router(config)# tacacs-server host hostname</code> | Specifies an AAA server. For RADIUS servers, use the radius server host command. |
| Step 6 | <code>router(config)# tacacs-server key key</code> | Sets the authentication and encryption key for communications between the router and the AAA server. For RADIUS servers use the radius server key command. |
| Step 7 | <code>router(config)# access-list access-list-number permit tcp host source eq tacacs host destination</code> | Creates an ACL entry to allow the AAA server to return traffic to the firewall. The source address is the IP address of the AAA server, and the destination is the IP address of the router interface where the AAA server resides. |

In addition to configuring AAA on the firewall router, the authentication proxy requires a per-user access profile configuration on the AAA server. To support the authentication proxy, configure the AAA authorization service **auth-proxy** on the AAA server as outlined here:

- Define a separate section of authorization for the **auth-proxy** keyword to specify the downloadable user profiles. This keyword does not interfere with other type of services, such as EXEC. The following example shows a user profile on a TACACS server:

```
default authorization = permit
key = cisco
user = newuser1 {
login = cleartext cisco
service = auth-proxy
}
```

```
priv-lvl=15
proxyacl#1="permit tcp any any eq 26"
proxyacl#2="permit icmp any host 60.0.0.2"
proxyacl#3="permit tcp any any eq ftp"
proxyacl#4="permit tcp any any eq ftp-data"
proxyacl#5="permit tcp any any eq smtp"
proxyacl#6="permit tcp any any eq telnet"
}
}
```

- The only supported attribute in the AAA server user configuration is proxyacl#n. Use the proxyacl#n attribute when configuring the access lists in the profile. The attribute proxyacl#n is for both RADIUS and TACACS+ attribute-value (AV) pairs.
- The privilege level must be set to 15 for all users.
- The access lists in the user profile on the AAA server must have access commands that contain only the **permit** keyword.
- Set the source address to the **any** keyword in each of the user profile access list entries. The source address in the access lists is replaced with the source address of the host making the authentication proxy request when the user profile is downloaded to the firewall.
- The supported AAA servers are:
 - CiscoSecure ACS 2.1.x for Windows NT
 - CiscoSecure ACS 2.3 for Windows NT
 - CiscoSecure ACS 2.2.4 for UNIX
 - CiscoSecure ACS 2.3 for UNIX
 - TACACS+ server (vF4.02.alpha)
 - Ascend RADIUS server radius-980618 (required attribute-value pair patch)
 - Livingston RADIUS server (v1.16)

Refer to the section [“AAA Server User Profile Example”](#) for sample AAA server configurations.

Configuring the HTTP Server for Authentication Proxy

This task is used to enable the HTTP server on the firewall and configure the HTTP server's AAA authentication method for authentication proxy.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **ip http access-class** *access-list-number*

DETAILED STEPS

| | Command | Purpose |
|--------|--------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | ip http server Example: Router# ip http server | Enables the HTTP server on the router. The authentication proxy uses the HTTP server to communicate with the client for user authentication. |
| Step 4 | ip http access-class <i>access-list-number</i> Example: router(config)# configure terminal | Specifies the access list for the HTTP server. Use the standard access list number configured in the section “Interface Configuration: Example.” |

Configuring Authentication Proxy

Use the following commands to configure the authentication proxy:

SUMMARY STEPS

- enable**
- configure terminal**
- ip auth-proxy auth-cache-time** *min*
- ip auth-proxy auth-proxy-banner**
- ip auth-proxy name** *auth-proxy-name* **http** [**auth-cache-time** *min*] [**list** {*acl* |*acl-name*}]
- interface** *type*
- ip auth-proxy** *auth-proxy-name*

DETAILED STEPS

| | Command | Purpose |
|--------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |

| Command | Purpose |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Step 3</p> <pre>ip auth-proxy auth-cache-time min</pre> <p>Example: Router(config)# ip auth-proxy auth-cache-time 5</p> | <p>(Optional) 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.</p> <p>Note Use this 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.</p> |
| <p>Step 4</p> <pre>ip auth-proxy auth-proxy-banner</pre> <p>Example: Router(config)# configure terminal</p> | <p>(Optional) Displays the name of the firewall router in the authentication proxy login page. The banner is disabled by default.</p> |
| <p>Step 5</p> <pre>ip auth-proxy name auth-proxy-name http [auth-cache-time min] [list {acl acl-name}]</pre> <p>Example: Router(config)# ip auth-proxy name HQ_users http</p> | <p>Creates authentication proxy rules. The rules define how you apply authentication proxy. This command associates connections initiating HTTP protocol traffic with an authentication proxy name. You can associate the named rule with an access control list (ACL), providing control over which hosts use the authentication proxy feature. If no standard access list is defined, the named authentication proxy rule intercepts HTTP traffic from all hosts whose connection initiating packets are received at the configured interface.</p> <p>(Optional) The auth-cache-time option overrides the global authentication proxy cache timer. This option provides more control over timeout values for a specific authentication proxy rule. If no value is specified, the proxy rule assumes the value set with the ip auth-proxy auth-cache-time command.</p> <p>(Optional) The list option allows you to apply a standard, extended (1-199), or named access list to a named authentication proxy rule. HTTP connections initiated by hosts in the access list are intercepted by the authentication proxy.</p> |

| | Command | Purpose |
|--------|----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6 | interface <i>type</i> Example: Router(config)# interface Ethernet0/0 | Enters interface configuration mode by specifying the interface type on which to apply the authentication proxy. |
| Step 7 | ip auth-proxy <i>auth-proxy-name</i> Example: Router(config-if)# ip auth-proxy HQ_users http | In interface configuration mode, applies the named authentication proxy rule at the interface. This command enables the authentication proxy rule with that name. |

Verifying Authentication Proxy

Verifying the authentication proxy configuration can have several components:

- [Checking the Authentication Proxy Configuration](#) (Optional)
- [Establishing User Connections with JavaScript](#) (Optional)
- [Establishing User Connections Without JavaScript](#) (Optional)

Checking the Authentication Proxy Configuration

To check the current authentication proxy configuration, use the **show ip auth-proxy configuration** command in privileged EXEC mode:

| Command | Purpose |
|-------------------------------------------------|--------------------------------------------------|
| router# show ip auth-proxy configuration | Displays the authentication proxy configuration. |

In the following example, the global authentication proxy idle timeout value is set to 60 minutes, the named authentication proxy rule is “pxy”, and the idle timeout value for this named rule is one minute. The display shows that no host list is specified, meaning that all connections initiating HTTP traffic at the interface are subject to the authentication proxy rule.

```
router# show ip auth-proxy configuration
Authentication cache time is 60 minutes
Authentication Proxy Rule Configuration
Auth-proxy name pxy
http list not specified auth-cache-time 1 minutes
```

To verify that the authentication proxy is successfully configured on the router, ask a user to initiate an HTTP connection through the router. The user must have authentication and authorization configured at the AAA server. If the user authentication is successful, the firewall completes the HTTP connection for the user. If the authentication is unsuccessful, check the access list and the AAA server configurations.

Display the user authentication entries using the **show ip auth-proxy cache** command in privileged EXEC mode:

| Command | Purpose |
|-----------------------------------------|---------------------------------------------------|
| router# show ip auth-proxy cache | Displays the list of user authentication entries. |

The authentication proxy cache lists the host IP address, the source port number, the timeout value for the authentication proxy, and the state of the connection. If the authentication proxy state is HTTP_ESTAB, the user authentication was successful.

```
router# show ip auth-proxy cache
Authentication Proxy Cache
Client IP 192.168.25.215 Port 57882, timeout 1, state HTTP_ESTAB
```

Wait for one minute, which is the timeout value for this named rule, and ask the user to try the connection again. After one minute, the user connection is denied because the authentication proxy has removed the user’s authentication entry and any associated dynamic ACLs. The user is presented with a new authentication login page and must log in again to gain access through the firewall.

Establishing User Connections with JavaScript

To verify client connections using the authentication proxy with JavaScript enabled on the client browser, follow this procedure:

-
- Step 1** From a client host, initiate an HTTP connection through the firewall. This generates the authentication proxy login page.
 - Step 2** At the authentication proxy login page, enter a username and password.
 - Step 3** Click **OK** to submit the username and password to the AAA server.

A popup window appears indicating whether the login attempt succeeded or failed. If the authentication is successful, the connection is completed automatically. If the authentication fails, the authentication proxy reports the failure to the user and prompts the user with multiple retries.



Note If the authentication attempt is unsuccessful after five attempts, the user must wait two minutes and initiate another HTTP session to trigger authentication proxy.

Establishing User Connections Without JavaScript

To ensure secure authentication, the authentication proxy design requires JavaScript. You can use the authentication proxy without enabling JavaScript on the browser, but this poses a potential security risk if users do not properly establish network connections. The following procedure provides the steps to properly establish a connection with JavaScript disabled. Network administrators are strongly advised to instruct users on how to properly establish connections using the procedure in this section.



Note Failure to follow this procedure can cause user credentials to be passed to a network web server other than the authentication proxy or can cause the authentication proxy to reject the login attempt.

To verify client connections using the authentication proxy when JavaScript is not enabled on the client browser, follow this procedure:

-
- Step 1** Initiate an HTTP connection through the firewall.
This generates the authentication proxy login page.
 - Step 2** From the authentication proxy login page at the client, enter the username and password.
 - Step 3** Click **OK** to submit the username and password to the AAA server.

A popup window appears indicating whether the login attempt succeeded or failed. If the popup window indicates successful authentication, go to [Step 7](#).

- Step 4** If the popup window displays a failed authentication message, click **Close** on the browser **File** menu.



Note Do not click **Reload (Refresh** for Internet Explorer) to close the popup window.

- Step 5** From the original authentication login page, click **Reload (Refresh** for Internet Explorer) on the browser toolbar. The user login credentials are cleared from the form.



Note Do not click **OK**. You must click **Reload** or **Refresh** to clear the username and password and to reload the form before attempting to log in again.

Step 6 Enter the username and password again.

If the authentication is successful, a window appears displaying a successful authentication message. If the window displays a failed authentication message, go to [Step 4](#).

Step 7 Click **Close** on the browser **File** menu.

Step 8 From the original authentication proxy login page, click **Reload** (**Refresh** for Internet Explorer) on the browser toolbar.

The authentication proxy completes the authenticated connection with the web server.

Monitoring and Maintaining Authentication Proxy

This section describes how to view dynamic access list entries and how to manually remove authentication entries. This section contains the following sections:

- [Displaying Dynamic ACL Entries](#)
- [Deleting Authentication Proxy Cache Entries](#)

Displaying Dynamic ACL Entries

You can display dynamic access list entries when they are in use. After an authentication proxy entry is cleared by you or by the idle timeout parameter, you can no longer display it. The number of matches displayed indicates the number of times the access list entry was hit.

To view dynamic access lists and any temporary access list entries that are currently established by the authentication proxy, use the **show ip access-lists** command in privileged EXEC mode:

| Command | Purpose |
|-------------------------------------|------------------------------------------------------------------------------------------------------------|
| router# show ip access-lists | Displays the standard and extended access lists configured on the firewall, including dynamic ACL entries. |

Consider the following example where ACL 105 is applied inbound at the input interface where you configure authentication proxy. The initial display shows the contents of the ACLs prior to authentication. The second display shows the same displays after user authentication with the AAA server.



Note If NAT is configured, the **show ip access list** command might display the translated host IP address for the dynamic ACL entry or the IP address of the host initiating the connection. If the ACL is applied on the NAT outside interface, the translated address is displayed. If the ACL is applied on the NAT inside interface, the IP address of the host initiating the connection is displayed. The **show ip auth-proxy cache** command always displays the IP address of the host initiating the connection.

For example, the following is a list of ACL entries prior to the authentication proxy:

```
Router# show ip access-lists
.
.
.
Extended IP access list 105
 deny tcp any any eq telnet
 deny udp any any
 permit tcp any any (28 matches)
 permit ip any any
```

The following sample output shows a list of ACL entries following user authentication:

```
Router# show ip access-lists
.
.
.
Extended IP access list 105
! The ACL entries following user authentication are shown below.
 permit tcp host 192.168.25.215 any eq 26
 permit icmp host 192.168.25.215 host 60.0.0.2
 permit tcp host 192.168.25.215 any eq telnet
 permit tcp host 192.168.25.215 any eq ftp
 permit tcp host 192.168.25.215 any eq ftp-data
 permit tcp host 192.168.25.215 any eq smtp
 deny tcp any any eq telnet
 deny udp any any
 permit tcp any any (76 matches)
 permit ip any any
```

Deleting Authentication Proxy Cache Entries

When the authentication proxy is in use, dynamic access lists dynamically grow and shrink as authentication entries are added and deleted. To display the list of authentication entries, use the **show ip auth-proxy cache** command. To manually delete an authentication entry, use the **clear ip auth-proxy cache** command in privileged EXEC mode:

| Command | Purpose |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| router# clear ip auth-proxy cache {* host ip address} | Deletes authentication proxy entries from the firewall before they time out. Use an asterisk to delete all authentication cache entries. Enter a specific IP address to delete an entry for a single host. |

Configuration Examples for Authentication Proxy

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

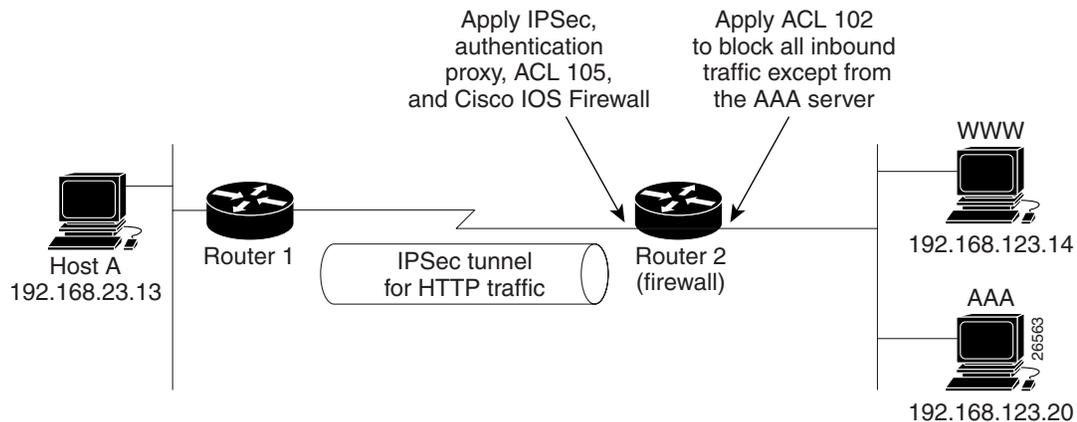
The following example shows a router configuration with the authentication proxy, IPSec, and CBAC features. [Figure 6](#) illustrates the configuration.



Note

If you are using this feature with Cisco IOS software release 12.3(8)T or later, see the [Crypto Access Check on Clear-Text Packets](#) document.

Figure 6 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 $1$E0OB$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

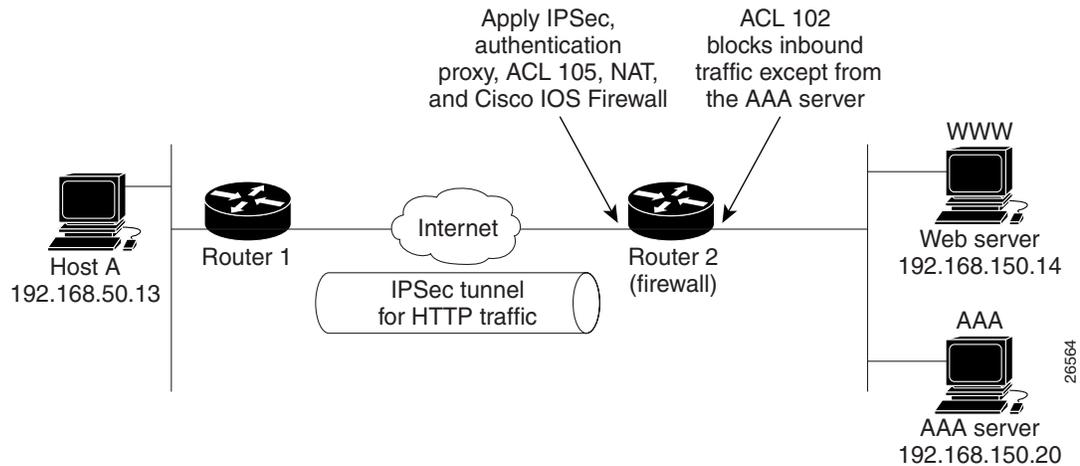
```

```
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 7](#) illustrates the configuration.

Figure 7 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
```
- Click **Submit**.
- Step 4** Click the User Setup icon.
- Click **List All Users**.
  - Add a username.
  - Scroll down to User Setup Password Authentication.
  - Select SDI SecurID Token Card from the Password Authentication drop-down menu.
  - 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"
```

# Additional References

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

## Related Documents

| Related Topic  | Document Title                               |
|----------------|----------------------------------------------|
| Authorization  | <a href="#">“Configuring Authorization”</a>  |
| Authentication | <a href="#">“Configuring Authentication”</a> |
| Accounting     | <a href="#">“Configuring Accounting”</a>     |
| RADIUS         | <a href="#">“Configuring RADIUS”</a>         |
| TACACS+        | <a href="#">“Configuring TACACS+”</a>        |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC                                                    | Title |
|--------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature. | —     |

## 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 Authentication Proxy

Table 3 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

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



**Note**

Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 3** Feature Information for Configuring Authentication

| Feature Name         | Releases | Feature Information                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authentication Proxy | 12.1(5)T | The Cisco IOS Firewall Authentication Proxy feature provides dynamic, per-user authentication and authorization, authenticating users against industry standard TACACS+ and RADIUS authentication protocols. Authenticating and authorizing connections by users provides more robust protection against network attacks. In 12.1(5)T, this feature was introduced on the Cisco IOS. |

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card 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. (0907R)

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

© 2000–2009 Cisco Systems, Inc. All rights reserved.



# Consent Feature for Cisco IOS Routers

---

**First Published: July 19, 2007**

**Last Updated: August 12, 2009**

The Consent Feature for Cisco IOS Routers enables organizations to provide temporary Internet and corporate access to end users through their wired and wireless networks by presenting a consent webpage. This webpage lists the terms and conditions in which the organization is willing to grant requested access to an end user. Users can connect to the network only after they accept the terms of use on the consent webpage.

## Finding Feature Information

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 Consent Feature for Cisco IOS Routers”](#) section on page 12.

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 Consent Feature for Cisco IOS Routers, page 2](#)
- [Information About Consent Feature for Cisco IOS Routers, page 2](#)
- [How to Configure Authentication Proxy Consent, page 4](#)
- [Configuration Examples for Authentication Proxy Consent, page 8](#)
- [Additional References, page 10](#)
- [Feature Information for Consent Feature for Cisco IOS Routers, page 12](#)



---

**Americas Headquarters:**

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

# Prerequisites for Consent Feature for Cisco IOS Routers

To enable a consent webpage, you must be running an Advanced Enterprise image.

## Information About Consent Feature for Cisco IOS Routers

Before enabling the consent feature for Cisco IOS routers, you should understand the following concepts:

- [Authentication Proxy Overview, page 2](#)
- [An Integrated Consent–Authentication Proxy Webpage, page 2](#)

## Authentication Proxy Overview

Authentication proxy is an ingress authentication feature that grants access to an end user (out an interface) only if the user submits valid username and password credentials for an ingress traffic that is destined for HTTP, Telnet, or FTP protocols. After the submitted authentication credentials have been checked against the credentials that are configured on an Authentication, Authorization, Accounting (AAA) server, access is granted to the requester (source IP address).

When an end user posts an HTTP(S), FTP, or Telnet request on a router's authentication-proxy-enabled ingress interface, the Network Authenticating Device (NAD) verifies whether or not the same host has already been authenticated. If a session is already present, the ingress request is not authenticated again, and it is subjected to the dynamic (Auth-Proxy) ACEs and the ingress interface ACEs. If an entry is not present, the authentication proxy responds to the ingress connection request by prompting the user for a valid username and password. When authenticated, the Network Access Profiles (NAPs) that are to be applied are either downloaded from the AAA server or taken from the locally configured profiles.

## An Integrated Consent–Authentication Proxy Webpage

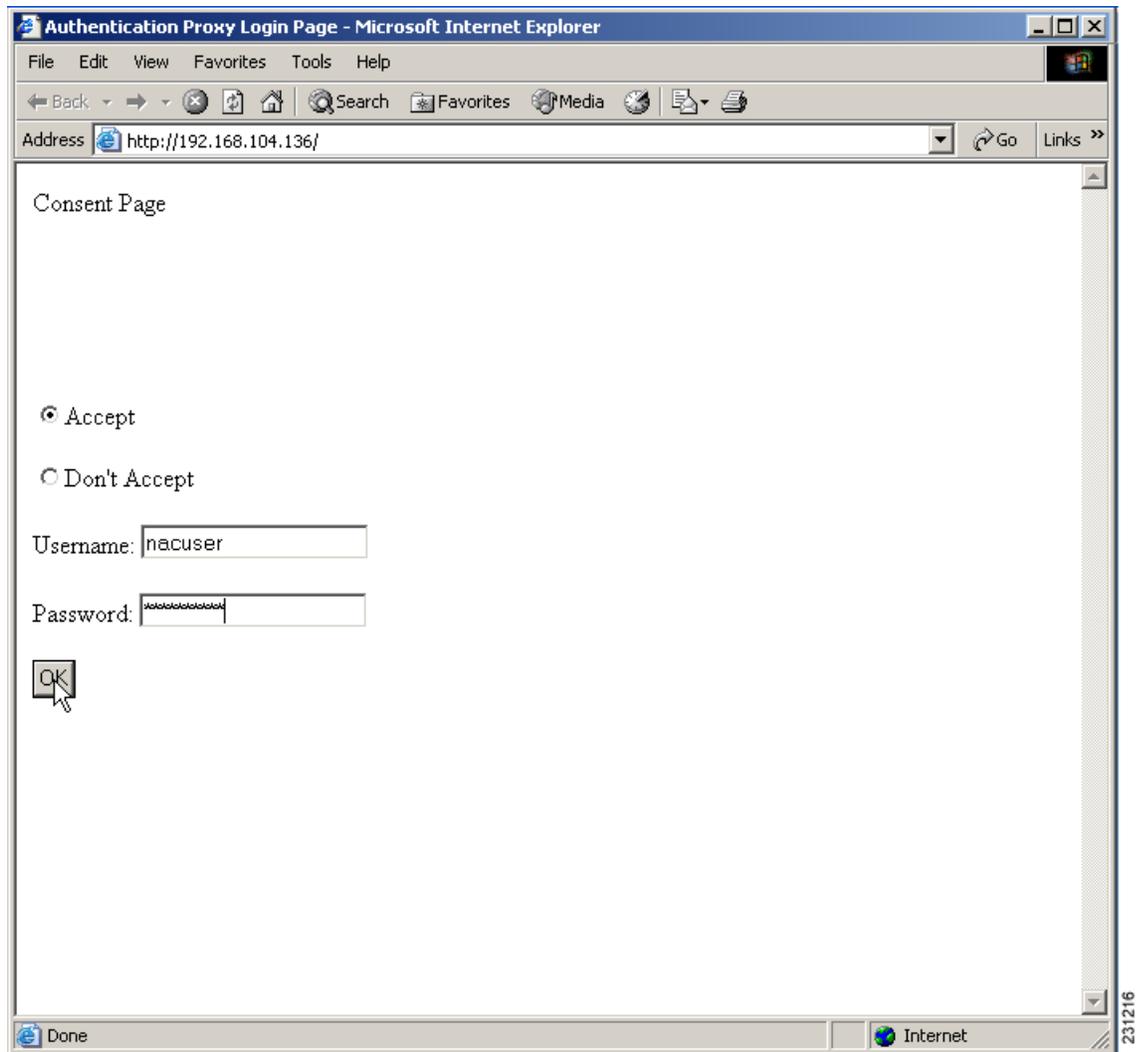
The HTTP authentication proxy webpage has been extended to support radio buttons—“Accept” and “Don't Accept”—for the consent webpage feature. The consent webpage radio buttons are followed by the authentication proxy input fields for a username and a password. (See [Figure 1](#).)

The following consent scenarios are possible:

- If consent is declined (that is, the “Don't Accept” radio button is selected), the authentication proxy radio buttons are disabled. The ingress client session's access will be governed by the default ingress interface ACL.
- If consent is accepted (that is, the “Accept” radio button is selected), the authentication proxy radio buttons are enabled. If the wrong username and password credentials are entered, HTTP-Auth-Proxy authentication will fail. The ingress client session's access will again be governed only by the default ingress interface ACL.
- If consent is accepted (that is, the “Accept” radio button is selected) and valid username and password credentials are entered, HTTP-Auth-Proxy authentication is successful. Thus, one of the following possibilities can occur:
  - If the ingress client session's access request is HTTP\_GET, the destination webpage will open and the ingress client session's access will be governed by the default ingress interface ACL and the dynamic (Auth-Proxy) ACEs.

- If the ingress client session's access request is HTTPS\_GET, a "Security Dialogue Box" will be displayed on the client's browser. If the user selects YES on the Security Dialogue Box window, the destination webpage will open and the ingress client session's access will be governed by the default ingress interface ACL and the dynamic (Auth-Proxy) ACEs. If the user selects NO on the Security Dialogue Box window, the destination page will not open and the user will see the message "Page cannot be displayed." However the ingress client session's access will still be governed by the default ingress interface ACL and the dynamic (Auth-Proxy) ACEs.

**Figure 1** Consent WebPage: Example



**Note**

When HTTP authentication proxy is configured together with the Consent feature, any HTTP authentication proxy-related configurations or policies will override the Consent Page-related configurations or policies. For example, if the **ip admission name admission-name consent** command is configured, the **ip admission consent banner** command is ignored, and only the banner that is configured by the **ip admission auth-proxy-banner** command is shown.

# How to Configure Authentication Proxy Consent

Use the following tasks to configure a consent webpage and enable a consent webpage that is to be displayed to end users:

- [Configuring an IP Admission Rule for Authentication Proxy Consent, page 4](#)
- [Defining a Parameter Map for Authentication Proxy Consent, page 6](#)

## Configuring an IP Admission Rule for Authentication Proxy Consent

Use this task to define the IP admission rule for authentication proxy consent and to associate the rule with an interface.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission name** *admission-name* **consent** [[**absolute-timer** *minutes*] [**event**] [**inactivity-time** *minutes*] [**list** {*acl* \ *acl-name*}] [**parameter-map** *consent-parameter-map-name*]]
4. **ip admission consent banner** [**file** *file-name* | **text** *banner-text*]
5. **interface** *type number*
6. **ip admission** *admission-name*

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Purpose                                                                                                                        |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/>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><br/>Router# configure terminal</p>                                                                                                                                                                                                                                                                                                                                                                                       | <p>Enters global configuration mode.</p>                                                                                       |
| Step 3 | <p><b>ip admission name</b> <i>admission-name</i> <b>consent</b><br/>[[<b>absolute-timer</b> <i>minutes</i>] [<b>event</b>]<br/>[<b>inactivity-time</b> <i>minutes</i>]<br/>[<b>list</b> {<i>acl</i>   <i>acl-name</i>}]<br/>[<b>parameter-map</b> <i>consent-parameter-map-name</i>]]</p> <p><b>Example:</b><br/>Router(config)# ip admission name consent_rule<br/>consent absolute-timer 304 list 103<br/>inactivity-time 204<br/>parameter-map consent_parameter_map</p> | <p>Defines the IP admission rule for authentication proxy consent.</p>                                                         |
| Step 4 | <p><b>ip admission consent banner</b> [<b>file</b> <i>file-name</i>  <br/><b>text</b> <i>banner-text</i>]</p> <p><b>Example:</b><br/>Router(config)# ip admission consent banner<br/>file flash:consent_page.html</p>                                                                                                                                                                                                                                                        | <p>(Optional) Displays a banner in the authentication proxy consent webpage.</p>                                               |
| Step 5 | <p><b>interface</b> <i>type number</i></p> <p><b>Example:</b><br/>Router(config)# interface FastEthernet 0/0</p>                                                                                                                                                                                                                                                                                                                                                             | <p>Specifies the interface in which the consent IP admission rule will be applied and enters interface configuration mode.</p> |
| Step 6 | <p><b>ip admission</b> <i>admission-name</i></p> <p><b>Example:</b><br/>Router(config-if)# ip admission consent_rule</p>                                                                                                                                                                                                                                                                                                                                                     | <p>Applies the IP admission rule created in Step 3 to an interface.</p>                                                        |

## Troubleshooting Tips

To display authentication proxy consent page information on the router, you can use the **debug ip admission consent** command.

```
Router# debug ip admission consent errors
IP Admission Consent Errors debugging is on
```

```
Router# debug ip admission consent events
IP Admission Consent Events debugging is on
```

```
Router# debug ip admission consent messages
IP Admission Consent Messages debugging is on
Router#
Router# show debugging
```

```
IP Admission Consent:
IP Admission Consent Errors debugging is on
IP Admission Consent Events debugging is on
IP Admission Consent Messages debugging is on
```

## Defining a Parameter Map for Authentication Proxy Consent

Use this task to define a parameter map that is to be used for authentication proxy consent.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type consent** *parameter-map-name*
4. **copy** *src-file-name* *dst-file-name*
5. **file** *file-name*
6. **authorize accept identity** *identity-policy-name*
7. **timeout file download** *minutes*
8. **logging enabled**
9. **exit**
10. **show** parameter-map type consent [*parameter-map-name*]

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                     | Purpose                                                                                                                                                                                                              |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/>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><br/>Router# configure terminal</p>                                                                                                | <p>Enters global configuration mode.</p>                                                                                                                                                                             |
| Step 3 | <p><b>parameter-map type consent</b> <i>parameter-map-name</i></p> <p><b>Example:</b><br/>Router(config)# parameter-map type consent consent_parameter_map</p>                        | <p>Defines an authentication proxy consent-specific parameter map and enters parameter-map type consent configuration mode.</p> <p>To use a default policy-map, enter <b>default</b> for the parameter-map-name.</p> |
| Step 4 | <p><b>copy</b> <i>src-file-name</i> <i>dst-file-name</i></p> <p><b>Example:</b><br/>Router(config-profile)# copy tftp://192.168.104.136/consent_page.html flash:consent_page.html</p> | <p>Transfers a file (consent webpage) from an external server to a local file system on your device.</p>                                                                                                             |
| Step 5 | <p><b>file</b> <i>file-name</i></p> <p><b>Example:</b><br/>Router(config-profile)# file flash:consent_page.html</p>                                                                   | <p>(Optional) Specifies a local filename that is to be used as the consent webpage.</p>                                                                                                                              |
| Step 6 | <p><b>authorize accept identity</b> <i>identity-policy-name</i></p> <p><b>Example:</b><br/>Router(config-profile)# authorize accept identity consent_identity_policy</p>              | <p>(Optional) Configures an accept policy.</p> <p><b>Note</b> Currently, only an accept policy can be configured.</p>                                                                                                |
| Step 7 | <p><b>timeout file download</b> <i>minutes</i></p> <p><b>Example:</b><br/>Router(config-profile)# timeout file download 35791</p>                                                     | <p>(Optional) Specifies how often the consent page file should be downloaded from the external TFTP server.</p>                                                                                                      |
| Step 8 | <p>logging enabled</p> <p><b>Example:</b><br/>Router(config-profile)# logging enabled</p>                                                                                             | <p>(Optional) Enables syslog messages.</p>                                                                                                                                                                           |

|         | Command or Action                                                                                                                       | Purpose                                                             |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| Step 9  | <b>exit</b><br><br><b>Example:</b><br>Router(config-profile)# exit<br>Router(config)# exit                                              | Returns to global configuration and privileged EXEC modes.          |
| Step 10 | <b>show parameter-map type consent</b><br><i>[parameter-map-name]</i><br><br><b>Example:</b><br>Router# show parameter-map type consent | (Optional) Displays all or a specified configured consent profiles. |

## Configuration Examples for Authentication Proxy Consent

This section contains the following configuration examples:

- [Ingress Interface ACL and Intercept ACL Configuration: Example, page 8](#)
- [Consent Page Policy Configuration: Example, page 9](#)
- [Parameter Map Configuration: Example, page 9](#)
- [IP Admission Consent Rule Configuration: Example, page 9](#)

### Ingress Interface ACL and Intercept ACL Configuration: Example

The following example shows how to define the ingress interface ACL (via the **ip access-list extended 102** command) to which the consent page policy ACEs will be dynamically appended. This example also shows how to define an intercept ACL (via the **ip access-list extended 103** command) to intercept the ingress interesting traffic by the IP admission consent rule.

```
ip access-list extended 102
 permit ip any 192.168.100.0 0.0.0.255
 permit ip any host 192.168.104.136
 permit udp any any eq bootps
 permit udp any any eq domain
 permit tcp any any eq www
 permit tcp any any eq 443
 permit udp any any eq 443
 exit
!
ip access-list extended 103
 permit ip any host 192.168.104.136
 permit udp any host 192.168.104.132 eq domain
 permit tcp any host 192.168.104.136 eq www
 permit udp any host 192.168.104.136 eq 443
 permit tcp any host 192.168.104.136 eq 443
 exit
!
```

## Consent Page Policy Configuration: Example

The following example shows how to configure the consent page policy ACL and the consent page identity policy:

```
ip access-list extended consent-pg-ip-acc-group
 permit ip any host 192.168.104.128
 permit ip any host 192.168.104.136
 exit
!
identity policy consent_identity_policy
 description ### Consent Page Identity Policy ###
 access-group consent-pg-ip-acc-group
 exit
```

## Parameter Map Configuration: Example

The following example shows how to define the consent-specific parameter map “consent\_parameter\_map” and a default consent parameter map:

```
parameter-map type consent consent_parameter_map
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity consent_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
parameter-map type consent default
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity test_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
```

## IP Admission Consent Rule Configuration: Example

The following example shows how to configure an IP admission consent rule, which includes the consent page parameter map as defined the in the “[Parameter Map Configuration: Example](#)” section:

```
ip admission name consent-rule consent inactivity-time 204 absolute-timer 304 param-map
 consent_parameter_map list 103
ip admission consent-banner file flash:consent_page.html
ip admission consent-banner text ^C Consen-Page-Banner-Text ^C
ip admission max-login-attempts 5
ip admission init-state-timer 15
ip admission auth-proxy-audit
ip admission inactivity-timer 205
ip admission absolute-timer 305
ip admission ratelimit 100
ip http server
ip http secure-server
!
interface FastEthernet 0/0
 description ### CLIENT-N/W ###
 ip address 192.168.100.170 255.255.255.0
 ip access-group 102 in
```

```
ip admission consent-rule
no shut
exit
!
interface FastEthernet 0/1
description ### AAA-DHCP-AUDIT-SERVER-N/W ###
ip address 192.168.104.170 255.255.255.0
no shut
exit
!
line con 0
exec-timeout 0 0
login authentication noAAA
exit
!
line vty 0 15
exec-timeout 0 0
login authentication noAAA
exit
!
```

## Additional References

The following sections provide references related to the Consent Feature for Cisco IOS Routers feature.

## Related Documents

| Related Topic                                       | Document Title                                                              |
|-----------------------------------------------------|-----------------------------------------------------------------------------|
| Additional authentication proxy configuration tasks | See the “ <a href="#">Configuring Authentication Proxy</a> ” feature module |

## Standards

| Standard | Title |
|----------|-------|
| None     | —     |

## MIBs

| MIB  | MIBs Link                                                                                                                                                                                                                  |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC  | Title |
|------|-------|
| None | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <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 Consent Feature for Cisco IOS Routers

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 Consent Feature for Cisco IOS Routers

| Feature Name                          | Releases  | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Consent Feature for Cisco IOS Routers | 12.4(15)T | <p>The Consent Feature for Cisco IOS Routers enables organizations to provide temporary Internet and corporate access to end users through their wired and wireless networks by presenting a consent webpage. This webpage lists the terms and conditions in which the organization is willing to grant requested access to an end user. Users can connect to the network only after they accept the terms of use on the consent webpage.</p> <p>In Cisco IOS Release 12.4(15)T, this feature was introduced.</p> <p>The following commands were introduced or modified:<br/> <b>authorize accept identity, copy (consent-parameter-map), debug ip admission consent, file (consent-parameter-map), ip admission consent banner, ip admission name, logging enabled, parameter-map type, show ip admission, timeout file download</b></p> |

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card 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. (0907R)

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.





# Firewall Authentication Proxy for FTP and Telnet Sessions

---

**First Published: May 14, 2003**

**Last Updated: August 13, 2009**

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.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Firewall Authentication Proxy for FTP and Telnet Session” section on page 18](#).

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 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 16](#)
- [Feature Information for Firewall Authentication Proxy for FTP and Telnet Session, page 18](#)



---

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

# 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

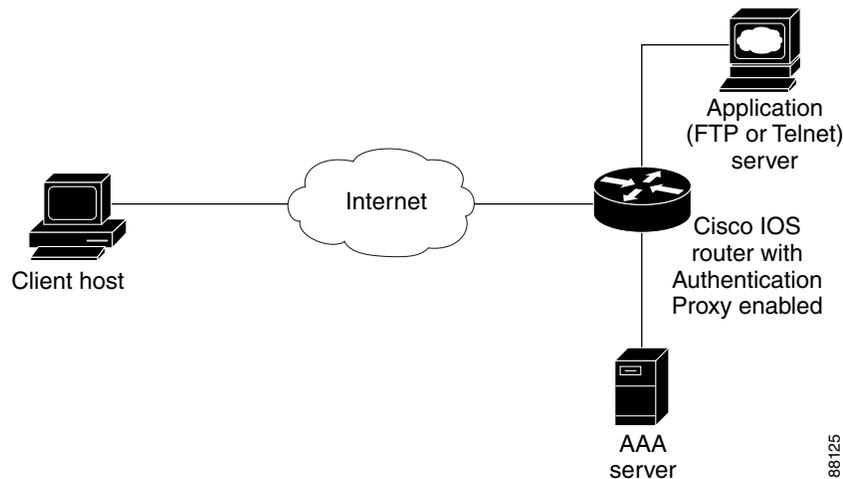
Authentication proxy for FTP and Telnet Sessions functions like authentication proxy for HTTP; that is, FTP and Telnet are independent components in the Cisco IOS software and can be enabled or disabled on the interface of an unauthenticated host.

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



88125

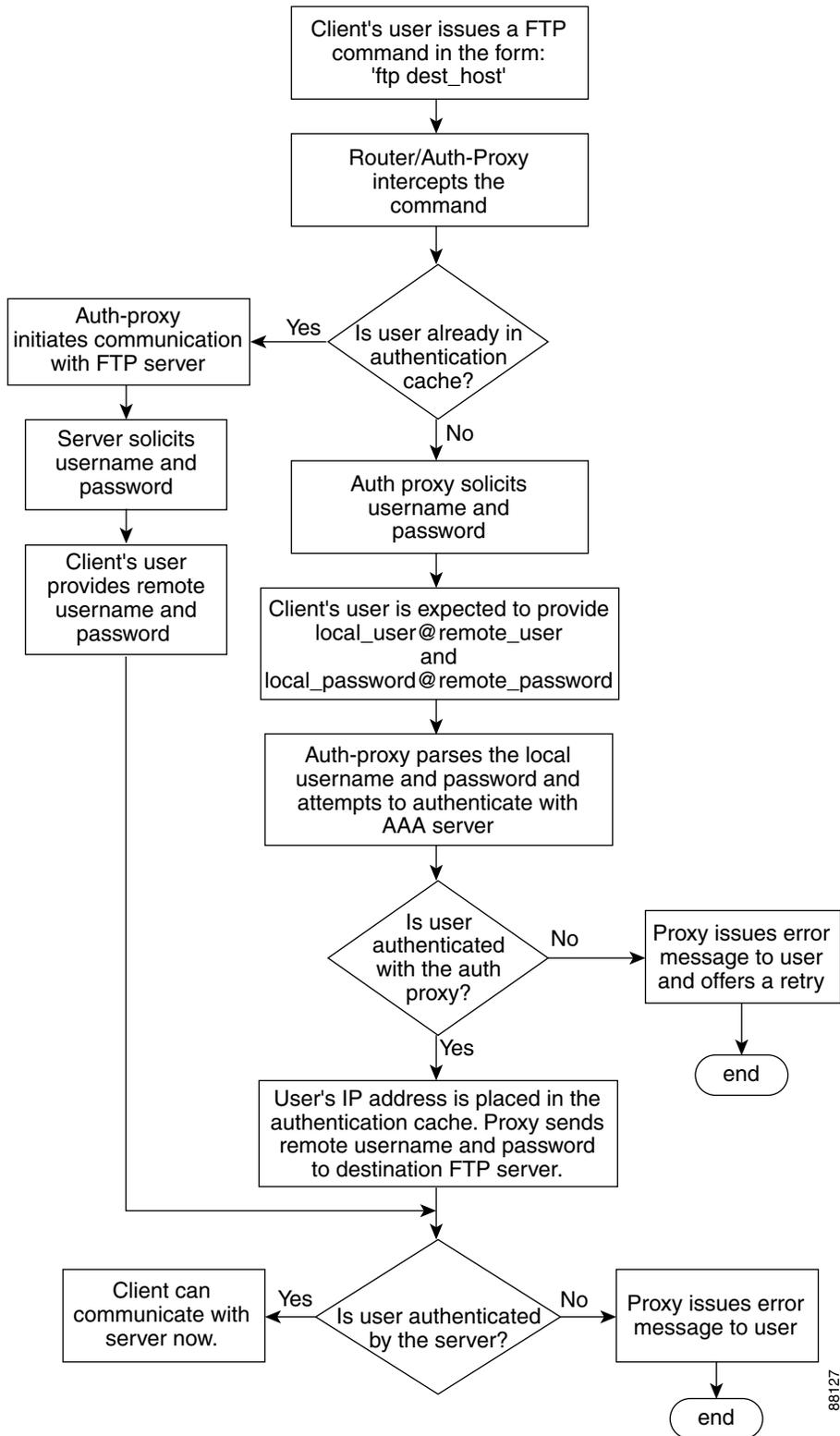
Just as with HTTP, the authentication proxy router intercepts traffic that is sent from the client host. Upon receiving a FTP or Telnet packet, the router will look into its authentication cache to check whether the client host has already been authenticated. If it has been authenticated, the router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



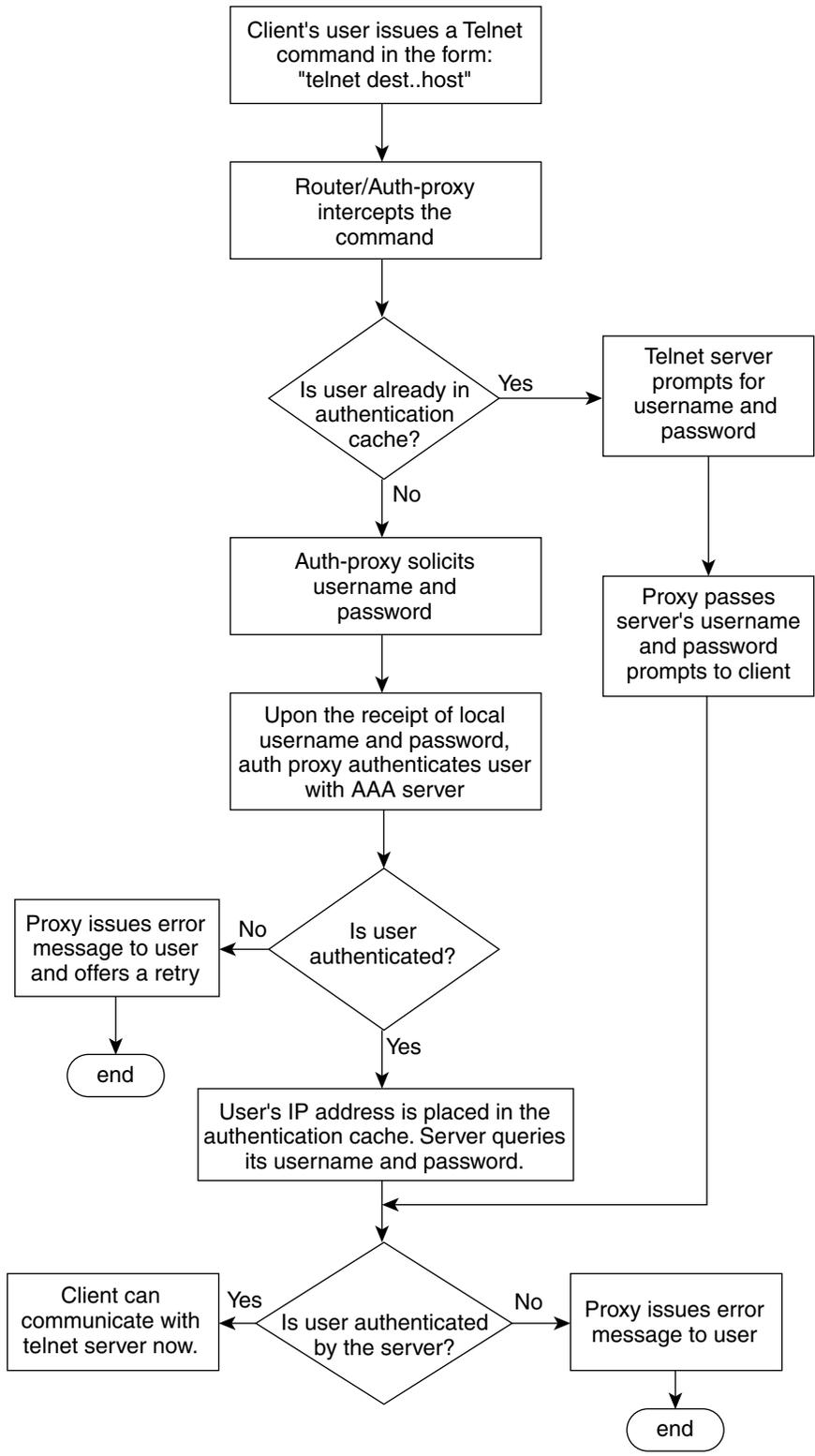
88127

## 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 (through the **ip auth-proxy name** command) or globally (through 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><br><br><b>Example:</b><br>Router> enable                                                                                                                                  | Enables higher privilege levels, such as privileged EXEC mode.<br><br>Enter your password if prompted. |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                          | Enters global configuration mode.                                                                      |
| Step 3 | <b>aaa new-model</b><br><br><b>Example:</b><br>Router (config)# aaa new-model                                                                                                           | Enables the AAA functionality on the router.                                                           |
| Step 4 | <b>aaa authentication login default group tacacs+ group radius</b><br><br><b>Example:</b><br>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]]<br><br><b>Example:</b><br>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]<br><br><b>Example:</b><br>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><br/>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><br/>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><br/>Router (config)# ip auth-proxy<br/>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><br/>Router (config)# ip auth-proxy<br/>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>]<br/>[<i>absolute-timer min</i>] [<i>list {acl   acl-name}</i>]</b></p> <p><b>Example:</b><br/>Router (config)# ip auth-proxy name ftp_list1<br/>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 through 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><br><br><b>Example:</b><br>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><br><br><b>Example:</b><br>Router(config-if)# ip auth-proxy authproxyrule | In interface configuration mode, applies the named authentication proxy rule at the interface.<br><br>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><br><br><b>Example:</b><br>Router> enable                                                     | Enables higher privilege levels, such as privileged EXEC mode.<br><br>Enter your password if prompted.                                                                                                                                                                                                                       |
| Step 2 | <b>show ip auth-proxy configuration</b><br><br><b>Example:</b><br>Router# show ip auth-proxy configuration | Displays the current authentication proxy configuration.                                                                                                                                                                                                                                                                     |
| Step 3 | <b>show ip auth-proxy cache</b><br><br><b>Example:</b><br>Router# show ip auth-proxy cache                 | Displays the list of user authentication entries.<br><br>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><br><br><b>Example:</b><br>Router> enable                                                                                                                       | Enables higher privilege levels, such as privileged EXEC mode.<br><br>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><br><br><b>Example:</b><br>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, page 13](#)
- [Livingston RADIUS User Profiles: Example, page 14](#)
- [Ascend RADIUS User Profiles: Example, page 15](#)

### 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 references related to the Firewall Authentication Proxy for FTP and Telnet Sessions feature.

### Related Documents

| Related Topic                                       | Document Title                                                                                                              |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Additional authentication proxy configuration tasks | <a href="#">“Configuring Authentication Proxy”</a>                                                                          |
| Additional authentication proxy commands            | <a href="#">Cisco IOS Security Command Reference</a>                                                                        |
| RADIUS and TACACS+ configuration information        | <a href="#">“Configuring RADIUS”</a> and <a href="#">“Configuring TACACS+”</a>                                              |
| RADIUS and TACACS+ attribute information            | <a href="#">“RADIUS Attributes Overview and RADIUS IETF Attributes”</a> and <a href="#">“TACACS+ Attribute-Value Pairs”</a> |
| Additional authentication proxy information         | <a href="#">“Firewall Support of HTTPS Authentication Proxy”</a>                                                            |

### Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

### MIBs

| MIBs | MIBs Link                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><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 Firewall Authentication Proxy for FTP and Telnet Session

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 Firewall Authentication Proxy for FTP and Telnet Sessions

| Feature Name                                              | Releases | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Firewall Authentication Proxy for FTP and Telnet Sessions | 12.3(1)  | <p>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.</p> <p>This feature was introduced in Cisco IOS Release 12.3(1).</p> <p>The following commands were introduced or modified:<br/> <b>debug ip auth-proxy</b>, <b>ip auth-proxy</b>, <b>ip auth-proxy auth-proxy-banner</b>, <b>ip auth-proxy name</b>.</p> |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card 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. (0907R)

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.



# Firewall Support of HTTPS Authentication Proxy

---

**First Published: December 23, 2002**

**Last Updated: August 13, 2009**

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.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Firewall Support of HTTPS Authentication Proxy”](#) section on [page 15](#).

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 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 13](#)
- [Feature Information for Firewall Support of HTTPS Authentication Proxy, page 15](#)
- [Glossary, page 16](#)



---

**Americas Headquarters:**

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

# 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.

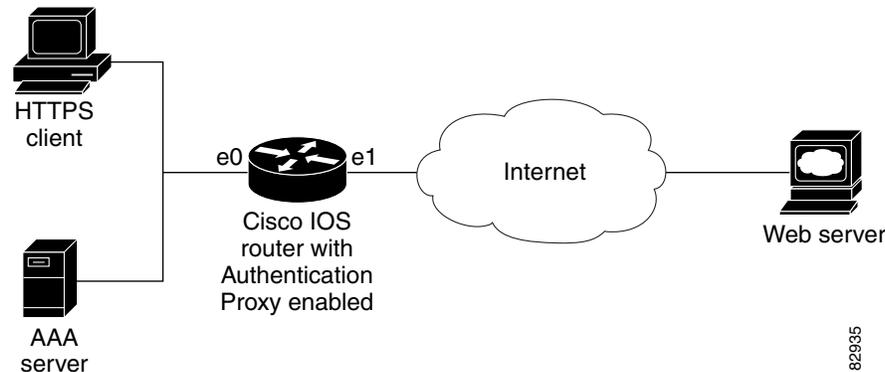
When authentication proxy is enabled on a Cisco router, users can log into the network or access the Internet via HTTP(S). When a user initiates an HTTP(S) session through the firewall, the authentication proxy is triggered. Authentication proxy first checks to see if the user has been authenticated. 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 1 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 1** *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, the authentication proxy for AAA services must be configured by enabling AAA and configuring a RADIUS or TACACS+ server. The certification authority (CA) certificate must also be obtained. See [“Related Documents” section on page 13](#) for more information on these tasks.

### 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 | <code>enable</code><br><br><b>Example:</b><br>Router> <code>enable</code>                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br>Router# <code>configure terminal</code> | Enters global configuration mode.                                                                                   |

|        | Command or Action                                                                                                      | Purpose                                                                                                                                                                                        |
|--------|------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <code>ip http server</code><br><br><b>Example:</b><br>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 | <code>ip http authentication aaa</code><br>Router (config)# ip http authentication aaa                                 | Sets the HTTP server authentication method to AAA.                                                                                                                                             |
| Step 5 | <code>ip http secure-server</code><br><br><b>Example:</b><br>Router (config)# ip http secure-server                    | Enables HTTPS.                                                                                                                                                                                 |
| Step 6 | <code>ip http secure-trustpoint name</code><br><br><b>Example:</b><br>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). See [“Related Documents” section on page 13](#) for more information on these tasks.

## Verifying HTTPS Authentication Proxy

To verify your HTTPS authentication proxy configuration, perform the following optional steps:

### SUMMARY STEPS

1. `enable`
2. `show ip auth-proxy configuration`
3. `show ip auth-proxy cache`
4. `show ip http server secure status`

### DETAILED STEPS

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

|        | Command or Action                                                                                            | Purpose                                                                                                                                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>show ip auth-proxy cache</b><br><br><b>Example:</b><br>Router# show ip auth-proxy cache                   | Displays the list of user authentication entries.<br><br>The authentication proxy cache lists the host IP address, the source port number, the timeout value for the authentication proxy, and the state of the connection. If the authentication proxy state is HTTP_ESTAB, the user authentication was successful. |
| Step 4 | <b>show ip http server secure status</b><br><br><b>Example:</b><br>Router# show ip http server secure status | Displays HTTPS status.                                                                                                                                                                                                                                                                                               |

## Monitoring Firewall Support of HTTPS Authentication Proxy

Perform the following task to troubleshoot your HTTPS authentication proxy configuration:

### SUMMARY STEPS

1. **enable**
2. **debug ip auth-proxy detailed**

### DETAILED STEPS

|        | Command or Action                                                                                              | Purpose                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>Example:</b><br>debug ip auth-proxy detailed<br><br><b>Example:</b><br>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 9](#)
- [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
 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 E076EB60
BF789728 5ED0D5FC 2C
quit
certificate 55A4795100000000000D
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 DEEEB73E 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:Protocol not configured on if_input
*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: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

The following sections provide references related to the Firewall Support of HTTPS Authentication Proxy feature.

### Related Documents

| Related Topic                                                   | Document Title                                                               |
|-----------------------------------------------------------------|------------------------------------------------------------------------------|
| Authentication proxy configuration tasks                        | <a href="#">“Configuring Authentication Proxy”</a>                           |
| Authentication proxy commands                                   | <a href="#">Cisco IOS Security Command Reference</a>                         |
| Information on adding HTTPS support to the Cisco IOS web server | <a href="#">“HTTPs - HTTP Server and Client with SSL 3.0”</a>                |
| Information on configuring and obtaining a CA certificate.      | <a href="#">“Trustpoint CLI”</a> , Cisco IOS Release 12.2(8)T feature module |

### Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

### MIBs

| MIBs | MIBs Link                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

### RFCs

| RFCs <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                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <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 Firewall Support of HTTPS Authentication Proxy

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://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 Firewall Support of HTTPS Authentication Proxy

| Feature Name                                   | Releases                | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Firewall Support of HTTPS Authentication Proxy | 12.2(11)YU<br>12.2(15)T | <p>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.</p> <p>This feature was introduced in Cisco IOS Release 12.2(11)YU.</p> <p>This feature was integrated in Cisco IOS Release 12.2(15)T.</p> |

# 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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card 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. (0907R)

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.



# Transparent Bridging Support for Authentication Proxy

---

**First Published: June 29, 2007**  
**Last Updated: October 9, 2009**

The Transparent Bridging Support for Authentication Proxy feature allows network administrators to configure transparent authentication proxy on existing networks without having to reconfigure the statically defined IP addresses of their network-connected devices. The result is that security policies are dynamically authenticated and authorized on a per user basis, which eliminates the tedious and costly overhead required to renumber devices on the trusted network.

Authentication proxy rules on bridged interfaces can coexist with router interfaces on the same device, whenever applicable, which allows administrators to deploy different authentication proxy rules on bridged and routed domains.

## 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 Transparent Authentication Proxy”](#) 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.

## Contents

- [Restrictions for Transparent Bridging Support for Authentication Proxy, page 2](#)
- [Information About Transparent Bridging Support for Authentication Proxy, page 2](#)
- [How to Configure Transparent Authentication Proxy, page 2](#)
- [Configuration Examples for Transparent Authentication Proxy, page 3](#)



---

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

- [Additional References, page 8](#)
- [Feature Information for Transparent Authentication Proxy, page 10](#)

## Restrictions for Transparent Bridging Support for Authentication Proxy

Authentication Proxy is not supported on vLAN trunk interfaces that are configured in a bridge group.

## Information About Transparent Bridging Support for Authentication Proxy

Authentication proxy provides dynamic, per-user authentication and authorization of network access connections to enforce security policies. Typically, authentication proxy is a Layer 3 functionality that is configured on routed interfaces with different networks and IP subnets on each interface.

Integrating authentication proxy with transparent bridging enables network administrators to deploy authentication proxy on an existing network without impacting the existing network configuration and IP address assignments of the hosts on the network.

### Transparent Bridging Overview

If configured for bridging, a Cisco IOS device can bridge any number of interfaces. The device can complete basic bridging tasks such as learning MAC addresses on ports to restrict collision domains and running Spanning Tree Protocol (STP) to prevent looping in the topology.

Within bridging, a user can configure Integrated Routed Bridging (IRB), which allows a device to bridge on some interfaces while a Layer 3 Bridged Virtual Interface (BVI) is presented for routing. The bridge can determine whether the packet is to be bridged or routed on the basis of the destination of the Layer 2 or Layer 3 IP address in the packet. Configured with an IP address, the BVI can manage the device even if no interface is configured for routing.

## How to Configure Transparent Authentication Proxy

To configure authentication proxy on bridged interfaces, you must configure the interface in a bridge group and apply an authentication proxy rule on the interface. You must also set up and configure the authentication, authorization, and accounting (AAA) server (Cisco ACS) for authentication proxy. For examples on how to configure authentication proxy on a bridged interface, see the section, [“Configuration Examples for Transparent Authentication Proxy” section on page 3.](#)

# Configuration Examples for Transparent Authentication Proxy

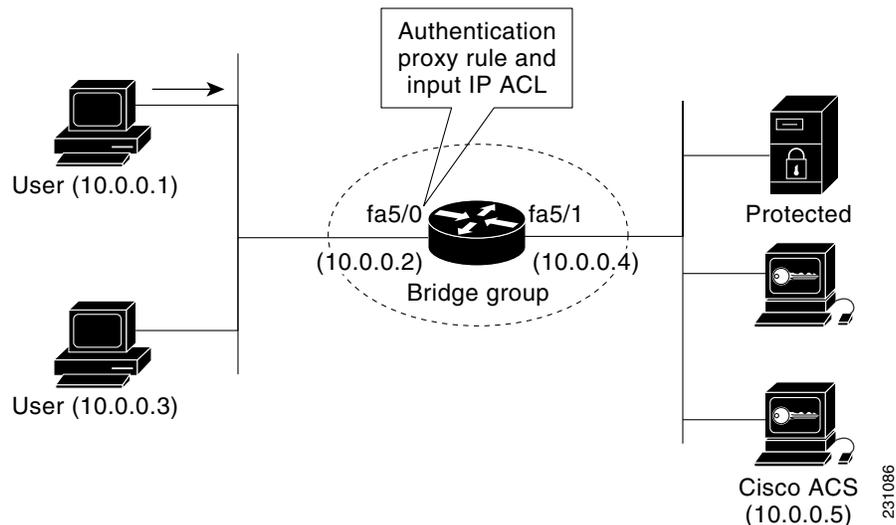
This section contains the following configuration examples, which show how to configure authentication proxy on a bridged interface:

- [Authentication Proxy in Transparent Bridge Mode: Example, page 3](#)
- [Authentication Proxy in Concurrent Route Bridge Mode: Example, page 4](#)
- [Authentication Proxy in Integrated Route Bridge Mode: Example, page 6](#)

## Authentication Proxy in Transparent Bridge Mode: Example

The following example (see [Figure 1](#)) shows how to configure authentication proxy in a transparent bridged environment in which network users (that is, hosts on the bridged interface FastEthernet 5/0) are challenged for user credentials before being given access to protected resources.

**Figure 1** Authentication Proxy in Transparent Bridging Mode: Sample Topology



```

aaa new-model
!
aaa authentication login default group radius
aaa authorization auth-proxy default group radius
aaa accounting auth-proxy default start-stop group radius
!
no ip routing
!
!
no ip cef
!
!
ip auth-proxy name AuthRule http inactivity-time 60
!
interface FastEthernet5/0
 ip address 10.0.0.2 255.255.255.0
 ip auth-proxy AuthRule
 ip access-group 100 in
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1

```

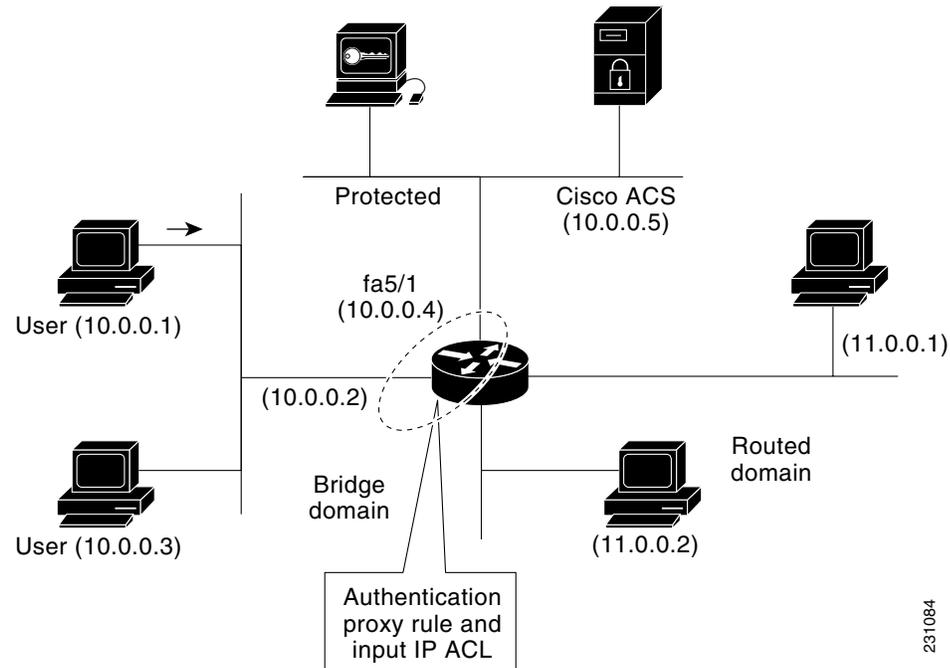
```
!
interface FastEthernet5/1
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
!
ip http server
ip http secure-server
!
radius-server host 10.0.0.5 auth-port 1645 acct-port 1646
radius-server key cisco
!
bridge 1 protocol ieee
!
Router# show ip auth-proxy cache

Authentication Proxy Cache
Client Name AuthRule, Client IP 10.0.0.1, Port 1100,
 timeout 60, Time Remaining 60, state ESTAB
```

## Authentication Proxy in Concurrent Route Bridge Mode: Example

Concurrent routing and bridging configuration mode allows routing and bridging to occur in the same router; however, the given protocol is not switched between the two domains. Instead, routed traffic is confined to the routed interfaces and bridged traffic is confined to the bridged interfaces.

The following example (see [Figure 2](#)) shows how to configure authentication proxy in a concurrent routing and bridging environment in which network users (that is, hosts on the bridged interface FastEthernet 5/0) are challenged for user credentials before being given access to protected resources.

**Figure 2 Authentication Proxy in Concurrent Route Bridge Mode: Sample Topology**

```

aaa new-model
!
aaa authentication login default group radius
aaa authorization auth-proxy default group radius
aaa accounting auth-proxy default start-stop group radiusb
!
ip cef
!
bridge crb
!
ip auth-proxy name AuthRule http inactivity-time 60
!
interface FastEthernet5/0
 ip address 10.0.0.2 255.255.255.0
 ip auth-proxy AuthRule
 ip access-group 100 in
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
!
interface FastEthernet5/1
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
!
ip http server
ip http secure-server
!
radius-server host 10.0.0.5 auth-port 1645 acct-port 1646
radius-server key cisco
!

```

```

bridge 1 protocol ieee
!
Router# show ip auth-proxy cache

Authentication Proxy Cache
Client Name AuthRule, Client IP 10.0.0.1, Port 1145,
timeout 60, Time Remaining 60, state ESTAB

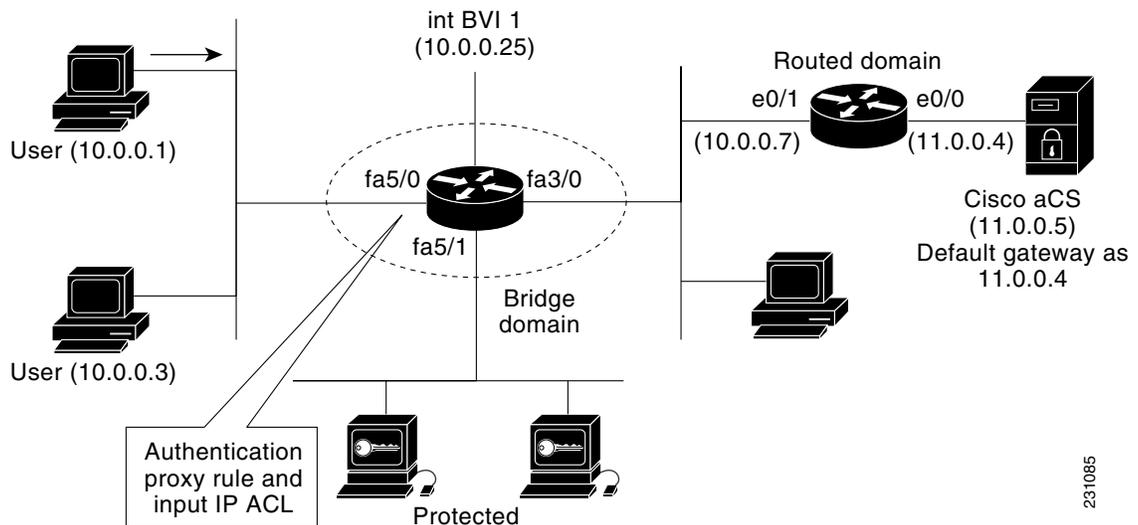
```

## Authentication Proxy in Integrated Route Bridge Mode: Example

In an integrated routing and bridging environment, a bridged network is interconnected with a router network. Both routing and bridging can occur in the same router with connectivity between routed and bridged domains.

The following example (see [Figure 3](#)) shows how to configure authentication proxy in an integrated routing and bridging environment in which network users (that is, hosts on the bridged interface FastEthernet 5/0) are challenged for user credentials before being given access to protected resources.

**Figure 3** Authentication Proxy in Integrated Route Bridge Mode: Sample Topology



```

!
aaa new-model
!
aaa authentication login default group radius
aaa authorization auth-proxy default group radius
aaa accounting auth-proxy default start-stop group radius
!
ip cef
!
ip auth-proxy name AuthRule http inactivity-time 60
!
bridge irb
!
interface FastEthernet3/0
no ip address
duplex half
bridge-group 1
!

```

231085

```
interface FastEthernet5/0
 no ip address
 ip auth-proxy AuthRule
 ip access-group 100 in
 duplex auto
 speed auto
 bridge-group 1
!
interface FastEthernet5/1
 no ip address
 duplex auto
 speed auto
 bridge-group 1
!
interface BVI1
 ip address 10.0.0.25 255.255.255.0
!
!
ip route 11.0.0.0 255.255.255.0 10.0.0.7
!
ip http server
ip http secure-server
!
radius-server host 11.0.0.5 auth-port 1645 acct-port 1646
radius-server key cisco
!
bridge 1 protocol ieee
bridge 1 route ip
!
Router# show ip auth-proxy cache

Authentication Proxy Cache
Client Name AuthRule, Client IP 10.0.0.1, Port 1100,
 timeout 60, Time Remaining 60, state ESTAB
```

## Additional References

The following sections provide references related to the Transparent Bridging Support for Authentication Proxy feature.

### Related Documents

| Related Topic                 | Document Title                                       |
|-------------------------------|------------------------------------------------------|
| Authentication proxy commands | <a href="#">Cisco IOS Security Command Reference</a> |
| Bridging commands             | <a href="#">Cisco IOS Bridging 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:<br><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 Transparent Authentication Proxy

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://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 Transparent Authentication Proxy

| Feature Name                                          | Releases  | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Transparent Bridging Support for Authentication Proxy | 12.4(15)T | <p>The Transparent Bridging Support for Authentication Proxy feature allows network administrators to configure transparent authentication proxy on existing networks without having to reconfigure the statically defined IP addresses of their network-connected devices. The result is that security policies are dynamically authenticated and authorized on a per user basis, which eliminates the tedious and costly overhead required to renumber devices on the trusted network.</p> <p>Authentication proxy rules on bridged interfaces can coexist with router interfaces on the same device, whenever applicable, which allows administrators to deploy different authentication proxy rules on bridged and routed domains.</p> <p>This feature was introduced in Cisco IOS Release 12.4(15)T.</p> |

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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.





## **Security Server Protocols**





**RADIUS**





# Configuring RADIUS

---

**First Published: July 27, 1998**

**Last Updated: October 16, 2009**

The Remote Authentication Dial-In User Service (RADIUS) security system 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.

## 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 RADIUS](#)” section on page 34.

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

- [Information About RADIUS](#), page 2
- [How to Configure RADIUS](#), page 4
- [Monitoring and Maintaining RADIUS](#), page 21
- [RADIUS Attributes](#), page 3
- [Configuration Examples for RADIUS](#), page 22
- [Additional References](#), page 32
- [Feature Information for Configuring RADIUS](#), page 34



---

**Americas Headquarters:**

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

# Information About RADIUS

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 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, see the [“Related Documents” section on page 32](#) for more information.

This section includes the following sections:

- [Vendor-Proprietary RADIUS Attributes, page 3](#)
- [RADIUS Tunnel Attributes, page 3](#)

## 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. See the [“Related Documents” section on page 32](#) for more information.

## 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. See the “[Related Documents](#)” section on page 5 for more information.

See also the following configuration examples:

- [RADIUS User Profile with RADIUS Tunneling Attributes: Example, page 28](#)
- [L2TP Access Concentrator: Examples, page 29](#)
- [L2TP Network Server: Examples, page 30](#)

See “[Related Documents](#)” section on page 32 for more information about L2F, L2TP, VPN, or VPDN.

## How to Configure RADIUS

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.
- Use the **aaa authentication** global configuration command to define method lists for RADIUS authentication. For more information about using the **aaa authentication** command, see the “[Configuring Authentication](#)” module.
- Use **line** and **interface** commands to enable the defined method lists to be used. For more information, see the “[Configuring Authentication](#)” module.

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, see “[Configuring AAA Server Groups](#)” section on page 10.
- 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, see “[Configuring AAA Server Group Selection Based on DNIS](#)” section on page 12.
- You may use the **aaa authorization** global command to authorize specific user functions. For more information about using the **aaa authorization** command, see the “[Configuring Authorization](#)” module.
- You may use the **aaa accounting** command to enable accounting for RADIUS connections. For more information about using the **aaa accounting** command, see the “[Configuring Accounting](#)” module.
- 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, see “[Configuring Suffix and Password in RADIUS Access Requests](#)” section on page 21.

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, page 5](#) (Required)

- [Configuring Router to Use Vendor-Specific RADIUS Attributes, page 7 \(Optional\)](#)
- [Configuring Router for Vendor-Proprietary RADIUS Server Communication, page 8 \(Optional\)](#)
- [Configuring Router to Query RADIUS Server for Static Routes and IP Addresses, page 8 \(Optional\)](#)
- [Configuring Router to Expand Network Access Server Port Information, page 9 \(Optional\)](#)
- [Configuring AAA Server Groups, page 10 \(Optional\)](#)
- [Configuring AAA Server Groups with Deadtime, page 11 \(Optional\)](#)
- [Configuring AAA DNIS Authentication, page 11](#)
- [Configuring AAA Server Group Selection Based on DNIS, page 12 \(Optional\)](#)
- [Configuring AAA Preauthentication, page 13](#)
- [Configuring a Guard Timer, page 19](#)
- [Specifying RADIUS Authentication, page 19](#)
- [Specifying RADIUS Authorization, page 20 \(Optional\)](#)
- [Specifying RADIUS Accounting, page 20 \(Optional\)](#)
- [Configuring RADIUS Login-IP-Host, page 20 \(Optional\)](#)
- [Configuring RADIUS Prompt, page 20 \(Optional\)](#)
- [Configuring Suffix and Password in RADIUS Access Requests, page 21 \(Optional\)](#)

For RADIUS configuration examples using the commands in this module, refer to the section “[Configuration Examples for RADIUS](#)” section on [page 22](#).

## 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 port-number</b> option to configure a specific UDP port on this RADIUS server to be used solely for authentication. Use the <b>acct-port port-number</b> 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 | Router(config)# <b>radius-server key</b> {0 string   7 string   string} | 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 | Router(config)# <b>radius-server retransmit</b> retries                 | Specifies how many times the router transmits each RADIUS request to the server before giving up (the default is 3).                                                                                                               |
| Step 3 | Router(config)# <b>radius-server timeout</b> seconds                    | Specifies for how many seconds a router waits for a reply to a RADIUS request before retransmitting the request.                                                                                                                   |
| Step 4 | Router(config)# <b>radius-server deadtime</b> minutes                   | Specifies for how many minutes a RADIUS server that is not responding to authentication requests is passed over by requests for RADIUS authentication.                                                                             |

## Configuring Router to Use Vendor-Specific RADIUS Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option has vendor-type 1, which is named "cisco-avpair." The value is a string of the following format:

```
protocol : attribute sep value *
```

"Protocol" is a value of the Cisco "protocol" attribute for a particular type of authorization; protocols that can be used include IP, IPX, VPDN, VOIP, SHELL, RSVP, SIP, AIRNET, OUTBOUND. "Attribute" and "value" are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification, and "sep" is "=" for mandatory attributes and "\*" for optional attributes. This allows the full set of features available for TACACS+ authorization to also be used for RADIUS.

For example, the following AV pair causes Cisco's "multiple named ip address pools" feature to be activated during IP authorization (during PPP's IPCP address assignment):

```
cisco-avpair= "ip:addr-pool=first"
```

If you insert an "\*", the AV pair "ip:addr-pool=first" becomes optional. Note that any AV pair can be made optional.

```
cisco-avpair= "ip:addr-pool*first"
```

The following example shows how to cause a user logging in from a network access server to have immediate access to EXEC commands:

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

Other vendors have their own unique vendor-IDs, options, and associated VSAs. For more information about vendor-IDs and VSAs, see ["RFCs" section on page 32](#).

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><br>[ <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, see the [“Related Documents” section on page 32](#) for more information.

## 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                                                                                                                                                                                                      |
|---------------|----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>radius-server host</b><br>{ <i>hostname</i>   <i>ip-address</i> } <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.                                                        |
| <b>Step 2</b> | Router(config)# <b>radius-server key</b> { <i>0 string</i>  <br><i>7 string</i>   <i>string</i> }        | 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 [accounting   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 information about RADIUS attributes and RADIUS port identification for PPP, see the [“Related Documents” section on page 32](#) for more information.

## 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 | <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> | Specifies and defines the IP address of the server host before configuring the AAA server-group. See <a href="#">“Configuring Router to RADIUS Server Communication” section on page 5</a> for more information on the <b>radius-server host</b> command.                                                                                         |
| Step 2 | <pre>Router(config-if)# aaa group server {radius   tacacs+} group-name</pre>                                                                                                                              | 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 | <pre>Router(config-sg)# server ip-address [auth-port port-number] [acct-port port-number]</pre>                                                                                                           | <p>Associates a particular RADIUS server with the defined server group. Each security server is identified by its IP address and UDP port number.</p> <p>Repeat this step for each RADIUS server in the AAA server group.</p> <p><b>Note</b> Each server in the group must be defined previously using the <b>radius-server host</b> command.</p> |

## Configuring AAA Server Groups with Deadtime

After you have configured a server host with a server name, you can use the **deadtime** command to configure each server per server group. Configuring deadtime within a server group allows you to direct AAA traffic to separate groups of servers that have different operational characteristics.

Configuring deadtime is no longer limited to a global configuration. A separate timer has been attached to each server host in every server group. Therefore, when a server is found to be unresponsive after numerous retransmissions and timeouts, the server is assumed to be dead. The timers attached to each server host in all server groups are triggered. In essence, the timers are checked and subsequent requests to a server (once it is assumed to be dead) are directed to alternate timers, if configured. When the network access server receives a reply from the server, it checks and stops all configured timers (if running) for that server in all server groups.

If the timer has expired, only the server to which the timer is attached is assumed to be alive. This becomes the only server that can be tried for later AAA requests using the server groups to which the timer belongs.



**Note**

Since one server has different timers and may have different deadtime values configured in the server groups, the same server may in the future have different states (dead and alive) at the same time.



**Note**

To change the state of a server, you must start and stop all configured timers in all server groups.

The size of the server group will be slightly increased because of the addition of new timers and the deadtime attribute. The overall impact of the structure depends on the number and size of the server groups and how the servers are shared among server groups in a specific configuration.

To configure deadtime within a server group, use the following commands beginning in global configuration mode:

|               | <b>Command</b>                                                     | <b>Purpose</b>                                                                                                                                                                                                                                   |
|---------------|--------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <code>Router(config)# <b>aaa group server radius</b> group1</code> | Defines a RADIUS type server group.                                                                                                                                                                                                              |
| <b>Step 2</b> | <code>Router(config-sg)# <b>deadtime</b> 1</code>                  | Configures and defines deadtime value in minutes.<br><br><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. |
| <b>Step 3</b> | <code>Router(config-sg)# <b>exit</b></code>                        | 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.                                                                         |
| 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](#)” section on page 5 and “[Configuring AAA Server Groups](#)” section on page 10.

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><br><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><br><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.  |
| <b>Step 4</b> | Router(config)# <b>aaa dnis map</b> <i>dnis-number</i> <b>accounting</b><br><b>network</b> [ <b>none</b>   <b>start-stop</b>   <b>stop-only</b> ] <b>group</b><br><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> ]<br>[ <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> ]<br>[ <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> ]<br>[ <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, page 15](#)
- [Setting Up the RADIUS Profile for Call Type Preauthentication, page 15](#)
- [Setting Up the RADIUS Profile for Preauthentication Enhancements for Callback, page 16](#)
- [Setting Up the RADIUS Profile for a Remote Host Name Used for Large-Scale Dial-Out, page 16](#)
- [Setting Up the RADIUS Profile for Modem Management, page 16](#)
- [Setting Up the RADIUS Profile for Subsequent Authentication, page 17](#)
- [Setting Up the RADIUS Profile for Subsequent Authentication Type, page 17](#)
- [Setting Up the RADIUS Profile to Include the Username, page 18](#)
- [Setting Up the RADIUS Profile for Two-Way Authentication, page 18](#)
- [Setting Up the RADIUS Profile to Support Authorization, page 19](#)

## 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.<br><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 "
```

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.

See “[Related Documents](#)” section on page 32 for more information on modem management.

## 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 2865 values for attribute 6. For information about possible Service-Type values, see [“Related Documents” section on page 32](#).



### 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><br>[ <b>on-expiry</b> { <b>accept</b>   <b>reject</b> }]      | 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><br>[ <b>on-expiry</b> { <b>accept</b>   <b>reject</b> }] | 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, see [“Related Documents” section on page 32](#).

## 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. |

# Configuration Examples for RADIUS

The following sections provide RADIUS configuration examples:

- [RADIUS Authentication and Authorization: Example, page 22](#)
- [RADIUS Authentication, Authorization, and Accounting: Example, page 23](#)
- [Vendor-Proprietary RADIUS Configuration: Example, page 23](#)
- [RADIUS Server with Server-Specific Values: Example, page 24](#)
- [Multiple RADIUS Servers with Global and Server-Specific Values: Example, page 24](#)
- [Multiple RADIUS Server Entries for the Same Server IP Address: Example, page 25](#)
- [RADIUS Server Group: Examples, page 25](#)
- [Multiple RADIUS Server Entries Using AAA Server Groups: Example, page 26](#)
- [AAA Server Group Selection Based on DNIS: Example, page 26](#)
- [AAA Preauthentication: Examples, page 27](#)
- [RADIUS User Profile with RADIUS Tunneling Attributes: Example, page 28](#)
- [Guard Timer: Examples, page 29](#)
- [L2TP Access Concentrator: Examples, page 29](#)
- [L2TP Network Server: Examples, page 30](#)

## 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.

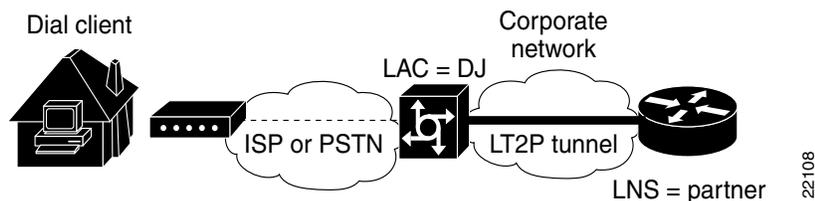
```
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
 cas-custom 0
 call guard-timer 20000 on-expiry accept

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 hgw1

```

The following example shows how to configure the LNS with a basic L2F and L2TP configuration using RADIUS tunneling attributes:

```

aaa new-model
aaa authentication login default none

```

```
aaa authentication login console none
aaa authentication ppp default local group radius
aaa authorization network default group radius if-authenticated
!
username l2f-cli-auth-id password 0 l2f-cli-pass
username l2f-svr-auth-id password 0 l2f-svr-pass
username l2tp-svr-auth-id password 0 l2tp-tnl-pass
!
vpdn enable
vpdn search-order domain
!
vpdn-group 1
accept-dialin
protocol l2f
virtual-template 1
terminate-from hostname l2f-cli-auth-id
local name l2f-svr-auth-id
!
vpdn-group 2
accept-dialin
protocol l2tp
virtual-template 2
terminate-from hostname l2tp-cli-auth-id
local name l2tp-svr-auth-id
!
interface Ethernet1/0
ip address 10.0.0.3 255.255.255.0
no ip route-cache
no ip mroute-cache
!
interface Virtual-Template1
ip unnumbered Ethernet1/0
ppp authentication pap
!
interface Virtual-Template2
ip unnumbered Ethernet1/0
ppp authentication pap
!
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server key <deleted>
```

## Additional References

The following sections provide references related to Configuring RADIUS.

### Related Documents

| Related Topic                      | Document Title                                                                                                                         |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| RADIUS attributes                  | <a href="#">“RADIUS Attributes Overview and RADIUS IETF Attributes”</a> module.                                                        |
| AAA                                | <a href="#">“Configuring Authentication”</a> module                                                                                    |
|                                    | <a href="#">“Configuring Authorization”</a> module.                                                                                    |
|                                    | <a href="#">“Configuring Accounting”</a> module.                                                                                       |
| L2F, L2TP, VPN, or VPDN            | <a href="#">Cisco IOS Dial Technologies Configuration Guide</a> and <a href="#">Cisco IOS VPDN Configuration Guide</a> , Release 15.0. |
| Modem Configuration and Management | <a href="#">Cisco IOS Dial Technologies Configuration Guide</a> , Release 15.0                                                         |
| RADIUS port identification for PPP | <a href="#">Cisco IOS Wide-Area Networking Configuration Guide</a> , Release 15.0.                                                     |

### Standards

| Standard | Title |
|----------|-------|
| None.    | —     |

### MIBs

| MIB   | MIBs Link                                                                                                                                                                                                              |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

### RFCs

| RFC                      | Title                                                              |
|--------------------------|--------------------------------------------------------------------|
| <a href="#">RFC 2139</a> | <i>RADIUS Accounting</i>                                           |
| <a href="#">RFC 2865</a> | <i>Remote Authentication Dial-In User Service (RADIUS)</i>         |
| <a href="#">RFC 2868</a> | <i>RADIUS Attributes for Tunnel Protocol Support</i>               |
| <a href="#">RFC 2867</a> | <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 Configuring RADIUS

Table 15 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 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 RADIUS

| Feature Name       | Releases                                                                 | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuring RADIUS | 11.1<br>Cisco IOS<br>XE<br>Release 2.1<br>Cisco IOS<br>XE<br>Release 2.3 | <p>The Remote Authentication Dial-In User Service (RADIUS) security system is a distributed client/server system that secures networks against unauthorized access.</p> <p>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.</p> <p>This feature was introduced in Cisco IOS Release 11.1.</p> <p>This feature was implemented on the Cisco ASR 1000 series routers in Cisco IOS XE Release 2.1.</p> <p>This feature was integrated into Cisco IOS XE Release 2.3.</p> |

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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.





# AAA-SERVER-MIB Set Operation

---

**First Published: November 1, 2005**

**Last Updated: November 20, 2009**

The AAA-SERVER-MIB Set Operation feature allows the authentication, authorization, and accounting (AAA) server configuration to be extended or expanded by using the CISCO-AAA-SERVER-MIB to create and add new AAA servers, modify the “KEY” under the CISCO-AAA-SERVER-MIB, and delete the AAA server 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 AAA-SERVER-MIB Set Operation”](#) 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 AAA-SERVER-MIB Set Operation, page 2](#)
- [Restrictions for AAA-SERVER-MIB Set Operation, page 2](#)
- [Information About AAA-SERVER-MIB Set Operation, page 2](#)
- [How to Configure AAA-SERVER-MIB Set Operation, page 2](#)
- [Configuration Examples for AAA-SERVER-MIB Set Operation, page 3](#)
- [Additional References, page 6](#)
- [Feature Information for AAA-SERVER-MIB Set Operation, page 8](#)



---

**Americas Headquarters:**

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

## Prerequisites for AAA-SERVER-MIB Set Operation

AAA must have been enabled on the router, that is, the **aaa new-model** command must have been configured. If this configuration has not been accomplished, the set operation fails.

## Restrictions for AAA-SERVER-MIB Set Operation

Currently, the CISCO SNMP set operation is supported only for the RADIUS protocol. Therefore, only RADIUS servers in global configuration mode can be added, modified, or deleted.

## Information About AAA-SERVER-MIB Set Operation

Before using the AAA-SERVER-MIB Set Operation feature, you should understand the following concepts:

- [CISCO-AAA-SERVER-MIB, page 2](#)
- [CISCO-AAA-SERVER-MIB Set Operation, page 2](#)

## CISCO-AAA-SERVER-MIB

The CISCO-AAA-SERVER-MIB provides that statistics reflect both the state of the AAA server operation with the server itself and of AAA communications with external servers. The CISCO-AAA-SERVER-MIB provides the following information:

- Statistics for each AAA operation
- Status of servers that are providing AAA functions
- Identities of external AAA servers

## CISCO-AAA-SERVER-MIB Set Operation

Before Cisco IOS Release 12.4(4)T, the CISCO-AAA-SERVER-MIB supported only the “get” operation. Effective with this release, the CISCO-AAA-SERVER-MIB supports the set operation. With the set operation, you can do the following:

- Create or add a new AAA server.
- Modify the KEY under the CISCO-AAA-SERVER-MIB. This “secret key” is used for secure connectivity to the AAA server, which is present with the network access server (NAS) and the AAA server.
- Delete the AAA server configuration.

## How to Configure AAA-SERVER-MIB Set Operation

This section contains the following information:

- [Configuring AAA-SERVER-MIB Set Operations, page 3](#)

- [Verifying SNMP Values, page 3](#)

## Configuring AAA-SERVER-MIB Set Operations

No special configuration is required for this feature. The Simple Network Management Protocol (SNMP) framework can be used to manage MIBs. See the section “[Additional References](#)” for a reference to configuring SNMP.

## Verifying SNMP Values

SNMP values can be verified by performing the following steps.

### SUMMARY STEPS

1. `enable`
2. `show running-config | include radius-server host`
3. `show aaa servers`

### DETAILED STEPS

|        | Command or Action                                                                                                                                             | Purpose                                                                                                                                  |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br>Router> <code>enable</code>                                                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                       |
| Step 2 | <code>show running-config   include radius-server host</code><br><br><b>Example:</b><br>Router# <code>show running-config   include radius-server host</code> | Displays all the RADIUS servers that are configured in the global configuration mode.                                                    |
| Step 3 | <code>show aaa servers</code><br><br><b>Example:</b><br>Router# <code>show aaa servers</code>                                                                 | Displays information about the number of requests sent to and received from authentication, authorization, and accounting (AAA) servers. |

## Configuration Examples for AAA-SERVER-MIB Set Operation

This section includes the following example:

- [RADIUS Server Configuration and Server Statistics: Example, page 4](#)

## RADIUS Server Configuration and Server Statistics: Example

The following sample output shows the RADIUS server configuration and server statistics before and after the set operation.

### Before the Set Operation

```
Router# show running-config | include radius-server host
```

```
! The following line is for server 1.
radius-server host 172.19.192.238 auth-port 2095 acct-port 2096 key cisco2
! The following line is for server 2.
radius-server host 172.19.192.238 auth-port 1645 acct-port 1646
```

### Server Statistics

```
Router# show aaa servers
```

```
RADIUS: id 2, priority 1, host 172.19.192.238, auth-port 2095, acct-port 2096
State: current UP, duration 25s, previous duration 0s
 Dead: total time 0s, count 7
Authen: request 8, timeouts 8
 Response: unexpected 0, server error 0, incorrect 0, time 0ms
 Transaction: success 0, failure 2
Author: request 0, timeouts 0
 Response: unexpected 0, server error 0, incorrect 0, time 0ms
 Transaction: success 0, failure 0
Account: request 0, timeouts 0
 Response: unexpected 0, server error 0, incorrect 0, time 0ms
 Transaction: success 0, failure 0
Elapsed time since counters last cleared: 5m

RADIUS: id 3, priority 2, host 172.19.192.238, auth-port 1645, acct-port 1646
State: current UP, duration 5s, previous duration 0s
 Dead: total time 0s, count 2
Authen: request 8, timeouts 8
 Response: unexpected 0, server error 0, incorrect 0, time 0ms
 Transaction: success 0, failure 4
Author: request 0, timeouts 0
 Response: unexpected 0, server error 0, incorrect 0, time 0ms
 Transaction: success 0, failure 0
Account: request 0, timeouts 0
 Response: unexpected 0, server error 0, incorrect 0, time 0ms
 Transaction: success 0, failure 0
Elapsed time since counters last cleared: 3m
```

### SNMP Get Operation to Check the Configuration and Statistics of the RADIUS Servers

```
aaa-server5:/users/smetri> getmany 10.0.1.42 casConfigTable
casAddress.2.2 = 172.19.192.238
casAddress.2.3 = 172.19.192.238
casAuthenPort.2.2 = 2095
casAuthenPort.2.3 = 1645
casAcctPort.2.2 = 2096
casAcctPort.2.3 = 1646
casKey.2.2 =
casKey.2.3 =
! The following line shows priority for server 1.
casPriority.2.2 = 1
! The following line shows priority for server 2.
casPriority.2.3 = 2
casConfigRowStatus.2.2 = active(1)
casConfigRowStatus.2.3 = active(1)
```

```
aaa-server5:/users/smetri>
```

### SNMP Set Operation

The key of the existing RADIUS server is being changed. The index "1" is being used. That index acts as a wildcard for addition, deletion, or modification of any entries.

Change the key for server 1:=>

```
aaa-server5:/users/smetri> setany -v2c 10.0.1.42 public casAddress.2.1 -a 172.19.192.238
casAuthenPort.2.1 -i 2095 casAcctPort.2.1 -i 2096 casKey.2.1 -o king
casAddress.2.1 = 172.19.192.238
casAuthenPort.2.1 = 2095
casAcctPort.2.1 = 2096
casKey.2.1 = king
aaa-server5:/users/smetri>
```

### After the Set Operation

After the above SNMP set operation, the configurations on the router change. The following output shows the output after the set operation.

```
Router# show running-config | include radius-server host
```

```
radius-server host 172.19.192.238 auth-port 1645 acct-port 1646
! The following line shows a change in the key value to "king."
radius-server host 172.19.192.238 auth-port 2095 acct-port 2096 key king
```

```
Router# show aaa servers
```

```
RADIUS: id 3, priority 1, host 172.19.192.238, auth-port 1645, acct-port 1646
State: current UP, duration 189s, previous duration 0s
 Dead: total time 0s, count 2
Authen: request 8, timeouts 8
 Response: unexpected 0, server error 0, incorrect 0, time 0ms
 Transaction: success 0, failure 4
Author: request 0, timeouts 0
 Response: unexpected 0, server error 0, incorrect 0, time 0ms
 Transaction: success 0, failure 0
Account: request 0, timeouts 0
 Response: unexpected 0, server error 0, incorrect 0, time 0ms
 Transaction: success 0, failure 0
Elapsed time since counters last cleared: 6m

! The following line shows a new server with new statistics.
RADIUS: id 4, priority 2, host 172.19.192.238, auth-port 2095, acct-port 2096
State: current UP, duration 209s, previous duration 0s
 Dead: total time 0s, count 7
Authen: request 0, timeouts 0
 Response: unexpected 0, server error 0, incorrect 0, time 0ms
 Transaction: success 0, failure 0
Author: request 0, timeouts 0
 Response: unexpected 0, server error 0, incorrect 0, time 0ms
 Transaction: success 0, failure 0
Account: request 0, timeouts 0
 Response: unexpected 0, server error 0, incorrect 0, time 0ms
```

## Additional References

The following sections provide references related to the AAA-SERVER-MIB Set Operation feature.

### Related Documents

| Related Topic    | Document Title                                                                                            |
|------------------|-----------------------------------------------------------------------------------------------------------|
| Configuring SNMP | <a href="#">“Configuring SNMP Support”</a> in the <i>Cisco IOS Network Management Configuration Guide</i> |

### Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

### MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

### RFCs

| RFC                                                                                                                         | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

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

# Feature Information for AAA-SERVER-MIB Set Operation

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 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.



## 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-SERVER-MIB Set Operation

| Feature Name                 | Releases                             | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AAA-SERVER-MIB Set Operation | 12.4(4)T<br>12.3(11)T<br>12.2(33)SRE | <p>The AAA-SERVER-MIB Set Operation feature allows the authentication, authorization, and accounting (AAA) server configuration to be extended or expanded by using the CISCO-AAA-SERVER-MIB to create and add new AAA servers, modify the “KEY” under the CISCO-AAA-SERVER-MIB, and delete the AAA server configuration.</p> <p>In Cisco IOS Release 12.4(4)T, this feature was introduced.</p> <p>In Cisco IOS XE Release XE 2.1 this feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">CISCO-AAA-SERVER-MIB Set Operation, page 2</a></li> <li>• <a href="#">Configuration Examples for AAA-SERVER-MIB Set Operation, page 3</a></li> </ul> <p>The following commands were introduced or modified:<br/><b>show aaa servers, show running-config, show running-config vrf.</b></p> |

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, 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 Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, 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. (0910R)

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.





# Offload Server Accounting Enhancement

---

**First Published: September 27, 2001**

**Last Updated: October 19, 2009**

The Offload Server Accounting Enhancement feature allows users to maintain authentication and accounting information between their network access servers (NASs) and the 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.

## 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 Offload Server Accounting Enhancement](#)” 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, page 2](#)
- [Information About Offload Server Accounting Enhancement, page 2](#)
- [How to Configure the Offload Server Accounting Enhancement, page 2](#)
- [Configuration Examples for the Offload Server Accounting Enhancement, page 4](#)
- [Additional References, page 5](#)
- [Feature Information for Offload Server Accounting Enhancement, page 7](#)
- [Glossary, page 7](#)



---

**Americas Headquarters:**

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

## Prerequisites

Before configuring the Offload Server Accounting Enhancement feature, you must perform the following tasks:

- Enable AAA. See the “[Configuring Authentication](#)” feature module for more information.
- Enable VPN. See the *Cisco IOS Security Configuration Guide: Secure Connectivity*, Release 12.4T for more information.

## Information About Offload Server Accounting Enhancement

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 through a 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 through Layer 2 Forwarding (L2F) options.
- The offload server includes the new, unique session-id in user access requests and user session accounting requests. The Class attribute that is passed from the NAS is included in the user access request, but a new Class attribute is received in the user access reply; this new Class attribute should be included in user session accounting requests.

## How to Configure the Offload Server Accounting Enhancement

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 3](#)(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 for the Offload Server Accounting Enhancement

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 the Offload Server Accounting Enhancement.

## Related Documents

| Related Topic | Document Title                                                                              |
|---------------|---------------------------------------------------------------------------------------------|
| Enable VPN    | <a href="#">Cisco IOS Security Configuration Guide: Secure Connectivity, Release 12.4T.</a> |
| Enable AAA    | <a href="#">“Configuring Authentication”</a> module.                                        |

## Standards

| Standard | Title |
|----------|-------|
| None     | —     |

## MIBs

| MIB  | MIBs Link                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><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 Offload Server Accounting Enhancement

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 Offload Server Accounting Enhancement

| Feature Name                          | Releases                              | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Offload Server Accounting Enhancement | 12.2(4)T<br>12.2(28)SB<br>12.2(33)SRC | <p>The Offload Server Accounting Enhancement feature allows users to maintain authentication and accounting information between their network access servers (NASs) and the offload server.</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>The following commands were introduced or modified:<br/> <b>radius-server attribute 44 extend-with-addr</b>,<br/> <b>radius-server attribute 44 sync-with-client</b></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.

**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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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.



# Per IP Subscriber DHCP Triggered RADIUS Accounting

---

**First Published: February 19, 2007**  
**Last Updated: August 25, 2009**

The Per IP Subscriber DHCP Triggered RADIUS Accounting feature enables system administrators to track IP session activity on a per-subscriber basis and periodically extract subscriber accounting records. Transactions between the client and the RADIUS accounting server are authenticated via an Access Client module that maintains per-subscriber accounting statistics.

Per IP Subscriber RADIUS Accounting works with DHCP IP address assignment on Cisco 7600 series routers only, and it improves the authentication, authorization, and accounting (AAA) of broadband service delivery. Subscribers are attributed a unique AAA ID in addition to the unique ID created by DHCP in order to process secure START and STOP accounting messages and allow them to abstract accounting information in a client-server environment.

## 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 IP Subscriber DHCP Triggered RADIUS Accounting” 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

- [Per IP Subscriber DHCP Triggered RADIUS Accounting](#), page 2
- [Restrictions for Per IP Subscriber DHCP Triggered RADIUS Accounting](#), page 2
- [Information About Per IP Subscriber DHCP Triggered RADIUS Accounting](#), page 2



---

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

[, page 5](#)

[Configuration Examples for Per IP Subscriber DHCP Triggered RADIUS Accounting, page 6](#)

[Additional References, page 7](#)

[Feature Information for Per IP Subscriber DHCP Triggered RADIUS Accounting, page 9](#)

## Prerequisites for Per IP Subscriber DHCP Triggered RADIUS Accounting

- `aaa accounting`
- `ip dhcp limit lease per interface 1`

## Restrictions for Per IP Subscriber DHCP Triggered RADIUS Accounting

- operating with Access Type interfaces on a Cisco 7600 series Broadband Remote Access Server (B-RAS).  
This feature does not support the collection of IP statistics from each source IP address. The feature collects IP statistics for each subinterface rather than each subscriber, and it is triggered only if the command to allow one IP address assignment via DHCP is configured.

## Information About Per IP Subscriber DHCP Triggered RADIUS Accounting

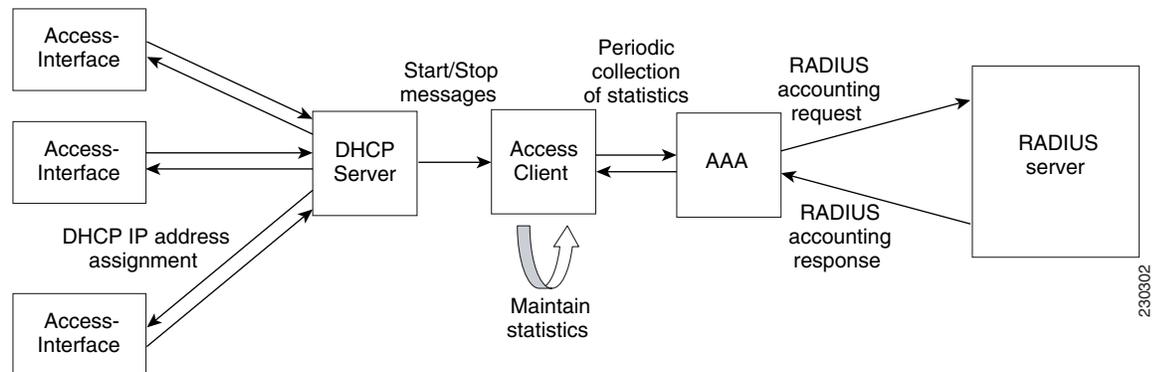
- [, page 3](#)

## Per IP Subscriber DHCP Triggered RADIUS Accounting Network Topology

- Access Interface—Used by subscribers to operate on a Cisco 7600 router.
- DHCP Server—Grants permission to the DHCP client to use a particular IP address for a specified lease time.
- AAA Server—Transmits secure START and STOP accounting messages.

Figure 1 shows how the Access Client, referred to as the “aaa-access-client” module, is initialized to serve as a client of the RADIUS accounting server. The module is independent of existing DHCP RADIUS Accounting modules.

**Figure 1** AAA Access Client Module Interaction



The Access Client comprises two sub-modules that enable improved IP session awareness, tracking, and reporting functionality:

**Access-Subscriber Management module (Access-Acct-Mgmt):** Invoked by a successful DHCP IP assignment, this sub-module generates a unique AAA ID for each subscriber that combines with the DHCP unique ID to track an accounting session.

**Access-Subscriber Accounting Management (Access-Acct-Update):** Invoked by the AAA server, this sub-module collects subscriber statistics and periodically reports on the accounting session.

## Benefits of Per IP Subscriber DHCP Triggered RADIUS Accounting

### IP Session Awareness and Security

## Per IP Subscriber Triggered RADIUS Accounting Behavior

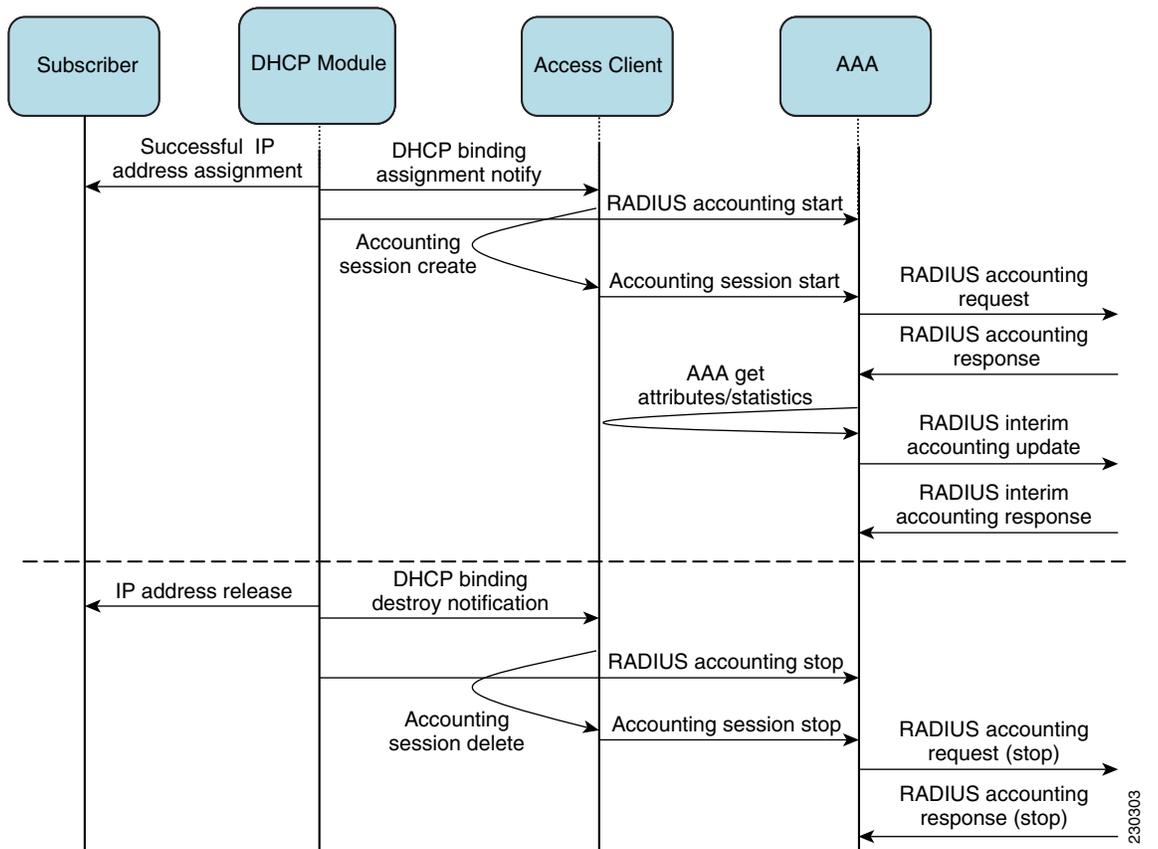
When a client with an Access Type of interface is configured for Per IP Subscriber RADIUS Accounting, the statistics collection and reporting mechanism can be invoked by the DHCP module. A successful DHCP IP assignment or release triggers three types of accounting events via the Access Client module:

1. **RADIUS accounting start:** An Accounting Start packet, ACCT\_START, is sent to the accounting server to flag the start of service delivery, the type of service being delivered, and the user it is being delivered to.

3.

- 
- 
- 

**Figure 2** *AAA Access Client Process Flow*



# How to Configure Per IP Subscriber DHCP Triggered RADIUS Accounting

- [Configuring Method Lists for Per IP Subscriber DHCP Triggered RADIUS Accounting, page 5.](#)

## Configuring Method Lists for Per IP Subscriber DHCP Triggered RADIUS Accounting

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*] *access*
4. **encapsulation dot1q** *vlan-id* **native**  
**ip address** *ip-address mask* **secondary**
6. **accounting dhcp source-ip** *aaa list method-list-name*

**DETAILED STEPS**

|               | <b>Command or Action</b>                                                                                                 | <b>Purpose</b>                                                                                    |
|---------------|--------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                   | Enables privileged EXEC mode.<br><br>Enter your password if prompted.                             |
|               | <b>configure terminal</b><br><br>Router# configure terminal                                                              |                                                                                                   |
|               | <b>interface</b> <i>type number [name-tag] access</i><br><br>Router(config)# interface gigabitethernet<br>1/0/1.2 access |                                                                                                   |
|               | <b>encapsulation dot1q</b> <i>vlan-id native</i><br><br>Router(config-subif)# encapsulation dot1q 102                    | Enables IEEE 802.1q encapsulation of traffic on a specified subinterface in a virtual LAN (VLAN). |
|               | <i>ip-address mask secondary</i><br><br>255.255.255.0                                                                    |                                                                                                   |
|               | <b>accounting dhcp source-ip</b> <i>aaa list method-list-name</i>                                                        |                                                                                                   |

# Configuration Examples for Per IP Subscriber DHCP Triggered RADIUS Accounting

.

## Subinterface RADIUS Accounting Configuration: Example

```
aaa new-model
radius-server host 75.0.1.1 auth-port 1645 acct-port 1646 key lab
radius-server key lab
!
aaa accounting network default start-stop group radius
aaa accounting update periodic 1
end
!
configure terminal
ip dhcp pool pool1
 network 10.0.1.0 255.255.255.0
 lease 0 0 3
!
configure terminal
interface GigabitEthernet 1/0/1.2 access
encapsulation dot1q 102
ip address 10.0.2.1 255.255.255.0
accounting dhcp source-ip aaa list default
end
```

| Related Topic | Document Title                                       |
|---------------|------------------------------------------------------|
|               | <a href="#">Cisco IOS Security Command Reference</a> |

| Standard | Title |
|----------|-------|
|          |       |

| MIB | MIBs Link |
|-----|-----------|
|     |           |

## RFCs

| RFC | Title |
|-----|-------|
|     |       |

## Technical Assistance

| Description | Link |
|-------------|------|
|             |      |

# Feature Information for Per IP Subscriber DHCP Triggered RADIUS Accounting



Note

**Table 1** Feature Information for Per IP Subscriber DHCP Triggered RADIUS Accounting

| Feature Name | Releases | Feature Information |
|--------------|----------|---------------------|
|              |          |                     |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card 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. (0907R)

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.





# RADIUS: Separate Retransmit Counter for Accounting

---

**First Published: February 3, 2003**  
**Last Updated: September 1, 2009**

The RADIUS: Separate Retransmit Counter for Accounting feature allows users to configure an exponential backoff retransmit. That is, after the normally configured retransmission retries have been used, the router continues trying with an interval that doubles on each retransmission failure until a configured maximum interval is reached. This functionality allows users to retransmit accounting requests for many hours without overloading the RADIUS server when it does come back up.

## 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: Separate Retransmit Counter for Accounting”](#) 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 RADIUS: Separate Retransmit Counter for Accounting, page 2](#)
- [Information About RADIUS: Separate Retransmit Counter for Accounting, page 2 page 1](#)
- [How to Configure RADIUS: Separate Retransmit Counter for Accounting, page 2](#)
- [Configuration Examples for RADIUS: Separate Retransmit Counter for Accounting, page 6](#)
- [Additional References, page 7](#)



---

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

- [Feature Information for RADIUS: Separate Retransmit Counter for Accounting, page 9](#)

## Restrictions for RADIUS: Separate Retransmit Counter for Accounting

The following tasks result in excessive memory consumption on the router:

- Configuring this feature on a router with a high call rate.
- Configuring the **aaa accounting send stop-record authentication failure** command: an accounting record and a RADIUS packet is generated for each user that fails to authenticate while the RADIUS server is down.
- Configuring interim accounting: new accounting records are generated and stored on the router.

## Information About RADIUS: Separate Retransmit Counter for Accounting

In many environments, a single RADIUS server is used for authentication and accounting. Whenever this server is down for approximately 24 hours, the accounting records of users already on the router are lost after authentication, authorization, and accounting (AAA) does all the retransmissions. Before the introduction of this feature, the retransmissions could be configured for a maximum of 100 retries and the timeout could be configured for 1,000 seconds. Although these configurations keep the accounting records on the router for 24 hours, a timeout of 1,000 seconds is unreasonable, causing problems when the RADIUS server cannot be reached due to network congestion.

The RADIUS: Separate Retransmit Counter for Accounting feature allows users to configure an exponential backoff retransmit. That is, after the normally configured retransmission retries have been used, the router continues trying with an interval that doubles on each retransmission failure until a configured maximum interval is reached. This functionality allows users to retransmit accounting requests for many hours without overloading the RADIUS server when it does come back up.

This feature can be configured globally (through the **radius-server backoff exponential** command), per server (through the **radius-server host** command), or per group (through the **backoff exponential** command).

## Benefits

With this feature, users can extend the time in which the RADIUS client (the router) sends accounting requests to the RADIUS server in the event that the RADIUS server or the connection to the server is down and there is no accounting response confirmation. This functionality enables accounting records to remain on the router for up to 24 hours.

## How to Configure RADIUS: Separate Retransmit Counter for Accounting

This section contains the following tasks:

- [Configuring a Retransmit Counter for Accounting Globally or per RADIUS Host](#) (required)
- [Configuring a Retransmit Counter for Accounting per RADIUS Server Group](#) (required)
- [Verifying Retransmit Configurations](#) (optional)

## Configuring a Retransmit Counter for Accounting Globally or per RADIUS Host

To configure exponential backoffs of RADIUS retransmits over an extended period of time on a global basis and per RADIUS host, perform the following steps:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server backoff exponential** [*max-delay minutes*] [**backoff-retry** *retransmits*]
4. **radius-server host** {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] [**idle-time** *seconds*] [**backoff exponential** {**backoff-retry** *number-of-retransmits* | **key** *encryption-key* | **max-delay** *minutes*}]

### DETAILED STEPS

|        | Command                                                                        | Purpose                                                              |
|--------|--------------------------------------------------------------------------------|----------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enters privileged EXEC mode.<br><br>Enter your password if prompted. |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                    |

|        | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Purpose                                                                                                                          |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <pre>Router(config)# radius-server backoff exponential [max-delay minutes] [backoff-retry retransmits]</pre> <p><b>Example:</b><br/>Router (config)# radius-server backoff<br/>exponential max-delay 60 backoff-retry 32 </p>                                                                                                                                                                                                                                                                                                          | Configures the router for exponential backoff retransmit of accounting requests.                                                 |
| Step 4 | <pre>Router(config)# radius-server host {hostname   ip-address} [test username user-name] [auth-port port-number] [ignore-auth-port] [acct-port port-number] [ignore-acct-port] [timeout seconds] [retransmit retries] [key string] [alias {hostname   ip-address}] [idle-time seconds] [backoff exponential {backoff-retry number-of-retransmits   key encryption-key   max-delay minutes}]</pre> <p><b>Example:</b><br/>Router (config)# radius-server host<br/>192.0.2.1 test username test1 auth-port<br/>1645 acct-port 1646 </p> | Specifies a RADIUS server host and configures that RADIUS server host for exponential backoff retransmit of accounting requests. |

## Configuring a Retransmit Counter for Accounting per RADIUS Server Group

To configure exponential backoffs of RADIUS retransmits over an extended period of time per RADIUS server group, perform the following steps:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa group server radius *group-name***
4. **backoff exponential [max-delay *minutes*] [backoff-retry *retransmits*]**

### DETAILED STEPS

|        | Command                                                                                       | Purpose                                                                                                           |
|--------|-----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Step 1 | <pre>enable</pre> <p><b>Example:</b><br/>Router&gt; enable </p>                               | Enters 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><br/>Router (config)# configure terminal </p> | Enters global configuration mode.                                                                                 |

|        | Command                                                                                                                                           | Purpose                                                                                                                          |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | Router(config)# <b>aaa group server radius</b><br><i>group-name</i>                                                                               | Groups different RADIUS server hosts into distinct lists and distinct methods and enters server-group RADIUS configuration mode. |
| Step 4 | Router(config-sg-radius)# <b>backoff</b><br><b>exponential</b> [ <b>max-delay</b> <i>minutes</i> ]<br>[ <b>backoff-retry</b> <i>retransmits</i> ] | Configures the router for exponential backoff retransmit of accounting requests per RADIUS server group.                         |

## Verifying Retransmit Configurations

To verify feature functionality, use any of the following EXEC commands:

### SUMMARY STEPS

1. **enable**
1. **debug radius**
2. **show accounting**
3. **show radius statistics**

### DETAILED STEPS

|        | Command                                                                                | Purpose                                                                                                           |
|--------|----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                 | Enters privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>debug radius</b><br><br><b>Example:</b><br>Router# debug radius                     | Displays information associated with RADIUS.                                                                      |
| Step 3 | <b>show accounting</b><br><br><b>Example:</b><br>Router# show accounting               | Displays all active sessions and prints all the accounting records for actively accounted functions.              |
| Step 4 | <b>show radius statistics</b><br><br><b>Example:</b><br>Router# show radius statistics | Displays the RADIUS statistics for accounting packets.                                                            |

# Configuration Examples for RADIUS: Separate Retransmit Counter for Accounting

This section provides the following configuration examples:

- [Retransmit Counter for Accounting Comprehensive Configuration: Example](#)
- [Per-Server Configuration: Example](#)

## Retransmit Counter for Accounting Comprehensive Configuration: Example

The following example shows how to configure your router for exponential backoff retransmit of accounting requests. In this example, an exponential backoff is configured globally (through the **radius-server backoff exponential** command) and for the RADIUS server host “172.107.164.206” (through the **radius-server host** command).

```

aaa new-model
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authorization exec default group radius
aaa authorization network default group radius
aaa accounting send stop-record authentication failure
aaa accounting update periodic 1
aaa accounting network default start-stop group radius
!
interface BRI1/0
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 no ip mroute-cache
 dialer idle-timeout 0
 dialer-group 1
 isdn switch-type basic-5ess
!
radius-server host 172.107.164.206 auth-port 1645 acct-port 1646 backoff exponential
max-delay 60 backoff-retry 32
radius-server backoff exponential max-delay 60 backoff-retry 32
radius-server retransmit 3
radius-server key rad123
end

```

## Per-Server Configuration: Example

The following example shows how to enable exponential backoff retransmits on a per-server basis. In this example, assume that the retransmit is configured for 3 retries and the timeout is configured for 5 seconds; that is, the RADIUS request is transmitted 3 times with a delay of 5 seconds. Thereafter, the router continues to retransmit RADIUS requests with a delayed interval that doubles each time until 32 retries have been achieved. The router stops doubling the retransmit intervals after the interval surpasses the configured 60 minutes; it transmits every 60 minutes.

```
radius-server host foo.xyz.com backoff exponential max-delay 60 backoff-retry 32
```

After enabling this command, the retransmits are sent as follows (“t” equals seconds):

```

t = 0 req sent
t = 5 retrans 1
t = 10 retrans 2
t = 15 retrans 3

```

```

t = 25 retrans 4
t = 45 retrans 5
t = 85 retrans 6
t = 165 retrans 7
t = 325 retrans 8
t = 645 retrans 9
t = 1285 retrans 10
t= 2565 retrans 11
t = 5125 retrans 12
t = 8725 retrans 13 (The interval has stabilized to 60 minutes here).
t = 12325 retrans 14 till retransmit 35

```

After all the retransmits are sent, the RADIUS request follows the same path that it would when all the normal retransmits are done.

## Additional References

The following sections provide references related to the RADIUS: Separate Retransmit Counter for Accounting.

## Related Documents

| Related Topic                                              | Document Title                                                                                                                                                                                          |
|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RADIUS and AAA accounting configuration tasks and commands | <ul style="list-style-type: none"> <li>“<a href="#">Configuring RADIUS</a>” and “<a href="#">Configuring Accounting</a>” feature modules.</li> <li><i>CiscoOS Security Command Reference</i></li> </ul> |

## Standards

| Standard | Title |
|----------|-------|
| None     | —     |

## MIBs

| MIB  | 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

| 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: Separate Retransmit Counter for 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://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: Separate Retransmit Counter for Accounting

| Feature Name                                       | Releases                 | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RADIUS: Separate Retransmit Counter for Accounting | 12.2(15)B<br>12.2(33)SRC | The RADIUS: Separate Retransmit Counter for Accounting feature allows users to configure an exponential backoff retransmit. That is, after the normally configured retransmission retries have been used, the router continues trying with an interval that doubles on each retransmission failure until a configured maximum interval is reached. This functionality allows users to retransmit accounting requests for many hours without overloading the RADIUS server when it does come back up.<br><br>The following commands were introduced or modified:<br><b>backoff exponential, radius-server host, radius-server backoff exponential.</b> |
| RADIUS: Separate Retransmit Counter for Accounting | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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.

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



## Define Interface Policy-Map AV Pairs AAA

---

**First Published: November 11, 2004**

**Last Published: July 29, 2009**

The Define Interface Policy-Map AV Pairs AAA feature introduces two Cisco RADIUS vendor-specific attributes (VSAs) that allow a new policy map to be applied or an existing policy map to be modified, without affecting its session, during a Point-to-Point Protocol over ATM (PPPoA) or Point-to-Point Protocol over Ethernet over ATM (PPPoEoA) session establishment. The process occurs on the ATM virtual circuit (VC) level.

The Define Interface Policy-Map AV Pairs AAA has the following benefits:

- The ability to apply QoS policies transparently as required without the disruption of session reauthentication provides a high degree of flexibility, smaller configuration files, and more efficient usage of queuing resources. This ability eliminated the need to pre-provision subscribers.
- The ability to modify the applied policy map as needed without session disruption (session dropped and reauthenticated) is an advantage to service providers.
- Nondisruptive support for special event triggers is essential to support new dynamic bandwidth services such as pre-paid and turbo button services.

The QoS policy map is used to define the subscriber user experience for broadband service and can facilitate delivery of higher value services such as VoIP and video.

## 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 Define Interface Policy-Map AV Pairs AAA” section on page 18](#).

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 Define Interface Policy-Map AV Pairs AAA, page 2](#)
- [Restrictions for Define Interface Policy-Map AV Pairs AAA, page 2](#)
- [Information About Define Interface Policy-Map AV Pairs AAA, page 2](#)
- [How to Configure Define Interface Policy-Map AV Pairs AAA, page 5](#)
- [Configuration Examples for Define Interface Policy-Map AV Pairs AAA, page 11](#)
- [Additional References, page 16](#)
- [Feature Information for Define Interface Policy-Map AV Pairs AAA, page 18](#)

## Prerequisites for Define Interface Policy-Map AV Pairs AAA

- Authentication, Authorization, and Accounting (AAA) must be enabled and already set up to use RADIUS.
- Configuring a service policy on the ATM subinterface requires enabling Dynamic Bandwidth Selection (DBS) on the VC.

## Restrictions for Define Interface Policy-Map AV Pairs AAA

### For the Cisco 7000 series routers:

- Only the PA-A3-OC3/T3/E3 and PA-A6-OC3/T3/E3 port adapters are supported for this feature.

### For the Cisco 10000 series routers:

- You cannot configure a service policy on a VC and on a session at the same time.
- All ATM line cards, including the 4-Port OC-3/STM-1 ATM, 8-Port E3/DS3 ATM, and 1-Port OC-12 ATM line cards, are supported for this feature.

## Information About Define Interface Policy-Map AV Pairs AAA

This section lists the concepts that the user should understand in order to perform the tasks in the [How to Configure Define Interface Policy-Map AV Pairs AAA](#). The following concept is described in this section:

- [Dynamically Applying and Modifying a Policy Map](#)

## Dynamically Applying and Modifying a Policy Map

The Define Interface Policy-Map AV Pairs AAA feature introduces two Cisco VSAs that allow you to dynamically apply a policy map and modify a policy map applied to a session, without session reauthentication, at the ATM VC level using RADIUS. The purpose of the Cisco VSA (attribute 26) is to

communicate vendor-specific information between the network access server (NAS) and the RADIUS server. The Cisco VSA encapsulates vendor-specific attributes that allow vendors such as Cisco to support their own extended attributes.

The Define Interface Policy-Map AV Pairs AAA feature allows the two new Cisco VSAs to be installed on an ATM VC after a PPPoA or PPPoEoA session establishment. Using RADIUS, this feature allows a policy map to be applied (“pulled”) and then modified by specific events (“pushed” by the policy server) while that session remains active.

Previously, a policy map could only be configured on a VC or ATM point-to-point subinterface by using the modular QoS CLI (MQC) or manually with the virtual template. Also previously, a service policy on a VC could be modified in the session but that session was dropped and reauthenticated. Currently for a PPPoA or PPPoEoA session, the pull part of the feature uses RADIUS to dynamically apply policy maps on an ATM VC and eliminates the need to statically configure a policy map on each VC. After a policy map is applied directly on the interface, certain events can signal the policy server to push a policy map onto a specific VC without the need for session reauthentication.

**Note**

Configuring a service policy on the ATM subinterface still requires MQC configuration.

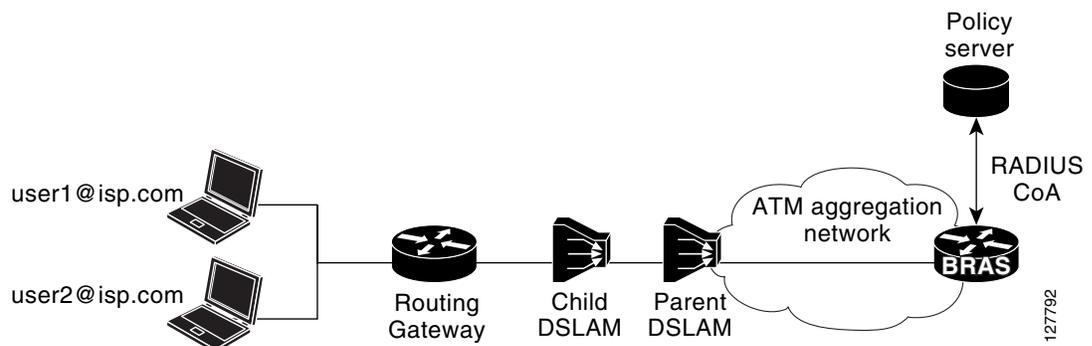
Two new Cisco AV pairs for service policy are set up in the user file on the RADIUS server. When the router requests the policy map name, the policy map name in the user file is pulled to the VC on the router when the PPPoA or PPPoEoA session is established. The Cisco AV pairs identify a “service policy-output” and “service policy-input” to identify QoS policies configured on the router from a RADIUS server. The Cisco AV pairs apply the appropriate policy map directly on the interface. Service policies are only applied at this time when the subscriber first authenticates the VC.

The “push” functionality of the feature allows you to modify an existing QoS profile (a policy map) applied to a session while that session remains active, thus allowing QoS policies to be applied as required without session reauthentication disruption. Specific events, including time-of-day, byte count, and user request, can signal the policy server to push a policy map onto a specific VC.

The policy server has the ability to send a Change of Authorization (CoA), which is the ability to change authorization of active sessions on the fly. The push functionality requires that CoA is enabled on the AAA server. One of the session attributes CoA pushes is the policy map, in an input and output direction.

[Figure 1](#) shows that a CoA request is sent from the policy server to a broadband rate access server (BRAS), which causes a policy map change on PPPoA sessions set up between the BRAS and the routing gateway (RG).

**Figure 1** Change of Authorization—Policy Map Change on PPPoA Sessions



For clarification, a policy map defines QoS actions and rules and associates these to a class map. In a policy map, you can define QoS actions for such things as policing and class-based weighted fair queuing (CBWFQ). After a policy map is configured on the router with the **policy-map** command, using the **service-policy** command attaches the configured policy map to a VC interface and specifies the direction (inbound or outbound) that the policy should be applied.

When a service policy is configured on the VC (or ATM point-to-point subinterface), the service policy is applied to all sessions that use that VC.

**Note**

For the Cisco 7200 series routers, you can configure a service policy on a VC and on a session at the same time. On the Cisco 10000 series routers, you must either configure a service policy on a VC or on a session, but not both at the same time.

**Note**

The Cisco 7200 series routers and Cisco 7301 router only support the PA-A3-OC3/T3/E3 and PA-A6-OC3/T3/E3 port adapters for this feature. The Cisco 10000 series routers support all ATM line cards, including the 4-Port OC-3/STM-1 ATM, 8-Port E3/DS3 ATM, and 1-Port OC-12 ATM line cards, for this feature.

## New Cisco VSAs

To support the Define Interface Policy-Map AV Pairs AAA feature, the following two new Cisco AV pairs for policy map are defined at the ATM VC level:

- Cisco VSA attribute is `vc-qos-policy-in`
- Cisco VSA attribute is `vc-qos-policy-out`

They are formatted as:

- `cisco-avpair = "atm:vc-qos-policy-in=<in policy name>"`
- `cisco-avpair = "atm:vc-qos-policy-out=<out policy name>"`

To further support the Define Interface Policy-Map AV Pairs AAA feature, two existing Cisco Generic RADIUS VSAs will replace and deprecate two others that do not correctly follow the Cisco VSA naming guidelines.

The two replacement VSAs are:

- `cisco-avpair = "ip:sub-qos-policy-in=<in policy name>"`
- `cisco-avpair = "ip:sub-qos-policy-out=<out policy name>"`

The replacement VSAs replace the following existing VSAs:

- `cisco-avpair = "ip:sub-policy-In=<in policy name>"`
- `cisco-avpair = "ip:sub-policy-Out=<out policy name>"`

We recommend using the new VSAs. However, the replaced attributes are currently still supported.

## Policy Map Troubleshooting Scenarios

- If a policy map is already configured on the ATM VC, the policy map pulled from the RADIUS server has higher precedence. This means that a **show policy-map** command shows the policy map pulled from the RADIUS server.

- After a policy map is successfully pulled on the VC, any configuration or unconfiguration after that using the **[no] service-policy input/output name** command does not affect the policy map used by the VC. Issuing a **show policy-map** command displays the pulled policy map. Issuing a **show run** command displays the current user configuration on the router.
- To remove the dynamic policy that is pulled from the RADIUS server, use the **no dbs enable** command or clear the PPPoA or PPPoEoA session associated with the VC.
- You should push both the input and output policy map together on the VC. If you push only one policy in one direction (for example, the input direction), then the output direction by default is a null policy push. The result is that on the VC, the input policy map is the policy pushed by the CoA. The output policy map is whatever policy was configured locally on the VC. If no output policy map was configured on the VC, there is no output policy map.

## How to Configure Define Interface Policy-Map AV Pairs AAA

This section contains the following tasks:

- [Configuring AV Pairs, Dynamic Authorization, and the Policy Map, page 5](#)
- [Verifying Define Interface Policy-Map AV Pairs AAA, page 8](#)

### Configuring AV Pairs, Dynamic Authorization, and the Policy Map

To configure the Define Interface Policy-Map AV Pairs AAA feature, follow the steps below on both the router and RADIUS server.

#### Prerequisites

- AAA must be enabled and already set up to use RADIUS.
- A PPPoEoA or PPPoA session is established.
- The CoA functionality is enabled—required for the push functionality.
- The **dbs enable** CLI is configured on the VC.
- The policy map is configured on the router.

#### SUMMARY STEPS

On the RADIUS server, configure the new Cisco AV pair attributes in the user file:

1. **atm:vc-qos-policy-in=<in policy name>**  
**atm:vc-qos-policy-out=<out policy name>**

On the local AAA server, configure dynamic authorization that supports CoA in global configuration mode:

1. **aaa server radius dynamic-author**

On the router:

1. **enable**
2. **configure terminal**
3. **interface atm [module/slot/port.subinterface] point-to-point**

4. **pvc** *vpi/vci*
5. **db**s enable
6. **exit**
7. **policy-map** *policy-map-name*
8. **end**

### DETAILED STEPS—RADIUS Server

|               | Command or Action                                                                                                                                                                                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <pre>atm:vc-qos-policy-in=&lt;in policy name&gt; atm:vc-qos-policy-out=&lt;out policy name&gt;</pre> <p><b>Example:</b><br/>On the RADIUS server, configure in the user file:</p> <pre>userid Password = "cisco"   Service-Type = Framed,   Framed-Protocol = PPP,   cisco-avpair = "atm:vc-qos-policy-out=dyn_out",   cisco-avpair = "atm:vc-qos-policy-in=test_vc"</pre> | <p>Enters the two new Cisco AV pairs for service policy on the RADIUS server in the user file. When the router requests the policy name, this information in the user file is “pulled.”</p> <p>A RADIUS user file contains an entry for each user that the RADIUS server will authenticate. Each entry, which is also referred to as a <i>user profile</i>, establishes an attribute the user can access.</p> <p>When looking at a user file, the data to the left of the equal sign (=) is an attribute defined in the dictionary file, and the data to the right of the equal sign is the configuration data.</p> <p>In this example, you have configured a service policy that attaches a policy map to the ATM VC interface and specifies the direction (inbound for data packets traveling into the interface or outbound for data packets leaving the interface).</p> <p>The policy map applied in the outbound direction is <code>dyn_out</code> and the inbound policy map is <code>test_vc</code>.</p> |

### DETAILED STEPS—AAA Server

|               | Command or Action                                                                    | Purpose                                                                      |
|---------------|--------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| <b>Step 1</b> | <pre>enable</pre> <p><b>Example:</b><br/>Router&gt; enable </p>                      | <p>Enables privileged EXEC mode.</p> <p>Enter your password if prompted.</p> |
| <b>Step 2</b> | <pre>configure terminal</pre> <p><b>Example:</b><br/>Router# configure terminal </p> | <p>Enters global configuration mode.</p>                                     |
| <b>Step 3</b> | <pre>aaa new-model</pre> <p><b>Example:</b><br/>Router(config)# aaa new-model </p>   | <p>Enables AAA.</p>                                                          |

| Command or Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Step 4</b></p> <pre>aaa server radius dynamic-author</pre> <p><b>Example:</b><br/>Router(config)# aaa server radius dynamic-author</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <p>Sets up the local AAA server for dynamic authorization service, which must be enabled to support the CoA functionality to push the policy map in an input and output direction and enters dynamic authorization local server configuration mode. In this mode, the RADIUS application commands are configured.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <p><b>Step 5</b></p> <p>Configure the <b>client</b> command and <b>server-key</b> keyword or the <b>client</b> command and <b>server-key</b> command.</p> <pre>aaa server radius dynamic-author   auth-type {any   all   session-key}   client {ip_addr   hostname} [server-key [0   7] string] [vrf vrfname [server-key [0   7] string]]   ignore {session-key   server-key}   port {port-num}   server-key [0   7] string</pre> <p><b>Example:</b><br/>On the AAA server, the following is an example configuration:</p> <pre>Router(config)aaa server radius dynamic-author Router(config-locsvr-da-radius)#client 192.168.0.5 vrf coa server-key cisco1 Router(config-locsvr-da-radius)#client 192.168.1.5 vrf coa server-key cisco2</pre> | <p>You can use the <b>client</b> command and <b>server-key</b> keyword and <i>string</i> argument to configure the server key at the “client” level, or use the <b>server-key</b> command and <i>string</i> argument to configure the server key at the “global” level, which allows all the clients configured with the <b>client</b> command to use the global server key.</p> <p><b>Note</b> Configuring the server key at the client level overrides the server key configured at the global level.</p> <p>For security purposes, we recommend configuring each client and configuring different server-keys for each client.</p> <p>The example configuration enables change of authorization and configures two client routers with different server-keys (cisco1 and cisco2).</p> <p>The <b>auth-type</b>, <b>domain</b>, <b>ignore session-key</b>, <b>ignore server-key</b>, and <b>port</b> commands are optional.</p> <p><b>Note</b> When using the <b>auth-type</b> command and <b>session-key</b> keyword, the session-key attribute must match for authorization to be successful. The only exception is if the session-id attribute is provided in the RADIUS Packet of Disconnect (POD) request, then the session ID is valid.</p> |

## DETAILED STEPS—Router

| Command or Action                                                                                        | Purpose                                                                      |
|----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| <p><b>Step 1</b></p> <pre>enable</pre> <p><b>Example:</b><br/>Router&gt; enable</p>                      | <p>Enables privileged EXEC mode.</p> <p>Enter your password if prompted.</p> |
| <p><b>Step 2</b></p> <pre>configure terminal</pre> <p><b>Example:</b><br/>Router# configure terminal</p> | <p>Enters global configuration mode.</p>                                     |

|        | Command or Action                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <pre>interface atm [module/slot/port.subinterface] point-to-point</pre> <p><b>Example:</b><br/>Router(config)# interface ATM 4/0/1 point-to-point </p> | <p>Specifies the interface, for example ATM4/0, and the encapsulation type on an ATM PVC.</p> <p>Enters subinterface mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 4 | <pre>pvc vpi/vci</pre> <p><b>Example:</b><br/>Router(config-if)# pvc 1/101 </p>                                                                        | <p>Creates or assigns a name to an ATM permanent virtual circuit (PVC) in subinterface configuration mode. The <b>pvc</b> command creates a PVC and attaches it to the virtual path identifier (VPI) and virtual channel identifier (VCI) specified.</p> <p>Enters ATM virtual circuit configuration mode.</p> <p>The example specifies VPI 1 and VCI 101 for this PVC.</p>                                                                                                                                                                                                                     |
| Step 5 | <pre>dbns enable</pre> <p><b>Example:</b><br/>Router(config-if-atm-vc)# dbns enable </p>                                                               | <p>Enables Dynamic Bandwidth Selection (DBS) in ATM VC configuration mode. Enabling this command allows the ATM shaping parameters to be retrieved from the RADIUS user profile.</p> <p> <b>Note</b> The <b>no dbns enable</b> command re-creates the VC and removes the dynamic policy that is pulled from the RADIUS server. Consequently, any configured modular QoS CLI (MQC) policy map on the PVC will be installed on the VC. Do not issue the <b>no dbns enable</b> command when the VC is active.</p> |
| Step 6 | <pre>exit</pre> <p><b>Example:</b><br/>Router(config-if-atm-vc)# exit </p>                                                                             | <p>Exits ATM VC configuration mode and returns to subinterface configuration mode.</p> <p>Repeat this step one more time to exit subinterface configuration mode and return to global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 7 | <pre>policy-map policy-map-name</pre> <p><b>Example:</b><br/>Router(config)# policy-map voice </p>                                                     | <p>Creates a policy map on the router.</p> <p>In the example, a policy map named voice is created.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 8 | <pre>end</pre> <p><b>Example:</b><br/>Router(config)# end </p>                                                                                         | <p>Exits global configuration mode and returns to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## Verifying Define Interface Policy-Map AV Pairs AAA

Perform this optional task to verify the configuration of the Define Interface Policy-Map AV Pairs AAA feature.

## SUMMARY STEPS

1. **show policy-map interface**
2. **show running-config (on router)**
3. **show running-config (on client)**

## DETAILED STEPS

---

### Step 1 **show policy-map interface**

The **show policy-map interface** command shows the policy map voice attached to the ATM VC:

```
Router# show policy-map interface atm 4/0
ATM4/0: VC 1/101 -

Service-policy input: voice

Class-map: class-default (match-any)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match: any
```

### Step 2 **show running-config**

The following example displays the running configuration on the router showing the AAA setup; policy map configuration; ATM VC, PPPoA, and DBS-enabled CLI configuration; Virtual-Template configuration; and RADIUS server configuration:

```
Router# show running-config

.
.
.

aaa new-model
!
aaa user profile TEST
!
aaa authentication ppp default group radius
aaa authorization network default group radius
!

aaa session-id common
ip subnet-zero

.
.
.

policy-map voice
class Class-Default
fair-queue

.
.
.

!
interface ATM4/0.1 point-to-point
 pvc 1/101
 dbs enable
```

```

 encapsulation aal5mux ppp Virtual-Template1
 !
 .
 .
 .
interface Virtual-Template1
 ip address negotiated
 peer default ip address pool POOL1
 ppp authentication chap
 !
 .
 .
 .
 !
radius-server host 172.19.197.225 auth-port 1890 acct-port 1891
radius-server timeout 15
radius-server key 7 060506324F41
radius-server vsa send accounting
radius-server vsa send authentication
 !
 .
 .
 .
 !
 !
end

```

**Step 3 show running-config**

The following example displays the PPPoA client configuration:

```

.
.
.
!
interface ATM4/0.1 point-to-point
 pvc 1/101
 encapsulation aal5mux ppp Virtual-Template1
 !
 !
interface Virtual-Template1
 ip address negotiated
 peer default ip address pool POOL1
 ppp chap hostname userid
 ppp chap password 7 030752180500
 !
 .
 .
 .

```

---

# Configuration Examples for Define Interface Policy-Map AV Pairs AAA

This section contains the following examples:

- [Service-Policy Map Already Configured: Example, page 11](#)
- [Service-Policy Map Pulled: Example, page 12](#)
- [Service-Policy Map Pushed: Example, page 13](#)

## Service-Policy Map Already Configured: Example

The following example shows the existing MQC used to attach policy maps voice and outname under PVC 4/103. Using the **show policy-map interface** command shows that MQC-configured policy maps voice and outname are installed on the VC:

```
!
interface ATM4/0.3 multipoint
 no atm enable-ilmi-trap
 pvc 4/103
 service-policy input voice
 service-policy output outname
 !
Router# show policy-map interface atm 4/0.3
ATM4/0.3: VC 4/103 -

Service-policy input: voice

Class-map: class-default (match-any)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match: any
 0 packets, 0 bytes
 5 minute rate 0 bps

Service-policy output: outname

Class-map: class-default (match-any)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match: any
 0 packets, 0 bytes
 5 minute rate 0 bps
Router#
```

The following example shows MQC used to establish a PPPoEoA session, which causes the policy maps (test\_vc and dyn\_out) set up on the RADIUS server to be downloaded or “pulled” to the VC. The policy maps downloaded from the RADIUS server have higher precedence than the MQC service-policy maps (voice and outname) configured on the PVC. Using the **show policy-map interface** command shows that the pulled policy maps are installed on the VC:

```
!
interface ATM4/0.3 multipoint
 no atm enable-ilmi-trap
 pvc 4/103
 dba enable
 encapsulation aal5autopp Virtual-Template1
 service-policy input voice
```

```

 service-policy output outname
 !
end

Router# show policy-map interface atm 4/0.3
ATM4/0.3: VC 4/103 -

Service-policy input: test_vc

Class-map: class-default (match-any)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match: any
 0 packets, 0 bytes
 5 minute rate 0 bps

Service-policy output: dyn_out

Class-map: class-default (match-any)
 5 packets, 370 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match: any
 5 packets, 370 bytes
 5 minute rate 0 bps
Router#

PPPoE Session Information
Uniq ID PPPoE RemMAC Port VT VA State
 SID LocMAC
 2 2 0010.1436.bc70 ATM4/0.3 1 Vi3.1 PTA
 0010.1436.b070 VC: 4/103 UP
Router#
```

## Service-Policy Map Pulled: Example

The following example shows a policy named voice configured for input service policy on the RADIUS server. The router is already configured for PPPoA and AAA. The PPPoA session pulls the service policy name from the RADIUS server.

The **show policy-map interface** command displays the input service policy named voice attached to the ATM interface:

```

Router# show policy-map interface atm 4/0.1
ATM4/0: VC 1/101 -

Service-policy input: voice

Class-map: class-default (match-any)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match: any
```

Using the **show run interface** command displays the currently running configuration, but not the pulled service policy:

```
Router# show run interface atm 4/0.1

Building configuration...

Current configuration : 107 bytes
!
interface ATM 4/0.1
 pvc 1/101
 dbs enable
 encapsulation aal5mux ppp Virtual-Template 1
 !
!
end
```

## Service-Policy Map Pushed: Example

This configuration example has five parts that show that PPPoA sessions are established between a broadband remote access server (BRAS) and a routing gateway (RG), the change of authorization (CoA push request) that passes between a policy server and the BRAS, and how the pulled policy maps are replaced by pushed policy maps after the CoA request.

The five parts are: BRAS PPPoA configuration, RG PPPoA configuration, session information on BRAS prior to a push, debug on BRAS after receiving the CoA request, and session information on BRAS after a CoA push request has taken place.

The following example shows the current PPPoA configuration on BRAS:

```
aaa new-model
!
aaa authentication ppp default group radius
aaa authorization network default group radius
!
aaa server radius dynamic-author
 client <address> server-key <key>
!
aaa session-id common
!
ip routing
!
policy-map DefaultIn
 class class-default
 set ip precedence 0
policy-map DefaultOut
 class class-default
 set ip precedence 0
!
policy-map PullMapIn
 class class-default
 set ip precedence 0
policy-map PullMapOut
 class class-default
 set ip precedence 0
!
policy-map 7up
 class class-default
 fair-queue
policy-map Sprite
 class class-default
 bandwidth 1000
```

```

!
policy-map PushMapIn
 class class-default
 set ip precedence 0
policy-map PushMapOut
 class class-default
 set ip precedence 0
!
!
vc-class atm xyz
 protocol ppp Virtual-Template1
 encapsulation aal5snap
!
interface Loopback0
 ip address 10.1.1.2 255.255.255.0
!
interface ATM4/0
 no ip address
 no atm ilmi-keepalive
 no atm enable-ilmi-trap
 no clns route-cache
 no shutdown
!
interface ATM4/0.1 point-to-point
 no atm enable-ilmi-trap
 pvc 0/101
 class-vc xyz
 vbr-nrt 400 300 50
 dbs enable
 service-policy in DefaultIn
 service-policy out DefaultOut
!
!
interface Virtual-Template1
 ip unnumbered Loopback0
 ppp authentication chap
!
radius-server host <address> auth-port <port> acct-port <port>
radius-server key <key>
radius-server vsa send authentication

```

The following example shows the PPPoA configuration set up on the RG:

```

aaa new-model
!
aaa session-id common
!
ip routing
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.0
!
interface ATM2/0/0
 no ip address
 no atm ilmi-keepalive
 no atm enable-ilmi-trap
 no clns route-cache
 no shutdown
!
interface ATM2/0/0.1 point-to-point
 pvc 0/101
 protocol ppp Virtual-Template1
!

```

```

!
interface Virtual-Templat1
 ip unnumbered Loopback0
 no peer default ip address
 ppp chap hostname InOut
 ppp chap password 0 <password>

```

The following example uses the **show subscriber session all** command to display session information on BRAS prior to policy maps being pushed. PullMapIn and PullMapOut are the profiles pulled from the AAA server. The CoA request pushes the BRAS to change its input policy map (PullMapIn) and output policy map (PullMapOut) to PushMapIn and PushMapOut respectively.

```

Router# show subscriber session all

Current Subscriber Information:Total sessions 1

Unique Session ID:54
Identifier:InOut
SIP subscriber access type(s):PPPoA/PPP
Current SIP options:Req Fwding/Req Fwded
Session Up-time:00:00:32, Last Changed:00:00:12
AAA unique ID:55
Interface:Virtual-Access1.1

Policy information:
Context 6531F6AC:Handle C700008A
Authentication status:authen
User profile, excluding services:
 Framed-Protocol 1 [PPP]
 service-type 2 [Framed]
 ssg-account-info "S10.1.1.1"
 vc-qos-policy-in "PullMapIn"
 vc-qos-policy-out "PullMapOut"
Prepaid context:not present

Configuration sources associated with this session:
Interface:Virtual-Templat1, Active Time = 00:00:32

```

The following example displays the output of the **debug aaa coa** and **debug pppatm event** commands to show that the input policy map, PushMapIn, and output policy map, PushMapOut, have been applied or pushed on the BRAS after the BRAS received the CoA push request from the policy server:

```

2d20h:RADIUS:COA received from id 41 10.0.56.145:1700, CoA Request, len 122
2d20h:COA:10.0.56.145 request queued
2d20h: +++++ CoA Attribute List +++++
2d20h:6523AE20 0 00000001 service-type(276) 4 Framed
2d20h:6523AF4C 0 00000009 ssg-account-info(392) 9 S10.1.1.1
2d20h:6523AF5C 0 00000009 ssg-command-code(394) 1 17
2d20h:6523AF6C 0 00000009 vc-qos-policy-in(342) 7 PushMapIn
2d20h:6523AF7C 0 00000009 vc-qos-policy-out(343) 4 PushMapOut
2d20h:
2d20h: PPPATM:Received VALID vc policy PushMapIn
2d20h: PPPATM:Received VALID vc policy PushMapOut
2d20h:PPPATM:ATM4/0.1 0/101 [54], Event = SSS Msg Received = 5
2d20h:Service policy input PushMapIn policy output PushMapOut applied on 0/101
2d20h: PPPATM:Applied VALID vc policy PushMapIn and PushMapOut
2d20h:RADIUS(00000000):sending
2d20h:RADIUS(00000000):Send CoA Ack Response to 10.0.56.145:1700 id 41, len 20
2d20h:RADIUS: authenticator 04 D5 05 E2 FE A3 A6 E5 - B2 07 C0 A1 53 89 E0 FF

```

The following example uses the **show subscriber session all** command to display session information on the BRAS after the BRAS received the CoA push request from the policy server. The policy information shows that PushMapIn and PushMapOut are the current policy maps on the BRAS that were pushed by the CoA request:

```
Router# show subscriber session all
Current Subscriber Information:Total sessions 1

Unique Session ID:54
Identifier:InOut
SIP subscriber access type(s):PPPoA/PPP
Current SIP options:Req Fwding/Req Fwded
Session Up-time:00:00:44, Last Changed:00:00:22
AAA unique ID:55
Interface:Virtual-Access1.1

Policy information:
Context 6531F6AC:Handle C700008A
Authentication status:authen
User profile, excluding services:
 Framed-Protocol 1 [PPP]
 service-type 2 [Framed]
 ssg-account-info "S10.1.1.1"
 vc-qos-policy-in "PushMapIn"
 vc-qos-policy-out "PushMapOut"
Prepaid context:not present

Configuration sources associated with this session:
Interface:Virtual-Templat1, Active Time = 00:00:44
```

## Additional References

The following sections provide references related to the Define Interface Policy-Map AV Pairs AAA feature.

## Related Documents

| Related Topic                                                                                  | Document Title                                                           |
|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| WAN commands: complete command syntax, command mode, defaults, usage guidelines, and examples. | <a href="#">Cisco IOS Wide-Area Networking Command Reference</a>         |
| Quality of Service commands, such as <b>show policy-map</b> .                                  | <a href="#">Cisco IOS Quality of Service Solutions Command Reference</a> |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

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

# Feature Information for Define Interface Policy-Map AV Pairs AAA

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 Define Interface Policy-Map AV Pairs AAA

| Feature Name                             | Releases                                                                               | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------|----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Define Interface Policy-Map AV Pairs AAA | 12.3(7)XI2<br>12.2(28)SB<br>12.2(33)SRC<br>12.4(20)T<br>Cisco IOS<br>XE<br>Release 2.1 | <p>The Define Interface Policy-Map AV Pairs AAA feature introduces two Cisco Remote Authentication Dial-In User Service (RADIUS) vendor-specific attributes (VSAs) that allow a new policy map to be applied or an existing policy map to be modified, without affecting its session, during a Point-to-Point Protocol over ATM (PPPoA) or Point-to-Point Protocol over Ethernet over ATM (PPPoEoA) session establishment. The process occurs on the ATM virtual circuit (VC) level.</p> <p>This feature was integrated into Cisco IOS Release 12.3(7)XI2 and introduced for the Cisco 10000 series routers, Cisco 7200 series routers, and Cisco 7301 router. The “pull” functionality was implemented.</p> <p>This feature was integrated into Cisco IOS Release 12.2(28)SB. Support for the “push” functionality was added on the Cisco 10000 series routers, Cisco 7200 series routers, and Cisco 7301 router. The name for this functionality is RADIUS Push for MOD CLI Policies, which was integrated into the Define Interface Policy-Map AV Pairs AAA feature module.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRC.</p> <p>This feature was integrated into Cisco IOS Release 12.4(20)T.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.</p> |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, 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 Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, 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. (0910R)

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, 2006–2009 Cisco Systems, Inc. All rights reserved.





**TACACS+**





# Configuring TACACS+

---

**First Published: May 15, 1996**

**Last Updated: August 12, 2009**

TACACS+ provides detailed accounting information and flexible administrative control over authentication and authorization processes. TACACS+ is facilitated through AAA.

## 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 TACACS+” section on page 15](#).

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 Configuring TACACS+, page 2](#)
- [Restrictions for Configuring TACACS+, page 2](#)
- [Information About TACACS+, page 2](#)
- [How to Configure TACACS+, page 4](#)
- [TACACS+ Configuration Examples, page 8](#)
- [Additional References, page 13](#)
- [Feature Information for Configuring TACACS+, page 15](#)



---

**Americas Headquarters:**

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

## Prerequisites for Configuring TACACS+

You must have access to and must configure a TACACS+ server before the configured TACACS+ features on your network access server are available.

## Restrictions for Configuring TACACS+

TACACS+ can be enabled only through AAA commands.

## Information 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.

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+ 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.”

## How to Configure TACACS+

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+.
- Use the **aaa authentication** global configuration command to define method lists that use TACACS+ for authentication. See the “[Configuring Authentication](#)” feature module for more information.
- Use **line** and **interface** commands to apply the defined method lists to various interfaces. See the “[Configuring Authentication](#)” feature module for more information.
- 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. See the “[Configuring Authorization](#)” feature module for more information.
- If needed, use the **aaa accounting** command to enable accounting for TACACS+ connections. See the “[Configuring Accounting](#)” feature module for more information.

Perform the tasks in the following sections to configure TACACS+:

- [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)

## 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 used to encrypt all exchanges between the network access server and the TACACS+ daemon, 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** The same key must be configured 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>tacacs-server host</b> <i>name</i><br>[ <b>single-connection</b> ] [ <b>port</b> <i>integer</i> ] [ <b>timeout</b> <i>integer</i> ]<br>[ <b>key</b> <i>string</i> ] | Specifies and defines the IP address of the server host before configuring the AAA server-group. See <a href="#">“Identifying the TACACS+ Server Host”</a> section on page 5 for more information on the <b>tacacs-server host</b> command.                                                                                                                                                                                                                                                  |
| <b>Step 2</b> | 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.                                                                                                                                                                                                                                                                                                |
| <b>Step 3</b> | 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.<br><br>Repeat this step for each TACACS+ server in the AAA server group.<br><br><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 [“Identifying the TACACS+ Server Host” section on page 5](#) and [“Configuring AAA Server Groups” section on page 6](#) for more information.

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. |

|        | Command                                                                                                                                                                       | Purpose                                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 2 | Router(config)# <b>aaa dnis map</b> <i>dnis-number</i><br><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>accounting 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. See the “[Configuring Authentication](#)” feature module for more information.

## 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. See the “[Configuring Authorization](#)” feature module for more information.

## 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. See the “[Configuring Accounting](#)” feature module for more information.

## 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 igmp 0.0.1.2 255.255.0.0 any"
 }
}
```

## Additional References

The following sections provide references related to the Configuring TACACS+ feature.

### Related Documents

| Related Topic | Document Title                                          |
|---------------|---------------------------------------------------------|
| AAA           | <i>Cisco IOS Security Guide: Securing User Services</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:<br><br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC                                                    | Title |
|--------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature. | —     |

## 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 TACACS+

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 Configuring TACACS+

| Feature Name        | Releases                               | Feature Information                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuring TACACS+ | 10.0<br>Cisco IOS<br>XE<br>Release 2.1 | TACACS+ 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.<br><br>In Cisco IOS Release 10.0, this feature was introduced.<br><br>In Cisco IOS XE Release 2.1, this feature was implemented on the Cisco ASR 1000 series routers. |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card 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. (0907R)

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.

© 1996–2009 Cisco Systems, Inc. All rights reserved.





## Per VRF for TACACS+ Servers

---

**First Published: March 1, 2004**  
**Last Updated: October 12, 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 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 Per VRF for TACACS+ Servers, page 1](#)
- [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](#)

### Prerequisites for Per VRF for TACACS+ Servers

- TACACS+ server access is required.



---

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

- 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><br><br><b>Example:</b><br>Router> enable                                                                                       | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                               | Enters global configuration mode.                                                                                  |
| Step 3 | <b>ip vrf</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router (config)# ip vrf cisco                                                        | Configures a VRF table and enters VRF configuration mode.                                                          |
| Step 4 | <b>rd</b> <i>route-distinguisher</i><br><br><b>Example:</b><br>Router (config-vrf)# rd 100:1                                                 | Creates routing and forwarding tables for a VRF instance.                                                          |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router (config-vrf)# exit                                                                              | Exits VRF configuration mode.                                                                                      |
| Step 6 | <b>interface</b> <i>interface-name</i><br><br><b>Example:</b><br>Router (config)# interface Loopback0                                        | Configures an interface and enters interface configuration mode.                                                   |
| Step 7 | <b>ip vrf forwarding</b> <i>vrf-name</i><br><br><b>Example:</b><br>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> ]<br><br><b>Example:</b><br>Router (config-if)# ip address 10.0.0.2<br>255.0.0.0 | Sets a primary or secondary IP address for an interface.                                                           |
| Step 9 | <b>exit</b><br><br><b>Example:</b><br>Router (config-if)# exit                                                                               | Exits interface configuration mode.                                                                                |

|         | Command or Action                                                                                                                                                                                                                                             | Purpose                                                                                                                    |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Step 10 | <pre>aaa group server tacacs+ group-name</pre> <p><b>Example:</b><br/>Router (config)# aaa group server tacacs+ tacacs1</p>                                                                                                                                   | Groups different TACACS+ server hosts into distinct lists and distinct methods and enters server-group configuration mode. |
| Step 11 | <pre>server-private {ip-address   name} [nat] [<b>single-connection</b>] [<b>port</b> port-number] [<b>timeout</b> seconds] [<b>key</b> [0   7] string]</pre> <p><b>Example:</b><br/>Router (config-sg-tacacs)# server-private 10.1.1.1 port 19 key cisco</p> | Configures the IP address of the private TACACS+ server for the group server.                                              |
| Step 12 | <pre>ip vrf forwarding vrf-name</pre> <p><b>Example:</b><br/>Router (config-sg-tacacs)# ip vrf forwarding cisco</p>                                                                                                                                           | Configures the VRF reference of a AAA TACACS+ server group.                                                                |
| Step 13 | <pre>ip tacacs source-interface subinterface-name</pre> <p><b>Example:</b><br/>Router (config-sg-tacacs)# ip tacacs source-interface Loopback0</p>                                                                                                            | Uses the IP address of a specified interface for all outgoing TACACS+ packets.                                             |
| Step 14 | <pre>exit</pre> <p><b>Example:</b><br/>Router (config-sg-tacacs)# exit</p>                                                                                                                                                                                    | 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><br><br><b>Example:</b><br>Router> enable                                           | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <code>debug tacacs authentication</code><br><br><b>Example:</b><br>Router# debug tacacs authentication | Displays information about AAA/TACACS+ authentication.                                                              |
| Step 3 | <code>debug tacacs authorization</code><br><br><b>Example:</b><br>Router# debug tacacs authorization   | Displays information about AAA/TACACS+ authorization.                                                               |
| Step 4 | <code>debug tacacs accounting</code><br><br><b>Example:</b><br>Router# debug tacacs accounting         | Displays information about accountable events as they occur.                                                        |
| Step 5 | <code>debug tacacs packets</code><br><br><b>Example:</b><br>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> module.        |
| Per VRF AAA         | <a href="#">“Per VRF AAA”</a> module.                |
| 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:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

### RFCs

| RFC                                                                                                                         | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

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

# 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<br>12.2(33)SRA1<br>12.2(33)SXI<br>12.2(33)SXH4<br>Cisco IOS XE Release 2.1 | 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.<br><br>This feature was introduced in Cisco IOS Release 12.3(7)T.<br><br>This feature was integrated into Cisco IOS Release 12.2(33)SRA1.<br><br>This feature was integrated into Cisco IOS Release 12.2(33)SXI.<br><br>This feature was integrated into Cisco IOS Release 12.2(33)SXH4.<br><br>This feature was integrated into Cisco IOS XE Release 2.1.<br><br>The following commands were introduced or modified: <b>ip tacacs source-interface</b> , <b>ip vrf forwarding (server-group)</b> , <b>server-private (TACACS+)</b> . |

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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

---

**First Published: March 19, 2001**  
**Last Updated: September 23, 2009**

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 module lists the RADIUS attributes currently supported.

## 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 Attributes Overview and RADIUS IETF Attributes” section on page 20](#).

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

- [Information About RADIUS Attributes, page 2](#)
- [RADIUS IETF Attributes, page 5](#)
- [Additional References, page 17](#)
- [Feature Information for RADIUS Attributes Overview and RADIUS IETF Attributes, page 19](#)



---

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

# Information About RADIUS Attributes

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](#)
- [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.

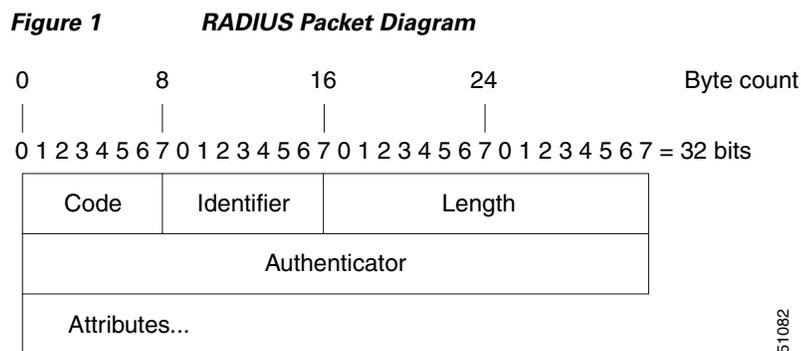
RADIUS vendor-specific attributes (VSAs) derived from one IETF attribute—vendor-specific (attribute 26). Attribute 26 allows a vendor to create an additional 255 attributes however they wish. That is, a vendor can create an attribute that does not match the data of any IETF attribute and encapsulate it behind attribute 26; thus, the newly created attribute is accepted if the user accepts attribute 26.

See “[Related Documents](#)” section on page 17 for more information on VSAs.

## 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 1](#) shows the fields within a RADIUS packet.



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 allows 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 authenticates 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 authenticates; 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"
```

## 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 1](#) 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 2](#) for a description of each listed attribute.

**Note**

---

Attributes implemented in special (AA) or early development (T) releases are added to the next mainline image.

---

**Table 1** 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  |
| 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   |

**Table 1** 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 |
|--------|-------------------------------------|------|------|------|---------|-------|------|------|------|
| 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  |
| 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   |

**Table 1** 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 |
|--------|------------------------------------|------|------|------|---------|-------|------|------|------|
| 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 2](#) lists and describes IETF RADIUS attributes. In cases where the attribute has a security server-specific format, the format is specified.

**Table 2** 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 <a href="#">RFC 2865</a> 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.                                                          |

Table 2 RADIUS IETF Attributes (continued)

| Number | IETF Attribute  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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>                                                        |
| 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> </ul> </li> </ul> <p>Exec User—Start an EXEC session.</p> <p>Service type is indicated by a particular numeric value as follows:</p> <ul style="list-style-type: none"> <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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

Table 2 RADIUS IETF Attributes (continued)

| Number | IETF Attribute     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8      | Framed-IP-Address  | 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.                                                                                                                                                                              |
| 9      | Framed-IP-Netmask  | 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.                                                                                                                                                                                                                                          |
| 10     | Framed-Routing     | 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.<br>Routing method is indicated by a numeric value as follows: <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          | 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.         |
| 12     | Framed-MTU         | 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.                                                                                                                                                                                                                                                                                                      |
| 13     | Framed-Compression | 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.<br>Compression protocol is indicated by a numeric value as follows: <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      | Indicates the host to which the user will connect when the Login-Service attribute is included. (This begins immediately after login.)                                                                                                                                                                                                                                                                                                            |
| 15     | Login-Service      | Indicates the service that should be used to connect the user to the login host.<br>Service is indicated by a numeric value as follows: <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     | Defines the TCP port with which the user is to be connected when the Login-Service attribute is also present.                                                                                                                                                                                                                                                                                                                                     |

Table 2 RADIUS IETF Attributes (continued)

| Number | IETF Attribute     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 18     | Reply-Message      | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 19     | Callback-Number    | Defines a dialing string to be used for callback.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 20     | Callback-ID        | Defines the name (consisting of one or more octets) of a place to be called, to be interpreted by the network access server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 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 1</a> lists supported vendor-specific RADIUS attributes (IETF attribute 26). The "TACACS+ Attribute-Value Pairs" module provides a complete list of supported TACACS+ attribute-value (AV) pairs that can be used with IETF attribute 26. (<a href="#">RFC 2865</a>)</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."                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

Table 2 RADIUS IETF Attributes (continued)

| Number | IETF Attribute           | Description                                                                                                                                                                                                                                                                                                                                                                  |
|--------|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.                                                                   |
| 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. |

Table 2 RADIUS IETF Attributes (continued)

| Number | IETF Attribute        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

Table 2 RADIUS IETF Attributes (continued)

| Number | IETF Attribute                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 52     | Acct-Input-Gigawords            | Indicates how many times the Acct-Input-Octets counter has wrapped around 2 <sup>32</sup> over the course of the provided service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 53     | Acct-Output-Gigawords           | Indicates how many times the Acct-Output-Octets counter has wrapped around 2 <sup>32</sup> while delivering service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 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 the <a href="#">Cisco IOS Configuration Fundamentals Configuration Guide</a>, Release 12.4T.)</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. See the <a href="#">Cisco IOS Configuration Fundamentals Command Reference</a> for more information on this command.</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 2 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<br/> 127.0.0.1 would indicate that loopback1 IP address is to be used<br/> ...<br/> 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 2 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.<br><br>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*.

# Additional References

The following sections provide references related to RADIUS IETF attributes.

## Related Documents

| Related Topic                     | Document Title                                                   |
|-----------------------------------|------------------------------------------------------------------|
| RADIUS                            | “ <a href="#">Configuring RADIUS</a> ” module.                   |
| Authentication                    | “ <a href="#">Configuring Authentication</a> ” module.           |
| Authorization                     | “ <a href="#">Configuring Authorization</a> ” module.            |
| Accounting                        | “ <a href="#">Configuring Accounting</a> ” module.               |
| RADIUS Vendor-Specific Attributes | “ <a href="#">RADIUS Vendor-Proprietary Attributes</a> ” module. |

## Standards

| Standard | Title |
|----------|-------|
| None.    | —     |

## MIBs

| MIB   | MIBs Link                                                                                                                                                                                                              |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC                      | Title                                                              |
|--------------------------|--------------------------------------------------------------------|
| <a href="#">RFC 2865</a> | <i>Remote Authentication Dial In User Service (RADIUS)</i>         |
| <a href="#">RFC 2866</a> | <i>RADIUS Accounting</i>                                           |
| <a href="#">RFC 2867</a> | <i>RADIUS Accounting Modifications for Tunnel Protocol Support</i> |
| <a href="#">RFC 2868</a> | <i>RADIUS Attributes for Tunnel Protocol Support</i>               |
| <a href="#">RFC 2869</a> | <i>RADIUS Extensions</i>                                           |

## Technical Assistance

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

# Feature Information for RADIUS Attributes Overview and RADIUS IETF Attributes

Table 3 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

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



## Note

Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 3** Feature Information for RADIUS Attributes Overview and RADIUS IETF Attributes

| Feature Name           | Releases                                           | Feature Information                                                                                                                                 |
|------------------------|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| RADIUS IETF Attributes | Cisco IOS Release 11.1<br>Cisco IOS XE Release 2.1 | This feature was introduced in Cisco IOS Release 11.1.<br>This feature was introduced on Cisco ASR 1000 Series Routers for Cisco IOS XE Release 2.1 |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLynx, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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 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)**

| Number | Vendor-Proprietary Attribute | Description                                                                                                                                                                                                                                                                  |
|--------|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.<br><br>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.<br><br>In 12.2(1) XE, this feature was introduced. |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLynX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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 Attribute 8 (Framed-IP-Address) in Access Requests

---

**First Published: August 12, 2002**  
**Last Updated: September 8, 2009**

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 IP addresses. With the RADIUS server, service applications can begin preparing user login information to have available in advance of a successful user authentication with the RADIUS server.

## 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 8 \(Framed-IP-Address\) in Access Requests” 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 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 2](#)
- [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**

- [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

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.

## 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 3](#)

## 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><br><br><b>Example:</b><br>Router> <code>enable</code>                                                                                           | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br>Router# <code>configure terminal</code>                                                                   | Enters global configuration mode.                                                                                  |
| Step 3 | <code>radius-server attribute 8 include-in-access-req</code><br><br><b>Example:</b><br>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><br><br><b>Example:</b><br>Router> enable                                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                           |
| Step 2 | <code>more system:running-config</code><br><br><b>Example:</b><br>Router# more system:running-config | Displays the contents of the current running configuration file. (Note that the <code>more system:running-config</code> command has replaced the <code>show running-config</code> command.) |
| Step 3 | <code>debug radius</code><br><br><b>Example:</b><br>Router# debug radius                             | Displays information associated with RADIUS. The output of this command shows whether attribute 8 is being sent in access requests.                                                         |

## Configuration Examples for RADIUS Attribute 8 (Framed-IP-Address) in Access Requests

This section provides the following configuration example:

- [NAS Configuration That Sends the IP Address of the Dial-in Host to the RADIUS Server in the RADIUS Access Request](#)

### NAS Configuration That Sends the IP Address of the Dial-in Host to the RADIUS Server in the RADIUS Access Request

The following example shows a NAS configuration that sends the IP address of the dial-in host to the RADIUS server in the RADIUS access request. The NAS is configured for RADIUS authentication, authorization, and accounting (AAA). A pool of IP addresses (async1-pool) has been configured and applied at interface Async1.

```
aaa new-model
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
!
ip address-pool local
!
interface Async1
 peer default ip address pool async1-pool
!
ip local pool async1-pool 209.165.200.225 209.165.200.229
!
radius-server host 172.31.71.146 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute 8 include-in-access-req
radius-server key radhost<xxx>: Example
```

## Additional References

The following sections provide references related to the RADIUS Attribute 8 (Framed-IP-Address) in Access Requests feature.

### Related Documents

| Related Topic                                     | Document Title                                                                                            |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| Configuring authentication and configuring RADIUS | “Configuring Authentication” and “Configuring RADIUS” chapters, <i>Cisco Security Configuration Guide</i> |
| RFC 2138 (RADIUS)                                 | RFC 2138, <i>Remote Authentication Dial In User Service (RADIUS)</i>                                      |

### Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

### MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

### RFCs

| RFC                                                                                                                         | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

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

# 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<br>12.2(28)SB<br>12.2(33)SRC | <p>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 IP addresses. With the RADIUS server, service applications can begin preparing user login information to have available in advance of a successful user authentication with the RADIUS server.</p> <p>The following sections provide information about this feature:</p> <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 2</a></li> <li>• <a href="#">Configuration Examples for RADIUS Attribute 8 (Framed-IP-Address) in Access Requests, page 4</a></li> </ul> <p>The following commands were introduced or modified:<br/><b>radius-server attribute 8 include-in-access-req.</b></p> |
| Sticky IP                                                 | Cisco IOS XE Release 2.1               | This feature was introduced on Cisco ASR 1000 Series Routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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 Tunnel Attribute Extensions

---

**First Published: November 27, 2000**

**Last Updated: October 6, 2009**

The RADIUS Tunnel Attribute Extensions feature allows a name to be specified (other than the default) for the tunnel initiator and the tunnel terminator in order to establish a higher level of security when setting up VPN tunneling.

## 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 Tunnel Attribute Extensions”](#) 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 Tunnel Attribute Extensions, page 2](#)
- [Restrictions for RADIUS Tunnel Attribute Extensions, page 2](#)
- [Information About RADIUS Tunnel Attribute Extensions, page 2](#)
- [How to Verify RADIUS Attribute 90 and RADIUS Attribute 91, page 3](#)
- [Configuration Examples for RADIUS Tunnel Attribute Extensions, page 3](#)
- [Additional References, page 5](#)
- [Feature Information for RADIUS Tunnel Attribute Extensions, page 7](#)
- [Glossary, page 7](#)



---

**Americas Headquarters:**

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

## Prerequisites for RADIUS Tunnel Attribute Extensions

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.

## Restrictions for RADIUS Tunnel Attribute Extensions

Your RADIUS server must support tagged attributes to use RADIUS tunnel attributes 90 and 91.

## Information About RADIUS Tunnel Attribute Extensions

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.

## How RADIUS Tunnel Attribute Extensions Work

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 1](#).



### 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 1** 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.

## How to Verify 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 for RADIUS Tunnel Attribute Extensions

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

```

# Additional References

The following sections provide references related to RADIUS Tunnel Attribute Extensions.

## Related Documents

| Related Topic                          | Document Title                                                                  |
|----------------------------------------|---------------------------------------------------------------------------------|
| Authentication                         | <a href="#">“Configuring Authentication”</a> module.                            |
| RADIUS Attributes                      | <a href="#">“RADIUS Attributes Overview and RADIUS IETF Attributes”</a> module. |
| Virtual private dialup networks (VPDN) | <a href="#">Cisco IOS VPDN Configuration Guide</a> , Release 15.0.              |

## Standards

| Standard | Title |
|----------|-------|
| None.    | —     |

## MIBs

| MIB   | MIBs Link                                                                                                                                                                                                              |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><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> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

# Feature Information for RADIUS Tunnel Attribute Extensions

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 RADIUS Tunnel Attribute Extensions

| Feature Name                                               | Releases                                                       | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Feature Information for RADIUS Tunnel Attribute Extensions | 12.1(5)T<br>12.2(4)B3<br>12.2(13)T<br>Cisco IOS XE Release 2.1 | The RADIUS Tunnel Attribute Extensions feature allows a name to be specified (other than the default) for the tunnel initiator and the tunnel terminator in order to establish a higher level of security when setting up VPN tunneling.<br><br>This feature was introduced in Cisco IOS Release 12.1(5)T.<br><br>This feature was integrated into Cisco IOS Release 12.2(4)B3.<br><br>This feature was integrated into Cisco IOS Release 12.2(13)T.<br><br>This feature was introduced on Cisco ASR 1000 Series Routers. |

## 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, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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.



# 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 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 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](#)
- [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 [“Related Documents” section on page 4](#).

## 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><br><br><b>Example:</b><br>Router> enable                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>debug aaa authorization</b><br><br><b>Example:</b><br>Router# debug aaa authorization | Displays information about AAA/TACACS+ authorization.                                                            |
| Step 3 | <b>debug aaa per-user</b><br><br><b>Example:</b><br>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                                                                                                                                                         |
|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AAA per-user and QoS configurations and information about the <b>policy-map</b> command | <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 |
|-----------|-------|
| None      | —     |

### MIBs

| MIBs | MIBs Link                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

### RFCs

| RFCs                                                   | Title |
|--------------------------------------------------------|-------|
| 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 Per-User QoS via AAA Policy Name

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://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 Per-User QoS via AAA Policy Name

| Feature Name                     | Releases                                                             | Feature Information                                                                                                                                                                                                                                                                                      |
|----------------------------------|----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Per-User QoS via AAA Policy Name | 12.2(15)B<br>12.2(15)T<br>12.2(33)SRC<br>Cisco IOS XE<br>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.<br><br>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, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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.





# AAA Per VC QoS Policy Support

---

**First Published: June 27, 2005**

**Last Updated: November 20, 2009**

The AAA Per VC QoS Policy Support feature provides the ability to modify an existing quality of service (QoS) profile applied to a session while that session remains active using new Cisco attribute-value (AV) pairs that specify service policy output and service policy input.

## 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 Per VC QoS Policy Support”](#) 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://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for AAA Per VC QoS Policy Support, page 2](#)
- [Restrictions for AAA Per VC QoS Policy Support, page 2](#)
- [Information About AAA Per VC QoS Policy Support, page 2](#)
- [Configuration Examples for AAA Per VC QoS Policy Support, page 4](#)
- [Additional References, page 5](#)
- [Feature Information for AAA Per VC QoS Policy Support, page 7](#)



---

**Americas Headquarters:**

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

# Prerequisites for AAA Per VC QoS Policy Support

You should be familiar with defining policy maps for managing subscriber sessions, and with configuring QoS traffic conditioning. See the [“Additional References”](#) section for information on these topics.

## Restrictions for AAA Per VC QoS Policy Support

Although there are no specific restrictions for using the AAA Per VC QoS Policy Support feature, defect report CSCef69140 describes a problem whereby in PPPoA sessions, an input service policy cannot be applied at the ATM virtual circuit (VC) level. Instead, an input service policy, and therefore an input policy AV pair, must be applied under interface virtual template mode.

Also, read through the configuration guidelines in the [“Interface Policy Map AAA Attributes”](#) section before using the attributes described in this document.

## Information About AAA Per VC QoS Policy Support

Familiarize yourself with the following information before using the attributes described in this document:

- [RADIUS Push and Pull, page 2](#)
- [Interface Policy Map AAA Attributes, page 3](#)

## RADIUS Push and Pull

Cisco Systems software offers applications for the DSL aggregation market and service providers that make powerful use of dynamic policy maps. Policy maps govern user services to be deployed in the network and are triggered by a service or by a user—concepts referred to as push and pull. Pull refers to a policy applied during authentication. Push refers to the dynamic change of policy on the session using Change of Authorization (CoA) message. Before the AAA Per VC QoS Policy Support feature introduced in Cisco IOS Release 12.4(2)T, there was no RADIUS push and pull capability for a policy map at the ATM VC level. RADIUS only supported dynamic bandwidth selection and virtual access interface policy maps applied during the establishment of a PPP session. The AAA Per VC QoS Policy Support feature provides support for RADIUS push and pull capability for a policy map at the ATM VC level.

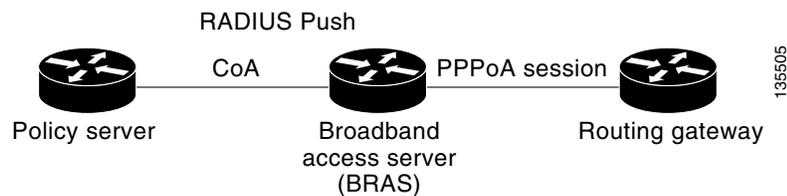
RADIUS pull of policy maps on a VC means that a policy map can be applied on the VC while a PPP over ATM (PPPoA) session is being established. PPPoA sessions are established between a policy server and a routing gateway.

Service policies are applied only when a subscriber first authenticates the VC. Software creates an identifier that is used as the session unique identifier between the router and the RADIUS server using RADIUS Internet Engineering Task Force (IETF) attribute 44. This identifier is sent with an Access Request message and all accounting records for that session.

RADIUS push functionality provides the ability to modify an existing QoS profile applied to a session while that session remains active. A policy server governs the authorization of active sessions with its ability to send a Change of Authorization (CoA) message (see [Figure 1](#)). Specific events can trigger the

CoA message and allow modification of the QoS configuration. Implementation of RADIUS push eliminates the need to preprovision subscribers, allowing QoS policies to be transparently applied where and when required without the disruption of session reauthentication.

**Figure 1** **RADIUS Push**



These abilities provide a high degree of flexibility, smaller configuration files, and more efficient use of queuing resources. And perhaps more importantly, RADIUS push and pull eliminates the need to statically configure a policy map on every VC or VLAN.

This feature is implemented by Cisco AV pairs that identify QoS policies configured on the router from a RADIUS server by defining service policy output and service policy input. The AV pairs place the appropriate policy map, which is identified by name, directly on the interface. The interface can be either an ATM VC or Ethernet VLAN.

After the initial subscriber authentication, authorization process, RADIUS returns the appropriate AV name for the policy maps to be applied at the VC and virtual-access interface level. The QoS policy maps define the subscriber user experience for broadband service and can be leveraged to deliver higher value services such as VoIP and video.

## Interface Policy Map AAA Attributes

Two new generic Cisco RADIUS VSA attributes are introduced by the AAA Per VC QoS Policy Support feature, as follows:

```
cisco-avpair = "atm:vc-qos-policy-in=in-policy-name"
cisco-avpair = "atm:vc-qos-policy-out=out-policy-name"
```

Use these attributes in the RADIUS server profile to define service policy output and service policy input. The AV pairs place the appropriate policy map, which is identified by name, directly on the interface. The interface can be either an ATM VC or Ethernet VLAN.

The AAA Per VC QoS Policy Support feature also replaces the following generic Cisco RADIUS vendor-specific attribute (VSA) attributes:

```
cisco-avpair = "ip:sub-policy-In=in-policy-name"
cisco-avpair = "ip:sub-policy-Out=out-policy-name"
```

with the following new attributes:

```
cisco-avpair = "ip:sub-qos-policy-in=in-policy-name"
cisco-avpair = "ip:sub-qos-policy-out=out-policy-name"
```

The replaced attributes will be supported for several more software releases, but profiles should be updated with the new attributes as soon as it is feasible to do so.

Remember the following guidelines as you configure these attributes:

- A policy map pulled or pushed from the RADIUS server has a higher precedence than a policy map configured under a permanent virtual circuit (PVC).

- The Cisco IOS **show policy-map interface EXEC** command will display the policy map pushed or pulled from the RADIUS server. This policy map is actually used by the driver, even though the policy map was configured using the **service-policy** command under PVC configuration mode.
- Once a policy map is pushed or pulled on the VC and successfully installed or updated, any configuration or removal of the configuration would affect only the running configuration, and not the driver and actual policy map used by the VC.
- You must enable dynamic bandwidth selection using the **dbns enable** command. Dynamic policies that are pulled and pushed from the RADIUS server must be specifically disabled using the **no dbns enable** command.

## Configuration Examples for AAA Per VC QoS Policy Support

This section contains the following examples:

- [RADIUS Interface Policy Map Profile: Example, page 4](#)
- [Define the Policy Map on the Router: Example, page 4](#)
- [Display the Service Policy: Example, page 5](#)

### RADIUS Interface Policy Map Profile: Example

Following is an example of a RADIUS profile defining an input service policy named test\_vc:

```
radius subscriber 2
vsa cisco generic 1 string "atm:vc-qos-policy-in=test_vc"
attribute 1 string "user@cisco.com"
attribute 44 string "00000002"
!
radius client 192.168.1.4 access-ports 1645 1645 accounting-ports 1646 1646
radius host 192.168.1.3 auth-port 1645 acct-port 1646 key 0 cisco
radius host 192.168.1.4 auth-port 1645 acct-port 1646
radius retransmit 0
radius timeout 15
radius key 0 cisco
radius server 192.168.1.4
client 192.168.1.3 shared-secret word
```

### Define the Policy Map on the Router: Example

The following example shows the Cisco IOS commands that are used to define the service policy on the router:

```
!
interface ATM4/0
no ip address
no atm ilmi-keepalive
pvc 1/101
dbns enable
service-policy input test_vc
!
end
```

## Display the Service Policy: Example

The following example shows the report from the **show policy-map interface** command when the policy map named test\_vc has been pushed on PVC 1/101:

```
Router# show policy interface atm 4/0

ATM4/0: VC 1/101 -

Service-policy input: test_vc

Class-map: class-default (match-any)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
Match: any
```

## Additional References

The following sections provide references related to the AAA Per VC QoS Policy Support feature.

### Related Documents

| Related Topic                    | Document Title                                                                                                                                                                               |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service policies and policy maps | <ul style="list-style-type: none"> <li><i>ISA Configuration Guide</i></li> <li><i>ISA Command Reference</i></li> </ul>                                                                       |
| Cisco VSA attributes             | <ul style="list-style-type: none"> <li><i>Cisco IOS Security Configuration Guide</i></li> </ul>                                                                                              |
| QoS traffic conditioning         | <ul style="list-style-type: none"> <li><i>Cisco IOS Quality of Service Solutions Configuration Guide</i></li> <li><i>Cisco IOS Quality of Service Solutions Command Reference</i></li> </ul> |

### Standards

| Standard                                                                                              | Title |
|-------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported, and support for existing standards has not been modified. | —     |

### MIBs

| MIB                                                                                         | MIBs Link                                                                                                                                                                                                              |
|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported, and support for existing MIBs has not been modified. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC                                                                  | Title |
|----------------------------------------------------------------------|-------|
| No new or modified RFCs are supported, and support for existing RFCs | —     |

## 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/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a> |

# Feature Information for AAA Per VC QoS Policy Support

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

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



## Note

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

**Table 1** Feature Information for AAA Per VC QoS Policy Support

| Feature Name                  | Releases                | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AAA Per VC QoS Policy Support | 12.4(2)T<br>12.2(33)SRE | The AAA Per VC QoS Policy Support feature provides the ability to modify an existing quality of service (QoS) profile applied to a session while that session remains active using new Cisco attribute-value (AV) pairs that specify service policy output and service policy input.<br><br>In 12.4(2)T, this feature was introduced on the Cisco 10000.<br><br>In Cisco IOS Release 12.2(33)SRE, the AAA Per VC QoS Policy Support feature was added for the Cisco 7600 series router. |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, 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. (0910R)

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.





## **TACACS+ Attributes**





# TACACS+ Attribute-Value Pairs

---

**Last Updated: October 9, 2009**

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 module lists the TACACS+ AV pairs currently supported.

## Contents

- [Information About TACACS+ Attribute-Value Pairs, page 1](#)
- [Additional References, page 23](#)

## Information About TACACS+ Attribute-Value Pairs

The following sections contain information about TACACS+ Attribute-Value Pairs:

- [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 1](#) lists and describes the supported TACACS+ authentication and authorization AV pairs and specifies the Cisco IOS release in which they are implemented.



---

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

**Table 1** 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  |
| addr-pool=x         | Specifies the name of a local pool from which to get the address of the remote host. Used with service=ppp and protocol=ip.<br><br>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:<br><br><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><br>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. | 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  |

**Table 1** 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-arg=x    | 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.<br><br><b>Note</b> This TACACS+ AV pair cannot be used with RADIUS attribute 26.                                        | yes  |
| 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.<br><br><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  |

**Table 1** Supported TACACS+ Authentication and Authorization AV Pairs (continued)

| Attribute                 | Description                                                                                                                                                                                                                                                                                                                                                                                                         | 11.0 | 11.1 | 11.2 | 11.3 | 12.0 | 12.1 | 12.2 |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|------|------|------|------|
| inac1=x                   | ASCII identifier for an interface input access list. Used with service=ppp and protocol=ip. Per-user access lists do not currently work with ISDN interfaces.                                                                                                                                                                                                                                                       | yes  |
| interface-config#<br><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.<br><br><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  |

**Table 1** 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-nosession-timeout | Specifies the number of seconds that a tunnel will stay active with no sessions before timing out and shutting down. Used with service=ppp and protocol=vpdn.                                                                                                                                                                                       | no   | no   | no   | no   | no   | yes  | yes  |
| l2tp-tos-reflect       | Copies the IP ToS field from the IP header of each payload packet to the IP header of the tunnel packet for packets entering the tunnel at the LNS. Used with service=ppp and protocol=vpdn.                                                                                                                                                        | no   | no   | no   | no   | no   | yes  | yes  |
| l2tp-tunnel-authen     | If this attribute is set, it performs L2TP tunnel authentication. Used with service=ppp and protocol=vpdn.                                                                                                                                                                                                                                          | no   | no   | no   | no   | no   | yes  | yes  |
| l2tp-tunnel-password   | Shared secret used for L2TP tunnel authentication and AVP hiding. Used with service=ppp and protocol=vpdn.                                                                                                                                                                                                                                          | no   | no   | no   | no   | no   | yes  | yes  |
| l2tp-udp-checksum      | This is an authorization attribute and defines whether L2TP should perform UDP checksums for data packets. Valid values are “yes” and “no.” The default is no. Used with service=ppp and protocol=vpdn.                                                                                                                                             | no   | no   | no   | no   | no   | yes  | yes  |
| link-compression=      | Defines whether to turn on or turn off “stac” compression over a PPP link. Used with service=ppp.<br><br>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  |

**Table 1** Supported TACACS+ Authentication and Authorization AV Pairs (continued)

| Attribute         | Description                                                                                                                                                                                                                                                                                                                                        | 11.0                            | 11.1 | 11.2 | 11.3 | 12.0 | 12.1 | 12.2 |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|------|------|------|------|------|------|
| 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  |
| 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<br>(PPP<br>/IP<br>only<br>) | 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 1** 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.<br>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 1 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 1** 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 1** 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  |

See “[Related Documents](#)” section on page 23 for the documents used to configure TACACS+, and TACACS+ authentication and authorization.

## TACACS+ Accounting AV Pairs

[Table 2](#) lists and describes the supported TACACS+ accounting AV pairs and specifies the Cisco IOS release in which they are implemented.

**Table 2** 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 3</a> for a list of Disconnect-Cause values and their meanings. | no   | no   | no   | yes  | yes  | yes  | yes  |

**Table 2** 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 2** 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 2** 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 3 lists the cause codes and descriptions for the Disconnect Cause Extended (disc-cause-ext) attribute.

**Table 3** 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  |

# Additional References

The following sections provide references related to TACACS+ Attribute-Value Pairs.

## Related Documents

| Related Topic          | Document Title                                         |
|------------------------|--------------------------------------------------------|
| TACACS+ authentication | “ <a href="#">Configuring Authentication</a> ” module. |
| TACACS+ Authorization  | “ <a href="#">Configuring Authorization</a> ” module.  |
| TACACS+ accounting     | “ <a href="#">Configuring Accounting</a> ” module.     |
| TACACS+                | “ <a href="#">Configuring TACACS+</a> ” module.        |

## Standards

| Standard | Title |
|----------|-------|
| None.    | —     |

## MIBs

| MIB   | MIBs Link                                                                                                                                                                                                              |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><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> |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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.

© 2009 Cisco Systems, Inc. All rights reserved.



## **Secure Shell (SSH)**





# Configuring Secure Shell

---

**First Published: December 12, 2004**  
**Last Updated: September 11, 2009**

The Secure Shell (SSH) feature 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 “[Secure Shell Version 2 Support](#)” feature module.



**Note**

---

Hereafter, unless otherwise noted, the term “SSH” denotes “SSH Version 1” only.

---

## 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 Secure Shell](#)” section on page 12.

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, page 2](#)
- [Restrictions, page 2](#)
- [Information About Secure Shell, page 2](#)
- [How to Configure SSH, page 3](#)
- [Troubleshooting Tips, page 5](#)
- [Configuration Examples for SSH, page 5](#)



---

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

- [Additional References, page 10](#)
- [Feature Information for Configuring Secure Shell, page 12](#)

## Prerequisites

Perform the following tasks before configuring SSH:

- Download the required image on the router. (The SSH server requires an IPsec (DES or 3DES) encryption software image from Cisco IOS Release 12.1(1)T or later; the SSH client requires an IPsec (DES or 3DES) encryption software image from Cisco IOS Release 12.1(3)T or later.) See the *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.4T for more information on downloading a software image.
- Configure a host name and host domain for your router by using the **hostname** and **ip domain-name** commands in global configuration mode.
- Generate an RSA key pair for your router, which automatically enables SSH and remote authentication by entering the **crypto key generate rsa** command in global configuration mode.

**Note**

---

To delete the RSA key-pair, use the **crypto key zeroize rsa** global configuration command. Once you delete the RSA key-pair, you automatically disable the SSH server.

---

- Configure user authentication for local or remote access. You can configure authentication with or without AAA. For more information, see the “[Configuring Authentication](#),” “[Configuring Authorization](#),” and “[Configuring Accounting](#)” feature modules for more information.

## Restrictions

SSH has the following 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.

## Information About Secure Shell

The following sections provide information about SSH:

- [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 works 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.

---

## How to Configure SSH

Perform the following tasks for configuring SSH.

- [Configuring SSH Server](#) (Required)
- [Verifying SSH](#) (Optional)

## Configuring SSH Server

Perform the following steps to enable the Cisco router for SSH.

**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. If SSH parameters are not configured, then the default values are used.

---

### SUMMARY STEPS

1. **enable**
2. **configure terminal**

### 3. `ip ssh {timeout seconds | authentication-retries integer}`

#### DETAILED STEPS

|        | Command or Action                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <pre>enable</pre> <p><b>Example:</b><br/>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><br/>Router# configure terminal </p>                                       | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 3 | <pre>ip ssh {timeout seconds   authentication-retries integer}</pre> <p><b>Example:</b><br/>Router# ip ssh timeout 30 </p> | (Required) Select one of the SSH control variables. <ul style="list-style-type: none"> <li>The <i>seconds</i> argument specifies the timeout in seconds, not exceeding 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.               <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> </li> <li>The <i>integer</i> argument specifies the number of authentication retries, not to exceeding 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. See the “[IPsec and Quality of Service](#)” feature module for more information.
  - No domain specified  
You must configure a host domain for the router using the **ip domain-name** global configuration command. See the “[IPsec and Quality of Service](#)” feature module for more information.
- The number of allowable SSH connections is limited to the maximum number of vty's configured for the router. Each SSH connection uses 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.

## Configuration Examples for SSH

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 sqe-registers
no exception linecard slot 1 sqe-registers
no exception linecard slot 2 sqe-registers
no exception linecard slot 3 sqe-registers
no exception linecard slot 4 sqe-registers
no exception linecard slot 5 sqe-registers
no exception linecard slot 6 sqe-registers
end

```

## Additional References

The following sections provide references related to the SSH feature.

## Related Documents

| Related Topic                                       | Document Title                                                                                                                                           |
|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authentication, Authorization, and Accounting (AAA) | <a href="#">“Configuring Authentication,”</a> <a href="#">“Configuring Authorization,”</a> and <a href="#">“Configuring Accounting”</a> feature modules. |
| IPsec                                               | <a href="#">“IPsec and Quality of Service”</a> feature module.                                                                                           |
| SSH Version 2                                       | <a href="#">“Secure Shell Version 2 Support”</a> feature module.                                                                                         |
| Downloading a software image.                       | <a href="#">Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.4T.</a>                                                                 |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC                                                    | Title |
|--------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature. | —     |

## 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 Configuring Secure Shell

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 Configuring Secure Shell

| Feature Name | Releases                                   | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Secure Shell | 12.0(5)S<br>Cisco IOS<br>XE<br>Release 2.1 | The Secure Shell (SSH) feature 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 <b>rexec</b> and <b>rsh</b> tools. There are currently two versions of SSH available: SSH Version 1 and SSH Version 2. This document describes SSH Version 1.<br><br>This feature was introduced in Cisco IOS Release 12.0(5)S.<br><br>This feature was introduced on Cisco ASR 1000 Series Routers. |

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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.





# Reverse SSH Enhancements

---

**First Published: September 18, 2004**

**Last Updated: October 7, 2009**

The Reverse SSH Enhancements feature, which is supported for SSH Version 1 and 2, provides an alternative way to configure reverse Secure Shell (SSH) so that separate lines do not need to be configured for every terminal or auxiliary line on which SSH must be enabled. This feature also eliminates the rotary-group limitation.

## 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 Reverse SSH Enhancements” 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.

## 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](#)
- [Feature Information for Reverse SSH Enhancements, page 10](#)



---

**Americas Headquarters:**

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

## 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 telnet 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. Telnet makes it easy to reach the router console from anywhere simply by telnet to the terminal server on a specific line. This telnet approach can be used to configure a router even if all network connectivity to that router is disconnected. Reverse telnet also allows modems that are attached to Cisco IOS routers to be used for dial-out (usually with a rotary device).

## Reverse SSH

Reverse telnet can be accomplished using SSH. Unlike reverse telnet, 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 [“How to Configure Reverse SSH Enhancements” section on page 2.](#)

## 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><br><br><b>Example:</b><br>Router> enable                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                     |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                           | Enters global configuration mode.                                                                                                      |
| Step 3 | <b>line</b> <i>line-number</i> [ <i>ending-line-number</i> ]<br><br><b>Example:</b><br>Router# line 1 3                  | Identifies a line for configuration and enters line configuration mode.                                                                |
| Step 4 | <b>no exec</b><br><br><b>Example:</b><br>Router (config-line)# no exec                                                   | Disables EXEC processing on a line.                                                                                                    |
| Step 5 | <b>login authentication</b> <i>listname</i><br><br><b>Example:</b><br>Router (config-line)# login authentication default | Defines a login authentication mechanism for the lines.<br><br><b>Note</b> The authentication method must use a username and password. |

|        | Command or Action                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|--------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6 | <code>transport input ssh</code><br><br><b>Example:</b><br>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 <code>ssh</code> keyword must be used for the Reverse SSH Enhancements feature.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 7 | <code>exit</code><br><br><b>Example:</b><br>Router (config-line)# exit                                             | Exits line configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 8 | <code>exit</code><br><br><b>Example:</b><br>Router (config)# exit                                                  | Exits global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Step 9 | <code>ssh -l userid:{number} {ip-address}</code><br><br><b>Example:</b><br>Router# ssh -l lab:1 router.example.com | Specifies the user ID to use when logging in on the remote networking device that is running the SSH server. <ul style="list-style-type: none"> <li><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><br><br><b>Example:</b><br>Router> enable                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                            |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                           | Enters global configuration mode.                                                                                                                                                                           |
| Step 3 | <b>line <i>line-number</i> [<i>ending-line-number</i>]</b><br><br><b>Example:</b><br>Router# line 1 200                  | Identifies a line for configuration and enters line configuration mode.                                                                                                                                     |
| Step 4 | <b>no exec</b><br><br><b>Example:</b><br>Router (config-line)# no exec                                                   | Disables EXEC processing on a line.                                                                                                                                                                         |
| Step 5 | <b>login authentication <i>listname</i></b><br><br><b>Example:</b><br>Router (config-line)# login authentication default | Defines a login authentication mechanism for the lines.<br><b>Note</b> The authentication method must use a username and password.                                                                          |
| Step 6 | <b>rotary <i>group</i></b><br><br><b>Example:</b><br>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><br><br><b>Example:</b><br>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><br><br><b>Example:</b><br>Router (config-line)# exit                                                         | Exits line configuration mode.                                                                                                                                                                              |
| Step 9 | <b>exit</b><br><br><b>Example:</b><br>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><br/>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><br/>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><br/>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><br><br><b>Example:</b><br>Router> <code>enable</code>             | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <code>debug ip ssh</code><br><br><b>Example:</b><br>Router# <code>debug ip ssh</code> | Displays debugging messages for the SSH server.                                                                    |
| Step 3 | <code>show ssh</code><br><br><b>Example:</b><br>Router# <code>show ssh</code>         | Displays the status of the SSH server connections.                                                                 |
| Step 4 | <code>show line</code><br><br><b>Example:</b><br>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 | See the following modules: <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                                                                                                                                                                                                              |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs  | Title |
|-------|-------|
| None. | —     |

## Technical Assistance

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

# Feature Information for Reverse SSH 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://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 Reverse SSH Enhancements

| Feature Name             | Releases                                    | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reverse SSH Enhancements | 12.3(11)T<br>Cisco IOS<br>XE<br>Release 2.1 | <p>The Reverse SSH Enhancements feature, which is supported for SSH Version 1 and 2, provides an alternative way to configure reverse Secure Shell (SSH) so that separate lines do not need to be configured for every terminal or auxiliary line on which SSH must be enabled. This feature also eliminates the rotary-group limitation.</p> <p>This feature was introduced in Cisco IOS Release 12.3(11)T.</p> <p>This feature was introduced on Cisco ASR 1000 Series Routers.</p> <p>The following command was introduced: <b>ssh</b>.</p> |

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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.





# Secure Copy

---

**First Published: May 31, 2001**  
**Last Updated: October 8, 2009**

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.

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

## 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 6](#)
- [Feature Information for Secure Copy, page 8](#)
- [Glossary, page 8](#)



---

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

## 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 | <p><b>enable</b></p> <p><b>Example:</b><br/>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><br/>Router# configure terminal</p>                                                                                                                                                   | <p>Enters global configuration mode.</p>                                                                                                                                                                                                  |
| Step 3 | <p><b>aaa new-model</b></p> <p><b>Example:</b><br/>Router (config)# aaa new-model</p>                                                                                                                                                    | <p>Sets AAA authentication at login.</p>                                                                                                                                                                                                  |
| Step 4 | <p><b>aaa authentication login {default   list-name} method1 [method2...]</b></p> <p><b>Example:</b><br/>Router (config)# aaa authentication login default group tacacs+</p>                                                             | <p>Enables the AAA access control system.</p>                                                                                                                                                                                             |
| Step 5 | <p><b>aaa authorization {network   exec   commands level   reverse-access   configuration} {default   list-name} [method1 [method2...]]</b></p> <p><b>Example:</b><br/>Router (config)# aaa authorization exec default group tacacs+</p> | <p>Sets parameters that restrict user access to a network.</p> <p><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.</p> |
| Step 6 | <p><b>username name [privilege level] {password encryption-type encrypted-password}</b></p> <p><b>Example:</b><br/>Router (config)# username superuser privilege 2 password 0 superpassword</p>                                          | <p>Establishes a username-based authentication system.</p> <p><b>Note</b> You may skip this step if a network-based authentication mechanism—such as TACACS+ or RADIUS—has been configured.</p>                                           |
| Step 7 | <p><b>ip scp server enable</b></p> <p><b>Example:</b><br/>Router (config)# ip scp server enable</p>                                                                                                                                      | <p>Enables SCP server-side functionality.</p>                                                                                                                                                                                             |

## Verifying SCP

To verify SCP server-side functionality, perform the following steps.

**SUMMARY STEPS**

1. `enable`
2. `show running-config`

**DETAILED STEPS**

|               | <b>Command or Action</b>                                                                            | <b>Purpose</b>                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <code>enable</code><br><br><b>Example:</b><br>Router> <code>enable</code>                           | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| <b>Step 2</b> | <code>show running-config</code><br><br><b>Example:</b><br>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**

|               | <b>Command or Action</b>                                                              | <b>Purpose</b>                                                                                                     |
|---------------|---------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <code>enable</code><br><br><b>Example:</b><br>Router> <code>enable</code>             | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| <b>Step 2</b> | <code>debug ip scp</code><br><br><b>Example:</b><br>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 Version 1 and 2 support.        | <a href="#">“Configuring Secure Shell”</a> module.<br><a href="#">“Secure Shell Version 2 Support”</a> module.                                                 |
| Authentication and authorization commands    | <a href="#">Cisco IOS Security Command Reference</a>                                                                                                           |
| Configuring authentication and authorization | “Authentication, Authorization, and Accounting (AAA)” section of <a href="#">Cisco IOS Security Configuration Guide: Securing User Services</a> , Release 15.0 |

### Standards

| Standards | Title |
|-----------|-------|
| None.     | —     |

### MIBs

| MIBs  | MIBs Link                                                                                                                                                                                                              |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

### RFCs

| RFCs  | Title |
|-------|-------|
| None. | —     |

## Technical Assistance

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

## Feature Information for Secure Copy

Table 68 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 68 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 68** Feature Information for Secure Copy

| Feature Name | Releases                                                             | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------|----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Secure Copy  | 12.2(2)T<br>12.0(21)S<br>12.2(25)S<br>Cisco IOS<br>XE<br>Release 2.1 | <p>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.</p> <p>This feature was introduced in Cisco IOS Release 12.2(2)T.</p> <p>This feature was integrated into Cisco IOS Release 12.0(21)S.</p> <p>This feature was integrated into Cisco IOS Release 12.2(25)S.</p> <p>This feature was introduced on Cisco ASR 1000 Series Routers in Cisco IOS XE Release 2.1.</p> <p>The following commands were introduced or modified:<br/><b>debug ip scp, ip scp server enable.</b></p> |

## Glossary

**AAA**—authentication, authorization, and accounting. Framework of security services that provide the method for identifying users (authentication), for remote access control (authorization), and for collecting and sending security server information used for billing, auditing, and reporting (accounting).

**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.

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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.





# Secure Shell Version 2 Support

---

**First Published: November 3, 2003**

**Last Updated: October 8, 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 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 24.

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

## Contents

- [Prerequisites for Secure Shell Version 2 Support, page 2](#)
- [Restrictions for Secure Shell Version 2 Support, page 2](#)
- [Information About Secure Shell Version 2 Support, page 2](#)
- [How to Configure Secure Shell Version 2 Support, page 5](#)
- [Configuration Examples for Secure Shell Version 2 Support, page 17](#)
- [Where to Go Next, page 22](#)



---

**Americas Headquarters:**

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

- [Additional References, page 22](#)
- [Feature Information for Secure Shell Version 2 Support, page 24](#)

## 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 Guide](#), Release 12.4T and [Cisco IOS Network Management Configuration Guide](#), Release 15.0.

## 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:
  - 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](#)
- [Secure Shell Version 2 Enhancements, page 3](#)
- [Secure Shell Version 2 Enhancements for RSA Keys, 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.

## Secure Shell Version 2 Enhancements for RSA Keys

Cisco IOS SSH supports keyboard-interactive and password-based authentication methods. In addition to these authentication methods SSHv2 Enhancements for RSA Keys supports public key-based user authentication in Cisco IOS SSH. The RSA-based user authentication method uses private-public key

pair association. SSH users present a private key encrypted authentication signature. This authentication signature along with their public keys are sent to the SSH server for authentication. If a match is found, the RSA-based verification is completed using the public key.

To complete authentication you must generate a private-public key pair. The public key must be configured and saved on the SSH server.

**Note**

---

Storing public keys on a server uses memory; therefore, the number of public keys configurable on an SSH server is restricted to 10 users, with a maximum of two public keys per user.

---

## 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 “[Configuring SNMP Support](#)” module in the *Cisco IOS Network Management Configuration Guide*, Release 15.0.

**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](#)” section on page 18.”

---

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](#)” section on page 20.

## 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](#)” section on page 18.”

# 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)
- [Configuring a Router for SSH Version 2 Using Private Public Key Pairs, page 7](#) (optional)
- [Starting an Encrypted Session with a Remote Device, page 8](#) (optional)
- [Enabling Secure Copy Protocol on the SSH Server, page 9](#) (optional)
- [Verifying the Status of the Secure Shell Connection Using the show ssh Command, page 12](#) (optional)
- [Verifying the Secure Shell Status Using the show ip ssh Command, page 13](#) (optional)
- [Monitoring and Maintaining Secure Shell Version 2, page 14](#) (optional)

## Configuring a Router for SSH Version 2 Using a Host Name and Domain Name

Perform this task to configure your router for SSH Version 2 using a host name and domain name. 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”](#) section on page 6”).

### 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><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                       |

|        | Command or Action                                                                                                                     | Purpose                                                           |
|--------|---------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| Step 3 | <code>hostname hostname</code><br><br><b>Example:</b><br>Router(config)# hostname cisco 7200                                          | Configures a host name for your router.                           |
| Step 4 | <code>ip domain-name name</code><br><br><b>Example:</b><br>Router(config)# ip domain-name example.com                                 | Configures a domain name for your router.                         |
| Step 5 | <code>crypto key generate rsa</code><br><br><b>Example:</b><br>Router(config)# crypto key generate rsa                                | Enables the SSH server for local and remote authentication.       |
| Step 6 | <code>ip ssh [time-out seconds   authentication-retries integer]</code><br><br><b>Example:</b><br>Router(config)# ip ssh time-out 120 | (Optional) Configures SSH control variables on your router.       |
| Step 7 | <code>ip ssh version [1   2]</code><br><br><b>Example:</b><br>Router(config)# ip ssh version 1                                        | (Optional) Specifies the version of SSH to be run on your router. |

## Configuring a Router for SSH Version 2 Using RSA Key Pairs

To enable SSH Version 2 without configuring a host name or domain name, perform the following steps. SSH Version 2 will be enabled if the key pair that you configure already exists or if it is generated later. You may also configure SSH Version 2 by using the host name and domain name configuration (See the section [“Configuring a Router for SSH Version 2 Using a Host Name and Domain Name”](#) section on page 5”).

### 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 | <p><b>enable</b></p> <p><b>Example:</b><br/>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><br/>Router# configure terminal</p>                                                                                                                                     | <p>Enters global configuration mode.</p>                                                                                                                                                                                                                                                                                                |
| Step 3 | <p><b>ip ssh rsa keypair-name</b> <i>keypair-name</i></p> <p><b>Example:</b><br/>Router (config)# ip ssh rsa keypair-name sshkeys</p>                                                                                      | <p>Specifies which RSA keypair to use for SSH usage.</p> <p><b>Note</b> A Cisco IOS router can have many RSA key pairs.</p>                                                                                                                                                                                                             |
| Step 4 | <p><b>crypto key generate rsa usage-keys</b> <b>label</b> <i>key-label</i> <b>modulus</b> <i>modulus-size</i></p> <p><b>Example:</b><br/>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> |
| Step 5 | <p><b>ip ssh</b> [<b>time-out</b> <i>seconds</i>   <b>authentication-retries</b> <i>integer</i>]</p> <p><b>Example:</b><br/>Router (config)# ip ssh time-out 120</p>                                                       | <p>Configures SSH control variables on your router.</p>                                                                                                                                                                                                                                                                                 |
| Step 6 | <p><b>ip ssh version 2</b></p> <p><b>Example:</b><br/>Router (config)# ip ssh version 2</p>                                                                                                                                | <p>Specifies the version of SSH to be run on a router.</p>                                                                                                                                                                                                                                                                              |

## Configuring a Router for SSH Version 2 Using Private Public Key Pairs

Perform this task to enable SSH Version 2 public key-based user authentication. SSH Version 2 will be approve authentication if the public-key and private-key encryption messages match the keys stored on the SSH server.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ssh pubkey-chain**
4. **server** *server-name*
5. **username** *user-name*

6. **key-hash** *key-type key-name*
7. **exit**

## DETAILED STEPS

|                                                                                                                                                  |                                                                                                                                    |
|--------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b><br><br><b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                      | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                 |
| <b>Step 2</b><br><br><b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                              | Enters global configuration mode.                                                                                                  |
| <b>Step 3</b><br><br><b>ip ssh pubkey-chain</b><br><br><b>Example:</b><br>Router (config)# ip ssh pubkey-chain                                   | Enters pubkey-chain configuration mode.                                                                                            |
| <b>Step 4</b><br><br><b>server</b> <i>server-name</i><br><br><b>Example:</b><br>Router (conf-ssh-pubkey)# server cisco                           | Enables the SSH server for public key authentication on the router.                                                                |
| <b>Step 5</b><br><br><b>username</b> <i>user-name</i><br><br><b>Example:</b><br>Router (conf-ssh-pubkey)# username stabilo                       | Configures the SSH username and enters public key user mode.                                                                       |
| <b>Step 6</b><br><br><b>key-hash</b> <i>key-type key-name</i><br><br><b>Example:</b><br>Router (conf-ssh-pubkey-user)# key-hash ssh-rsa<br>lemon | Specifies the SSH key type and version.<br><br><b>Note</b> Key-type must be ssh-rsa for configuration of private public key pairs. |
| <b>Step 7</b><br><br><b>exit</b><br><br><b>Example:</b><br>Router (conf-ssh-pubkey-user)# exit                                                   | Exits public key user mode.                                                                                                        |

## Starting an Encrypted Session with a Remote Device

Perform this task to start an encrypted session with a remote networking device, (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 <i>userid</i>] [-o <i>numberofpasswordprompts n</i>] [-p <i>port-num</i>] {<i>ip-addr</i>   <i>hostname</i>} [<i>command</i>]</pre> <p><b>Example:</b><br/>Router# <code>ssh -v 2 -c aes256-cbc -m hmac-sha1-96 -l user2 10.76.82.24</code></p> <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> <p><b>Example:</b><br/>Router# <code>ssh -v 2 -c aes256-cbc -m hmac-sha1-96 user2@10.76.82.24</code></p> | <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

Perform this task to configure server-side functionality for SCP. 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> | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                             |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                 | Enters global configuration mode.                                                                                                                                                                                                                               |
| <b>Step 3</b> | <b>aaa new-model</b><br><br><b>Example:</b><br>Router(config)# aaa new-model                                                                                   | Enables the authentication, authorization, and accounting (AAA) access control model.                                                                                                                                                                           |
| <b>Step 4</b> | <b>aaa authentication login default local</b><br><br><b>Example:</b><br>Router(config)# aaa authentication login default local                                 | Sets authentication, authorization, and accounting (AAA) authentication at login to use the local username database for authentication.                                                                                                                         |
| <b>Step 5</b> | <b>aaa authorization exec default local</b><br><br><b>Example:</b><br>Router(config)# aaa authorization exec default local                                     | 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.                                           |
| <b>Step 6</b> | <b>username name privilege privilege-level password password</b><br><br><b>Example:</b><br>Router(config)# username samplename privilege 15 password password1 | Establishes a username-based authentication system, specifies the username, the privilege level, and an unencrypted password.<br><br><b>Note</b> The minimum <i>privilege-level</i> is 15. A privilege level of less than 15 results in the connection closing. |
| <b>Step 7</b> | <b>ip ssh time-out seconds</b><br><br><b>Example:</b><br>Router(config)# ip ssh time-out 120                                                                   | Sets the time interval (in seconds) that the router waits for the SSH client to respond.                                                                                                                                                                        |
| <b>Step 8</b> | <b>ip ssh authentication-retries integer</b><br><br><b>Example:</b><br>Router(config)# ip ssh authentication-retries 3                                         | Sets the number of authentication attempts after which the interface is reset.                                                                                                                                                                                  |
| <b>Step 9</b> | <b>ip scp server enable</b><br><br><b>Example:</b><br>Router (config)# ip scp server enable                                                                    | 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><br><b>enable</b><br><br><b>Example:</b><br>Router> enable     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| <b>Step 2</b><br><b>show ssh</b><br><br><b>Example:</b><br>Router# show ssh | 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

Perform this task to verify your SSH configuration.

### SUMMARY STEPS

1. **enable**
2. **show ip ssh**

### DETAILED STEPS

|                                                                                   |                                                                                                                    |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b><br><b>enable</b><br><br><b>Example:</b><br>Router> enable           | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| <b>Step 2</b><br><b>show ip ssh</b><br><br><b>Example:</b><br>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

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><br><br><b>Example:</b><br>Router> enable                       | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| <b>Step 2</b> | <b>debug ip ssh</b><br><br><b>Example:</b><br>Router# debug ip ssh           | Displays debugging messages for SSH.                                                                               |
| <b>Step 3</b> | <b>debug snmp packet</b><br><br><b>Example:</b><br>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 17](#)
- [Configuring Secure Shell Version 2: Example, page 17](#)
- [Configuring Secure Shell Versions 1 and 2: Example, page 18](#)
- [Starting an Encrypted Session with a Remote Device: Example, page 18](#)
- [Configuring Server-Side SCP: Example, page 18](#)
- [Setting an SNMP Trap: Example, page 18](#)
- [SSH Keyboard Interactive Authentication: Examples, page 18](#)
- [SNMP Debugging: Example, page 20](#)
- [SSH Debugging Enhancements: Examples, page 21](#)

### 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” section on page 20.](#)

```
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="#">Cisco IOS Security Configuration Guide: Securing User Services</a> , Release 15.0.                                                                  |
| Configuring a host name and host domain | “Configuring Secure Shell” module.                                                                                                                              |
| Configuring Secure Shell                |                                                                                                                                                                 |
| Debugging commands                      | <a href="#">Cisco IOS Debug Command Reference</a>                                                                                                               |
| Downloading a Cisco software image      | <a href="#">Cisco IOS Configuration Fundamentals Guide</a> , Release 12.4T and <a href="#">Cisco IOS Network Management Configuration Guide</a> , Release 15.0. |
| IOS configuration fundamentals          |                                                                                                                                                                 |
| IPSec                                   | <a href="#">Cisco IOS Security Configuration Guide: Secure Connectivity</a> , Release 15.0.                                                                     |
| Security commands                       | <a href="#">Cisco IOS Security Command Reference</a>                                                                                                            |
| SNMP, configuring traps                 | “Configuring SNMP Support” module in the <a href="#">Cisco IOS Network Management Configuration Guide</a> , Release 15.0.                                       |

## 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                                                                                                                                                                                                                         |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li></li> </ul> | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

| 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> |

# 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<br>12.2(25)S    | <p>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.</p> <p>In 12.3(11)T, support was added for the Cisco 10000.&gt;&gt;</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Information About Secure Shell Version 2 Support, page 2</a></li> <li>• <a href="#">How to Configure Secure Shell Version 2 Support, page 5</a></li> </ul> <p>The following commands were introduced or modified: <b>debug ip ssh</b>, <b>ip ssh min dh size</b>, <b>ip ssh rsa keypair-name</b> and <b>ip ssh version, ssh</b>.</p> |
| Secure Shell Version 2 Client and Server Support | 12.3(7)JA<br>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)                 | <p>The Cisco IOS image was updated to provide for the automatic generation of SNMP traps when an SSH session terminates.</p> <p>For information about this feature, see the following section:</p> <ul style="list-style-type: none"> <li>• <a href="#">“SNMP Trap Generation” section on page 4</a></li> <li>• <a href="#">“SNMP Debugging: Example” section on page 20</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SSH Keyboard Interactive Authentication          | 12.4(18)<br>12.2(33)SXH3 | <p>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.</p> <p>For information about this feature see the following sections:</p> <ul style="list-style-type: none"> <li>• <a href="#">“SSH Keyboard Interactive Authentication” section on page 4</a></li> <li>• <a href="#">“SSH Keyboard Interactive Authentication: Examples” section on page 18</a></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<br>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 18</a></li> </ul>                                                                       |
| Secure Shell Version 2 Enhancements for RSA Keys. | 15.0(1)M                              | <p>The Secure Shell Version 2 Enhancements for RSA Keys includes a number of additional capabilities to support RSA key based user authentication for SSH and SSH server host key storage and verification.</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 for RSA Keys, page 3</a></li> <li>• <a href="#">Configuring a Router for SSH Version 2 Using Private Public Key Pairs, page 7</a></li> </ul> <p>The following commands were introduced or modified: <b>ip ssh pubkey-chain</b> and <b>ip ssh stricthostkeycheck</b>.</p> |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLynx, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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

---

**First Published: October 2, 2002**  
**Last Updated: November 5, 2009**

The SSH Terminal-Line Access feature provides users secure access to tty (text telephone) lines. tty allows the hearing- and speech-impaired to communicate by using a telephone to type messages.

## 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 SSH Terminal-Line Access”](#) 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 SSH Terminal-Line Access, page 2](#)
- [Restrictions for SSH Terminal-Line Access, page 2](#)
- [Information About SSH Terminal-Line Access, page 2](#)
- [How to Configure SSH Terminal-Line Access, page 3](#)
- [Configuration Examples for SSH Terminal-Line Access, page 5](#)
- [Additional References, page 7](#)
- [Feature Information for SSH Terminal-Line Access, page 9](#)



---

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

## Prerequisites for SSH Terminal-Line Access

Download the required image to your router. The secure shell (SSH) server requires the router to have an IPsec (Data Encryption Standard (DES) or 3DES) encryption software image from Cisco IOS Release 12.1(1)T or a later release. The SSH client requires the router to have an IPsec (DES or 3DES) encryption software image from Cisco IOS Release 12.1(3)T or a later release. See the [Cisco IOS Configuration Fundamentals Configuration Guide](#), Release 12.4T for more information on downloading a software image.

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.

---

## Restrictions for SSH Terminal-Line Access

### 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 user want 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.)

## Information About SSH Terminal-Line Access

To configure the SSH Terminal-Line Access feature, you should understand the following concept:

- [Overview of SSH Terminal-Line Access, page 2](#)

## Overview of SSH Terminal-Line Access

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 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 provides 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. Currently two versions of SSH are 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.
- 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 of each of the lines through a locally defined username and password, TACACS+, or RADIUS.

**Note**

The **session slot** command that is used to start a session with a module requires Telnet to be accepted on the virtual tty (vty) lines. When you restrict vty lines only to SSH, you cannot use the command to communicate with the modules. This applies to any Cisco IOS device where the user can telnet to a module on the device.

## How to Configure SSH Terminal-Line Access

This section contains the following task:

- [Configuring SSH Terminal-Line Access, page 3](#)

## Configuring SSH Terminal-Line Access

Perform this task to configure a Cisco router to support reverse secure Telnet:

**Note**

SSH must already be configured on the router.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line** *line-number* [*ending-line-number*]
4. **no exec**
5. **login** {**local** | **authentication** *listname*}
6. **rotary** *group*
7. **transport input** {**all** | **ssh**}
8. **exit**
9. **ip ssh port** *portnum* **rotary** *group*

## DETAILED STEPS

|        | Command or Action                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <p><b>enable</b></p> <p><b>Example:</b><br/>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><br/>Router# configure terminal</p>                                                                  | <p>Enters global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 3 | <p><b>line</b> <i>line-number</i> [<i>ending-line-number</i>]</p> <p><b>Example:</b><br/>Router(config)# line 1 200</p>                                 | <p>Identifies a line for configuration and enters line configuration mode.</p> <p><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.</p> <p><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.</p> |
| Step 4 | <p><b>no exec</b></p> <p><b>Example:</b><br/>Router(config-line)# no exec</p>                                                                           | <p>Disables exec processing on each of the lines.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 5 | <p><b>login</b> {<b>local</b>   <b>authentication</b> <i>listname</i>}</p> <p><b>Example:</b><br/>Router(config-line)# login authentication default</p> | <p>Defines a login authentication mechanism for the lines.</p> <p><b>Note</b> The authentication method must utilize a username and password.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 6 | <p><b>rotary</b> <i>group</i></p> <p><b>Example:</b><br/>Router(config-line)# rotary 1</p>                                                              | <p>Defines a group of lines consisting of one or more lines.</p> <p><b>Note</b> All rotaries used must be defined, and each defined rotary must be used when SSH is enabled.</p>                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 7 | <p><b>transport input</b> {<b>all</b>   <b>ssh</b>}</p> <p><b>Example:</b><br/>Router(config-line)# transport input ssh</p>                             | <p>Defines which protocols to use to connect to a specific line of the router.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

|        | Command or Action                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 8 | <code>exit</code><br><br><b>Example:</b><br>Router(config-line)# <code>exit</code>                                             | Exits line configuration mode.                                                                                                                                                                                                                                                                                                                                         |
| Step 9 | <code>ip ssh port portnum rotary group</code><br><br><b>Example:</b><br>Router(config)# <code>ip ssh port 2000 rotary 1</code> | Enables secure network access to the tty lines. <ul style="list-style-type: none"> <li>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.</li> </ul> <p><b>Note</b> The <i>group</i> argument must correspond with the <i>rotary group</i> number chosen in Step 6.</p> |

## Verifying SSH Terminal-Line Access

To verify that this functionality is working, you can connect to a router using an SSH client.

## Configuration Examples for SSH Terminal-Line Access

This section provides the following configuration examples:

- [SSH Terminal-Line Access Configuration: Example, page 5](#)
- [SSH Terminal-Line Access for a Console \(Serial Line\) Ports Configuration: Example, page 6](#)

### 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 an 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 1](#).

**Table 1** 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
```

# Additional References

The following sections provide references related to the SSH Terminal-Line Access feature.

## Related Documents

| Related Topic                | Document Title                                                        |
|------------------------------|-----------------------------------------------------------------------|
| SSH                          | <i>Cisco IOS Security Configuration Guide: Securing User Services</i> |
| SSH commands                 | <a href="#">Cisco IOS Security Command Reference</a>                  |
| Dial Technologies            | <i>Cisco IOS Dial Technologies Configuration Guide</i>                |
| Dial commands                | <a href="#">Cisco IOS Dial Technologies Command Reference</a>         |
| Downloading a software image | <i>Cisco IOS Configuration Fundamentals Configuration Guide</i>       |

## Standards

| Standard | Title |
|----------|-------|
|          | —     |

## MIBs

| MIB | MIBs Link                                                                                                                                                                                                              |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><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 SSH Terminal-Line Access

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 SSH Terminal-Line Access

| Feature Name             | Releases                             | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSH Terminal-Line Access | 12.2(4)JA<br>12.2(15)T<br>12.2(6th)S | <p>The SSH Terminal-Line Access feature provides users secure access to tty (text telephone) lines. tty allows the hearing- and speech-impaired to communicate by using a telephone to type messages.</p> <p>This feature was introduced in Cisco IOS Release 12.2(4)JA.</p> <p>This feature was integrated into Cisco IOS Release 12.2(15)T.</p> <p>This feature was integrated into Cisco IOS Release 12.2(6th)S.</p> <p>The following command was introduced or modified: <b>ip ssh port</b>.</p> |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, 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 Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, 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. (0910R)

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.





# Cisco IOS Login Enhancements (Login Block)

---

**First Published: August 2005**

**Last Updated: August 26, 2009**

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.

## 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 Login Enhancements \(Login Block\)” 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

- [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 7](#)
- [Feature Information for Cisco IOS Login Enhancements \(Login Block\), page 9](#)



---

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

# 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 2](#)

## 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 network 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 are not 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:

- Through the **auto secure** command. If you enable the AutoSecure feature, the default login delay time of one second is automatically enforced.
- Through 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.
- Through 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 does 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 through the new global configuration mode command **login block-for**. The predefined ACL that is excluded from the quiet period can be specified through 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 through 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 through autosecure.



### Note

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

## What to Do Next

After you have configured login parameters on your router, you may wish to verify the settings. To complete this task, see the following section [“Verifying Login Parameters” section on page 5.](#)”

## 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><br><br><b>Example:</b><br>Router> enable                    | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                         |
| Step 2 | <b>show login [failures]</b><br><br><b>Example:</b><br>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 are denied during the quiet period except hosts from the ACL "myacl." Also, logging messages are 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                              | “ <a href="#">AutoSecure</a> ” feature module.            |
| Secure Management/Administrative Access | “ <a href="#">Role-Based CLI Access</a> ” feature module. |

## Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

## MIBs

| MIBs | MIBs Link                                                                                                                                                                                                                  |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs | Title |
|------|-------|
| None | —     |

## Technical Assistance

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

# Feature Information for Cisco IOS Login Enhancements (Login Block)

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 Login Enhancements (Login Block)

| Feature Name                               | Releases                                                                                                           | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco IOS Login Enhancements (Login Block) | 12.3(4)T<br>12.2(25)S<br>12.2(33)SRA<br>12.2(33)SRB<br>12.2(33)SXH<br>12.4(15)T1<br>Cisco IOS<br>XE<br>Release 2.1 | <p>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 DoS attack is detected.</p> <p>This feature was introduced in Cisco IOS Release 12.3(4)T.</p> <p>This feature was integrated into Cisco IOS Release 12.2(25)S.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRA.</p> <p>Support for HTTP login blocking was integrated into Cisco IOS Release 12.2(33)SRB, 12.2(33)SXH, 12.4(15)T1.</p> <p>This feature was introduced in Cisco IOS XE Release 2.1</p> <p>The following commands were introduced or modified:<br/><b>login block-for</b>, <b>login delay</b>, <b>login on-failure</b>, <b>login on-success</b>, <b>login quiet-mode access-class</b>, <b>show login</b>.</p> |

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card 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. (0907R)

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.



# Cisco IOS Resilient Configuration

---

**First Published: May 17, 2004**

**Last Updated: October 19, 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 | <code>enable</code><br><br><b>Example:</b><br>Router> <code>enable</code>                                 | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br>Router# <code>configure terminal</code>         | Enters global configuration mode.                                       |
| Step 3 | <code>secure boot-image</code><br><br><b>Example:</b><br>Router(config)# <code>secure boot-image</code>   | Enables Cisco IOS image resilience.                                     |
| Step 4 | <code>secure boot-config</code><br><br><b>Example:</b><br>Router(config)# <code>secure boot-config</code> | 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><br><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><br><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><br><br><b>Example:</b><br>Router# reload                                                                                            | (Optional) Enters ROM monitor mode, if necessary.                                                                                                                                                                                                               |
| Step 2 | <b>dir</b> [ <i>filesystem:</i> ]<br><br><b>Example:</b><br>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> ]<br><br><b>Example:</b><br>rommon 2 > boot slot0:c3745-js2-mz                          | Boots up the router using the secure bootset image.                                                                                                                                                                                                             |
| Step 4 | <b>no</b><br><br><b>Example:</b><br>--- System Configuration Dialog ---<br>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><br><br><b>Example:</b><br>Router> enable                                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                |
| Step 6 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                    | Enters global configuration mode.                                                                                                                                                                                                                               |
| Step 7 | <b>secure boot-config</b> [restore <i>filename</i> ]<br><br><b>Example:</b><br>Router(config)# secure boot-config restore slot0:rescue-cfg        | Restores the secure configuration to the supplied filename.                                                                                                                                                                                                     |

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

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

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

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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: September 14, 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 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 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](#)
- [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><br><br><b>Example:</b><br>Router> enable                             | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>           |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal     | Enters global configuration mode.                                                                                            |
| Step 3 | <b>file verify auto</b><br><br><b>Example:</b><br>Router(config)# file verify auto | Enables automatic image verification.                                                                                        |
| Step 4 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                         | Exits global configuration mode.<br><br>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><br><br><b>Example:</b><br>Router> enable                                                                                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 2 | <b>copy</b> [/erase] [/verify   /noverify] <i>source-url destination-url</i><br><br><b>Example:</b><br>Router# copy /verify<br>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><br><br><b>Example:</b><br>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><br/>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><br/>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 | <a href="#">“Using the Cisco IOS Integrated File System”</a> feature module in the <i>Cisco IOS Configuration Fundamentals and Network Management Configuration Guide</i> , Release 12.4T. |
| Additional commands for loading, maintaining, and rebooting system images                 | <i>Cisco IOS Configuration Fundamentals Command Reference</i> , Release 12.4T                                                                                                              |

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

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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

---

**First Published: January 25, 2002**

**Last Updated: August 14, 2009**

The IP Source Tracker feature tracks information in the following ways:

- Gathers information about the traffic that is flowing to a host that is suspected of being under attack.
- Generates all the necessary information in an easy-to-use format to track the network entry point of a DoS attack.
- Tracks Multiple IPs at the same time.
- Tracks DoS attacks across the entire network.

## 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 IP Source Tracker” 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.

## 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](#)
- [Feature Information for IP Source Tracker, page 10](#)



---

**Americas Headquarters:**

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

# 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](#)

## Identifying and Tracking Denial of Service Attacks

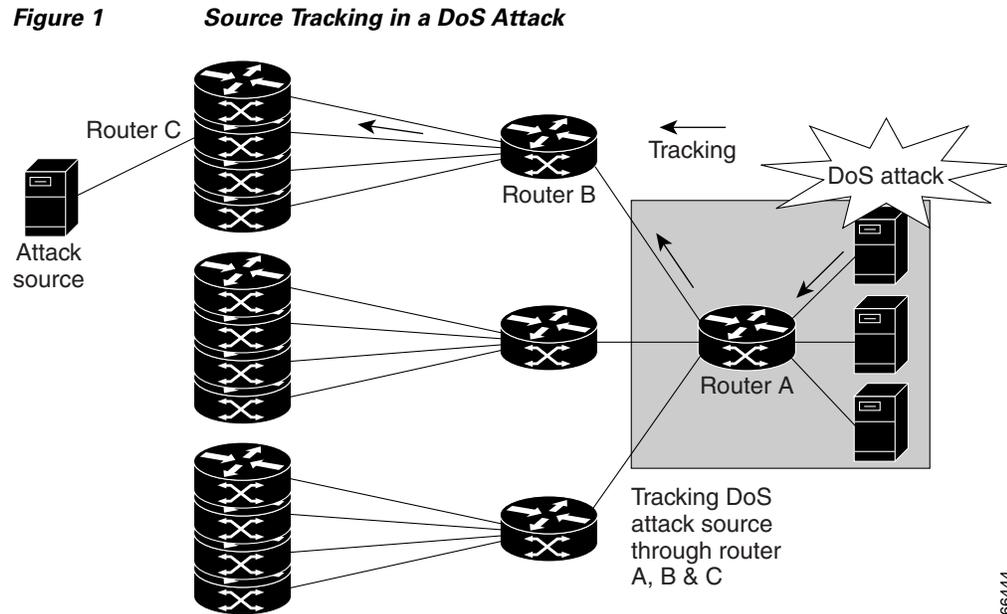
One of the many challenges faced by customers today is the tracking and blocking denial-of-service (DoS) attacks. Counteracting a DoS attack involves intrusion detection, source tracking, and blocking. This functionality addresses the need for source tracking.

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 1](#), 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.



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.

# 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><br><br><b>Example:</b><br>Router> enable                                                                        | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                           |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                | Enters global configuration mode.                                                                                                                                                                            |
| Step 3 | <b>ip source-track <i>ip-address</i></b><br><br><b>Example:</b><br>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 <i>number</i></b><br><br><b>Example:</b><br>Router(config)# ip source-track address-limit 10 | (Optional) Limits the number of hosts that can be simultaneously tracked at any given time.<br><br><b>Note</b> If this command is not enabled, there is no limit to the number of hosts that be can tracked. |

|        | Command or Action                                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <pre>ip source-track syslog-interval number</pre> <p><b>Example:</b><br/>Router(config)# ip source-track syslog-interval 2</p>  | <p>(Optional) Sets the time interval, in minutes, used to generate syslog messages that indicate IP source tracking is enabled.</p> <p><b>Note</b> If this command is not enabled, system log messages are not generated.</p>                                                                                                                                 |
| Step 6 | <pre>ip source-track export-interval number</pre> <p><b>Example:</b><br/>Router(config)# ip source-track export-interval 30</p> | <p>(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).</p> <p><b>Note</b> If this command is not enabled, traffic flow information is exported to the GRP and RSP every 30 seconds.</p> |

## 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 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                             | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                          |
| Step 2 | <b>show ip source-track</b> [ <i>ip-address</i> ] [ <b>summary</b>   <b>cache</b> ]<br><br><b>Example:</b><br>Router# show ip source-track summary | Displays traffic flow statistics for tracked IP host addresses                                                                                                                                            |
| Step 3 | <b>show ip source-track export flows</b><br><br><b>Example:</b><br>Router# show ip source-track export flows                                       | Displays the last 10 packet flows that were exported from the line card to the route processor.<br><br><b>Note</b> This command can be issued only on distributed platforms, such as the GRP and the RSP. |

## Examples

The following example, which is sample output from the **show ip source-track summary** command, shows how to verify that IP source tracking is enabled for one or more hosts:

```
Router# show ip source-track summary

Address Bytes Pkts Bytes/s Pkts/s
10.0.0.1 119G 1194M 443535 4432
192.168.1.1 119G 1194M 443535 4432
192.168.42.42 119G 1194M 443535 4432
```

The following example, which is sample output from the **show ip source-track summary** command, shows how to verify that no traffic has yet to be received for the destination hosts that are being tracked:

```
Router# show ip source-track summary

Address Bytes Pkts Bytes/s Pkts/s
10.0.0.1 0 0 0 0
192.168.1.1 0 0 0 0
192.168.42.42 0 0 0 0
```

The following example, which is sample output from the **show ip source-track** command, shows how to verify that IP source tracking is processing packets to the hosts and exporting statistics from the line card or port adapter to the GRP and RSP:

```
Router# show ip source-track

Address SrcIF Bytes Pkts Bytes/s Pkts/s
10.0.0.1 PO0/0 119G 1194M 513009 5127
192.168.1.1 PO0/0 119G 1194M 513009 5127
192.168.42.42 PO0/0 119G 1194M 513009 5127
```

# Configuration Examples for IP Source Tracker

This section includes the following examples:

- [Configuring IP Source Tracking: Example, page 7](#)
- [Verifying Source Interface Statistics for All Tracked IP Addresses: Example, page 7](#)
- [Verifying a Flow Statistic Summary for All Tracked IP Addresses: Example, page 7](#)
- [Verifying Detailed Flow Statistics Collected by a Line Card: Example, page 7](#)
- [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

IP Flow Switching Cache, 278544 bytes
 1 active, 4095 inactive, 13291 added
 198735 aged polls, 0 flow alloc failures
 Active flows timeout in 0 minutes
 Inactive flows timeout in 15 seconds
 last clearing of statistics never

Protocol Total Flows Packets Bytes Packets Active(Sec) Idle(Sec)
----- -
 Flows /Sec /Flow /Pkt /Sec /Flow /Flow

SrcIf SrcIPAddress DstIf DstIPAddress Pr TOS Flgs Pkts
Port Msk AS Port Msk AS NextHop B/Pk Active
PO0/0 101.1.1.0 Null 100.1.1.1 06 00 00 55K
0000 /0 0 0000 /0 0 0.0.0.0 100 10.1

```

## Verifying Flow Statistics Exported from Line Cards and Port Adapters: Example

The following example displays packet flow information that is exported from line cards and port adapters to the GRP and the RSP:

```

Router# show ip source-track export flows

SrcIf SrcIPAddress DstIf DstIPAddress Pr SrcP DstP Pkts
PO0/0 101.1.1.0 Null 100.1.1.1 06 0000 0000 88K
PO0/0 101.1.1.0 Null 100.1.1.3 06 0000 0000 88K
PO0/0 101.1.1.0 Null 100.1.1.2 06 0000 0000 88K

```

## Additional References

The following sections provide references related to IP Source Tracker.

## Related Documents

| Related Topic  | Document Title                                                                        |
|----------------|---------------------------------------------------------------------------------------|
| ACLs           | <i>Cisco IOS Security Configuration Guide: Securing the Data Plane, Release 12.4T</i> |
| Dynamic ACLs   | “Configuring Lock-and-Key Security (Dynamic Access Lists)”                            |
| DoS prevention | “Configuring TCP Intercept (Preventing Denial-of-Service Attacks)”                    |

## Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

## MIBs

| MIBs | MIBs Link                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs | Title |
|------|-------|
| None | —     |

## Technical Assistance

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

# Feature Information for IP Source Tracker

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 IP Source Tracker

| Feature Name      | Releases                                                     | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP Source Tracker | 12.0(21)S<br>12.0(22)S<br>12.0(26)S<br>12.3(7)T<br>12.2(25)S | <p>The IP Source Tracker feature allows information to be gathered about the traffic that is flowing to a host that is suspected of being under attack.</p> <p>This feature was introduced in Release 12.0(21)S on the Cisco 12000 series.</p> <p>This feature was implemented in Release 12.0(22)S on the Cisco 7500 series.</p> <p>This feature was implemented in Release 12.0(26)S on the Cisco 12000 series IP Service Engine (ISE) line cards.</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(25)S.</p> <p>The following commands were introduced or modified: <b>ip source-track</b>, <b>ip source-track address-limit</b>, <b>ip source-track export-interval</b>, <b>ip source-track syslog-interval</b>, <b>show ip source-track</b>, <b>show ip source-track export flows</b>.</p> |

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card 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. (0907R)

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.





## Role-Based CLI Access

---

**First Published: February 24, 2004**

**Last Updated: October 8, 2009**

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 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 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
- [Feature Information for Role-Based CLI Access](#), page 14



---

**Americas Headquarters:**

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

# 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><br/>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><br/>Router# configure terminal</p>                                                                                                                   | <p>Enters global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 3 | <p><code>parser view view-name</code></p> <p><b>Example:</b><br/>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><br/>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><br/>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><br/>Router(config-view)# exit</p>                                                                                                                                  | <p>Exits view configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

|        | Command or Action                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                    | Exits global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 8 | <b>enable</b> [ <i>privilege-level</i> ] [ <b>view</b> <i>view-name</i> ]<br><br><b>Example:</b><br>Router# enable view first | Prompts the user for a password, which allows the user to access a configured CLI view, and is used to switch from one view to another view.<br><br>After the correct password is given, the user can access the view.                                                                                                                                                                                                                                                                                                    |
| Step 9 | <b>show parser view</b> [ <b>all</b> ]<br><br><b>Example:</b><br>Router# show parser view                                     | (Optional) Displays information about the view that the user is currently in.<br><br><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><br><br><b>Example:</b><br>Router> enable view                                                                                                                                                                                                          | Enables root view.<br><br><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><br><br><b>Example:</b><br>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><br><br><b>Example:</b><br>Router(config)# li-view lipass user li_admin password li_adminpass                                                                                | Initializes a lawful intercept view.<br><br>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><br><br><b>Example:</b><br>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><br><br><b>Example:</b><br>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><br><br><b>Example:</b><br>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><br><br><b>Example:</b><br>Router(config-view)# name second                   | (Optional) Changes the name of a lawful intercept view.<br><br>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><br><br><b>Example:</b><br>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><br><br><b>Example:</b><br>Router# configure terminal                                                     | Enters global configuration mode.                                                                                                                           |
| <b>Step 3</b> | <b>parser view</b> <i>superview-name</i> <b>superview</b><br><br><b>Example:</b><br>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><br><br><b>Example:</b><br>Router(config-view)# secret 5 secret                           | Associates a CLI view or superview with a password.<br><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><br><br><b>Example:</b><br>Router(config-view)# view view_three                                        | Adds a normal CLI view to a superview.<br>Issue this command for each CLI view that is to be added to a given superview.                                    |
| <b>Step 6</b> | <b>exit</b><br><br><b>Example:</b><br>Router(config-view)# exit                                                                    | Exits view configuration mode.                                                                                                                              |

|        | Command or Action                                                                | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                       | Exits global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 8 | <b>show parser view [all]</b><br><br><b>Example:</b><br>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> <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> |

## 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 1Mcmh$QuZaU8PIMP1ff9sFCZvgW/
commands exec include configure terminal
commands exec include configure
commands exec include all show ip
commands exec include show version
commands exec include show
!
parser view second
secret 5 1iP2M$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 the Role-Based CLI Access feature.

### Related Documents

| Related Topic                 | Document Title                                                                                                                                |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| SNMP, MIBs, CLI configuration | <a href="#">Cisco IOS Network Management Configuration Guide</a> , Release 15.0.                                                              |
| Privilege levels              | “ <a href="#">Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices</a> ” module. |

### Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

### MIBs

| MIBs | MIBs Link                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs | Title |
|------|-------|
| None | —     |

## Technical Assistance

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

# 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 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 Role-Based CLI Access

| Feature Name          | Releases                                                                                      | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------|-----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Role-Based CLI Access | 12.3(7)T<br>12.3(11)T<br>12.2(33)SRB<br>12.2(33)SB<br>Cisco IOS XE Release 2.1<br>12.2(33)SXI | <p>This feature enables network administrators to restrict user access to CLI and configuration information.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers</p> <p>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.</p> <ul style="list-style-type: none"> <li>The following commands were introduced or modified: <b>commands (view), enable, li-view, name (view), parser view, parser view superview, secret, show parser view, show users, username, view.</b></li> </ul> |

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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

