Cisco IOS Mobile Wireless Home Agent Command Reference

July 2008

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

Cisco IOS Mobile Wireless Home Agent Command Reference

About Cisco IOS and Cisco IOS XE Software Documentation

Last updated: August 6, 2008

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

Documentation Objectives

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

Audience

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

Documentation Conventions

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

This section includes the following topics:

Typographic Conventions

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.)
string	A string is a nonquoted set of characters shown in italics. For example, when setting a Simple Network Management Protocol (SNMP) community string to *public*, 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.
italic	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional keyword or argument.
|	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a pipe indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a pipe indicate a required choice.
[x {y | z}]	Braces and a pipe within square brackets indicate a required choice within an optional element.

Software Conventions

Cisco IOS uses the following program code conventions:

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

Reader Alert Conventions

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

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

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

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

Documentation Organization

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

Cisco IOS Documentation Set

Cisco IOS documentation consists of the following:

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

Cisco IOS Documentation on Cisco.com

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

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

New Features List

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

Feature Guides

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

Configuration Guides

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

Command References

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

Cisco IOS Supplementary Documents and Resources

Supplementary documents and resources are listed in Table 2 on page xi.

Configuration Guides, Command References, and Supplementary Resources

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

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

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

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

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

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS Bridging and IBM Networking Configuration Guide *Cisco IOS Bridging Command Reference* *Cisco IOS IBM Networking Command Reference*	• Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRSM). • Data-link switching plus (DLSw+), serial tunnel (STUN), block serial tunnel (BSTUN); logical link control, type 2 (LLC2), synchronous data link control (SDLC); IBM Network Media Translation, including Synchronous Data Logical Link Control (SDLLC) and qualified LLC (QLLC); downstream physical unit (DSPU), Systems Network Architecture (SNA) service point, SNA frame relay access, advanced peer-to-peer networking (APPN), native client interface architecture (NCIA) client/server topologies, and IBM Channel Attach.
Cisco IOS Broadband and DSL Configuration Guide *Cisco IOS XE Broadband and DSL Configuration Guide* *Cisco IOS Broadband and DSL Command Reference*	Point-to-Point Protocol (PPP) over ATM (PPPoA) and PPP over Ethernet (PPPoE).
Cisco IOS Carrier Ethernet Configuration Guide *Cisco IOS Carrier Ethernet Command Reference*	Connectivity fault management (CFM), Ethernet Local Management Interface (ELMI), IEEE 802.3ad link bundling, Link Layer Discovery Protocol (LLDP), media endpoint discovery (MED), and operations, administration, and maintenance (OAM).
Cisco IOS Configuration Fundamentals Configuration Guide *Cisco IOS XE Configuration Fundamentals Configuration Guide* *Cisco IOS Configuration Fundamentals Command Reference*	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.
Cisco IOS DECnet Configuration Guide *Cisco IOS XE DECnet Configuration Guide* *Cisco IOS DECnet Command Reference*	DECnet protocol.
Cisco IOS Dial Technologies Configuration Guide *Cisco IOS XE Dial Technologies Configuration Guide* *Cisco IOS Dial Technologies Command Reference*	Asynchronous communications, dial backup, dialer technology, dial-in terminal services and AppleTalk remote access (ARA), large scale dialout, dial-on-demand routing, dialout, modem and resource pooling, ISDN, multilink PPP (MLP), PPP, virtual private dialup network (VPDN).
Cisco IOS Flexible NetFlow Configuration Guide *Cisco IOS Flexible NetFlow Command Reference*	Flexible NetFlow.

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS H.323 Configuration Guide	Gatekeeper enhancements for managed voice services, Gatekeeper Transaction Message Protocol, gateway codec order preservation and shutdown control, H.323 dual tone multifrequency relay, H.323 version 2 enhancements, Network Address Translation (NAT) support of H.323 v2 Registration, Admission, and Status (RAS) protocol, tokenless call authorization, and VoIP gateway trunk and carrier-based routing.
Cisco IOS High Availability Configuration Guide *Cisco IOS XE High Availability Configuration Guide* *Cisco IOS High Availability Command Reference*	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.
Cisco IOS Integrated Session Border Controller Command Reference	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).
Cisco IOS Intelligent Service Gateway Configuration Guide *Cisco IOS Intelligent Service Gateway Command Reference*	Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, session state monitoring.
Cisco IOS Interface and Hardware Component Configuration Guide *Cisco IOS XE Interface and Hardware Component Configuration Guide* *Cisco IOS Interface and Hardware Component Command Reference*	LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration.
Cisco IOS IP Addressing Services Configuration Guide *Cisco IOS XE Addressing Services Configuration Guide* *Cisco IOS IP Addressing Services Command Reference*	Address Resolution Protocol (ARP), Network Address Translation (NAT), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Next Hop Address Resolution Protocol (NHRP).
Cisco IOS IP Application Services Configuration Guide *Cisco IOS XE IP Application Services Configuration Guide* *Cisco IOS IP Application Services Command Reference*	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).
Cisco IOS IP Mobility Configuration Guide *Cisco IOS IP Mobility Command Reference*	Mobile ad hoc networks (MANet) and Cisco mobile networks.
Cisco IOS IP Multicast Configuration Guide *Cisco IOS XE IP Multicast Configuration Guide* *Cisco IOS IP Multicast Command Reference*	Protocol Independent Multicast (PIM) sparse mode (PIM-SM), bidirectional PIM (bidir-PIM), Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), Internet Group Management Protocol (IGMP), and Multicast VPN (MVPN).

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS IP Routing Protocols Configuration Guide *Cisco IOS XE IP Routing Protocols Configuration Guide* *Cisco IOS IP Routing Protocols Command Reference*	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).
Cisco IOS IP SLAs Configuration Guide *Cisco IOS XE IP SLAs Configuration Guide* *Cisco IOS IP SLAs Command Reference*	Cisco IOS IP Service Level Agreements (IP SLAs).
Cisco IOS IP Switching Configuration Guide *Cisco IOS XE IP Switching Configuration Guide* *Cisco IOS IP Switching Command Reference*	Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS).
Cisco IOS IPv6 Configuration Guide *Cisco IOS XE IPv6 Configuration Guide* *Cisco IOS IPv6 Command Reference*	For IPv6 features, protocols, and technologies, go to the IPv6 "Start Here" document at the following URL: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html
Cisco IOS ISO CLNS Configuration Guide *Cisco IOS XE ISO CLNS Configuration Guide* *Cisco IOS ISO CLNS Command Reference*	ISO connectionless network service (CLNS).
Cisco IOS LAN Switching Configuration Guide *Cisco IOS XE LAN Switching Configuration Guide* *Cisco IOS LAN Switching Command Reference*	VLANs, Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, IEEE 802.1Q encapsulation, and multilayer switching (MLS).
Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide *Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference*	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.
Cisco IOS Mobile Wireless Home Agent Configuration Guide *Cisco IOS Mobile Wireless Home Agent Command Reference*	Cisco Mobile Wireless Home Agent, an anchor point for mobile terminals for which mobile IP or proxy mobile IP services are provided.
Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide *Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference*	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.
Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide *Cisco IOS Mobile Wireless Radio Access Networking Command Reference*	Cisco IOS radio access network products.

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

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

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS Service Selection Gateway Configuration Guide *Cisco IOS Service Selection Gateway Command Reference*	Subscriber authentication, service access, and accounting.
Cisco IOS Software Activation Configuration Guide *Cisco IOS Software Activation Command Reference*	An orchestrated collection of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.
Cisco IOS Software Modularity Installation and Configuration Guide *Cisco IOS Software Modularity Command Reference*	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.
Cisco IOS Terminal Services Configuration Guide *Cisco IOS Terminal Services Command Reference* *Cisco IOS XE Terminal Services Command Reference*	DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD).
Cisco IOS Virtual Switch Command Reference	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, refer to the product-specific software configuration information for the Cisco Catalyst 6500 series switch or for the Metro Ethernet 6500 series switch.
Cisco IOS Voice Configuration Library *Cisco IOS Voice Command Reference*	Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. The library includes documentation for IP telephony applications.
Cisco IOS VPDN Configuration Guide *Cisco IOS XE VPDN Configuration Guide* *Cisco IOS VPDN Command Reference*	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.
Cisco IOS Wide-Area Networking Configuration Guide *Cisco IOS XE Wide-Area Networking Configuration Guide* *Cisco IOS Wide-Area Networking Command Reference*	Frame Relay, Layer 2 Tunneling Protocol Version 3 (L2TPv3), Link Access Procedure, Balanced (LAPB), Switched Multimegabit Data Service (SMDS), and X.25.
Cisco IOS Wireless LAN Configuration Guide *Cisco IOS Wireless LAN Command Reference*	Broadcast key rotation, IEEE 802.11x support, IEEE 802.1x authenticator, IEEE 802.1x local authentication service for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Multiple Basic Service Set ID (BSSID), Wi-Fi Multimedia (WMM) required elements, and Wi-Fi Protected Access (WPA).

Table 2 Cisco IOS Supplementary Documents and Resources

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

Additional Resources and Documentation Feedback

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

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

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

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

Last updated: August 6, 2008

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

For more information about using the CLI, see the "Using the Cisco IOS Command-Line Interface" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information about the software documentation set, see the "About Cisco IOS and Cisco IOS XE Software Documentation" document.

Initially Configuring a Device

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

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

Changing the Default Settings for a Console or AUX Port

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

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

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

Using the CLI

This section describes the following topics:

Understanding Command Modes

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.	• 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.	• 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.	• Run as the default operating mode when a valid image cannot be loaded. • Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted. • Perform password recovery when a CTRL-Break sequence is issued within 60 seconds of a power-on or reload event.
Diagnostic (available only on the Cisco ASR1000 series router)	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. • 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)#`	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. If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or using a method that is configured to connect to the Cisco IOS CLI. 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.	• Inspect various states on the router, including the Cisco IOS state. • Replace or roll back the configuration. • Provide methods of restarting the Cisco IOS software or other processes. • Reboot hardware, such as the entire router, an RP, an ESP, a SIP, a SPA, or possibly other hardware components. • Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.

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

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

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

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

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

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

Using the Interactive Help Feature

The CLI includes an interactive Help feature. Table 2 describes how to use the Help feature.

Table 2 CLI Interactive Help Commands

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

The following examples show how to use the help commands:

help

```
Router> help

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

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?')
and describes each possible argument.

2. Partial help is provided when an abbreviated argument is entered and you want to know
what arguments match the input (e.g. 'show pr?'.)
```

?

```
Router# ?
Exec commands:
  access-enable        Create a temporary access-List entry
  access-profile       Apply user-profile to interface
  access-template      Create a temporary access-List entry
  alps                 ALPS exec commands
  archive              manage archive files
<snip>
```

***partial command*?**

```
Router(config)# zo?
zone  zone-pair
```

***partial command*<Tab>**

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

***command* ?**

```
Router(config-if)# pppoe ?
  enable        Enable pppoe
  max-sessions  Maximum PPPOE sessions
```

***command keyword* ?**

```
Router(config-if)# pppoe enable ?
  group  attach a BBA group
  <cr>
```

Understanding Command Syntax

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

Specific conventions convey information about syntax and command elements. Table 3 describes these conventions.

Table 3 CLI Syntax Conventions

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

The following examples show syntax conventions:

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

Understanding Enable and Enable Secret Passwords

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

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

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

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

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

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

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

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

Using the Command History Feature

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

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

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

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

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

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

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

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

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

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

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

Abbreviating Commands

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

Using Aliases for CLI Commands

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

Table 4 shows the default command aliases.

Table 4 Default Command Aliases

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

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

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

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

For more information about the **alias** command, see http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html.

Using the no and default Forms of Commands

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

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

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

Using the debug Command

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

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

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

Filtering Output Using Output Modifiers

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

Three output modifiers are available and are described as follows:

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

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

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

```
Router# show interface | include protocol

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

Understanding CLI Error Messages

You may encounter some error messages while using the CLI. Table 5 shows the common CLI error messages.

Table 5 Common CLI Error Messages

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

For more system error messages, see the following documents:

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

Saving Changes to a Configuration

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

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

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

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

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

Additional Information

- "Using the Cisco IOS Command-Line Interface" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*:

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html

  or

  "Using Cisco IOS XE Software" chapter of the *Cisco ASR1000 Series Aggregation Services Routers Software Configuration Guide*:

  http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/using_cli.html
- Cisco Product Support Resources

  http://www.cisco.com/web/psa/products/index.html
- Support area on Cisco.com (also search for documentation by task or product)

  http://www.cisco.com/en/US/support/index.html
- *White Paper: Cisco IOS Reference Guide*

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a008018305e.shtml
- Software Download Center (downloads; tools; licensing, registration, advisory, and general information) (requires Cisco.com User ID and password)

  http://www.cisco.com/kobayashi/sw-center/
- Error Message Decoder, a tool to help you research and resolve error messages for Cisco IOS software

  http://www.cisco.com/pcgi-bin/Support/Errordecoder/index.cgi

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

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

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

  https://www.cisco.com/pcgi-bin/Support/OutputInterpreter/home.pl\

Home Agent Commands

aaa accounting

To enable authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, use the **aaa accounting** command in global configuration mode. To disable AAA accounting, use the **no** form of this command.

aaa accounting {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level* | **dot1x**} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *group-name*

no aaa accounting {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level* | **dot1x**} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *group-name*

Syntax Description

auth-proxy	Provides information about all authenticated-proxy user events.
system	Performs accounting for all system-level events not associated with users, such as reloads. **Note** When system accounting is used and the accounting server is unreachable at system startup time, the system will not be accessible for approximately two minutes.
network	Runs accounting for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP Network Control Protocols (NCPs), and AppleTalk Remote Access Protocol (ARAP).
exec	Runs accounting for the EXEC shell session. This keyword might return user profile information such as what is generated by the **autocommand** command.
connection	Provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler and disassembler (PAD), and rlogin.
commands *level*	Runs accounting for all commands at the specified privilege level. Valid privilege level entries are integers from 0 through 15.
dot1x	Provides information about all IEEE 802.1x-related user events.
default	Uses the listed accounting methods that follow this keyword as the default list of methods for accounting services.
list-name	Character string used to name the list of at least one of the following accounting methods: • **group radius**—Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command. • **group tacacs+**—Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command. • **group** *group-name*—Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group *group-name* argument.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration. VRF is used *only* with system accounting.

start-stop	Sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the "start" accounting notice was received by the accounting server.
stop-only	Sends a "stop" accounting notice at the end of the requested user process.
none	Disables accounting services on this line or interface.
broadcast	(Optional) 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.
group *group-name*	Specifies the accounting method list. Enter at least one of the following keywords: • **auth-proxy**—Creates a method list to provide accounting information about all authenticated hosts that use the authentication proxy service. • **commands**—Creates a method list to provide accounting information about specific, individual EXEC commands associated with a specific privilege level. • **connection**—Creates a method list to provide accounting information about all outbound connections made from the network access server. • **exec**—Creates a method list to provide accounting records about user EXEC terminal sessions on the network access server, including username, date, and start and stop times. • **network**—Creates a method list to provide accounting information for SLIP, PPP, NCPs, and ARAP sessions. • **resource**—Creates a method list to provide accounting records for calls that have passed user authentication or calls that failed to be authenticated. • **tunnel**—Creates a method list to provide accounting records (Tunnel-Start, Tunnel-Stop, and Tunnel-Reject) for virtual private dialup network (VPDN) tunnel status changes. • **tunnel-link**—Creates a method list to provide accounting records (Tunnel-Link-Start, Tunnel-Link-Stop, and Tunnel-Link-Reject) for VPDN tunnel-link status changes.

Defaults

AAA accounting is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	Group server support was added.
12.1(1)T	The **broadcast** keyword was introduced on the Cisco AS5300 and Cisco AS5800 universal access servers.

Release	Modification
12.1(5)T	The **auth-proxy** keyword was added.
12.2(1)DX	The **vrf** keyword and *vrf-name* argument were introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were integrated into Cisco IOS Release 12.2(13)T.
12.2(15)B	The tunnel and tunnel-link accounting methods were introduced.
12.3(4)T	The tunnel and tunnel-link accounting methods were integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **dot1x** keyword was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS release 12.(33)SXH.

Usage Guidelines

General Information

Use the **aaa accounting** command to enable accounting and to create named method lists that define specific accounting methods on a per-line or per-interface basis.

Table 1 contains descriptions of keywords for AAA accounting methods.

Table 1 aaa accounting Methods

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

In Table 1, the **group radius** and **group tacacs+** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Cisco IOS software supports the following two methods of accounting:

- 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.
- TACACS+—The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.

Method lists for accounting define the way accounting will be performed. Named accounting method lists enable you to designate a particular security protocol to be used on specific lines or interfaces for particular types of accounting services. Create a list by entering values for the *list-name* argument where *list-name* is any character string used to name this list (excluding the names of methods, such as RADIUS or TACACS+) and method list keywords to identify the methods to be tried in sequence as given.

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 (where this accounting type applies) 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.

Note System accounting does not use named accounting lists; you can define the default list only for system accounting.

For minimal accounting, include the **stop-only** keyword to send a "stop" record accounting notice at the end of the requested user process. For more accounting, you can include the **start-stop** keyword, so that RADIUS or TACACS+ sends a "start" accounting notice at the beginning of the requested process and a "stop" accounting notice at the end of the process. Accounting is stored only on the RADIUS or TACACS+ server. The **none** keyword disables accounting services for the specified line or interface.

To specify an accounting configuration for a particular VRF, specify a default system accounting method list, and use the **vrf** keyword and *vrf-name* argument. System accounting does not have knowledge of VRF unless specified.

When AAA accounting is activated, the network access server monitors either RADIUS accounting attributes or TACACS+ AV pairs pertinent to the connection, depending on the security method you have implemented. The network access server reports these attributes as accounting records, which are then stored in an accounting log on the security server. For a list of supported RADIUS accounting attributes, see the appendix "RADIUS Attributes" in the *Cisco IOS Security Configuration Guide*. For a list of supported TACACS+ accounting AV pairs, see the appendix "TACACS+ Attribute-Value Pairs" in the *Cisco IOS Security Configuration Guide*.

Note This command cannot be used with TACACS or extended TACACS.

Cisco Service Selection Gateway Broadcast Accounting

To configure Cisco Service Selection Gateway (SSG) broadcast accounting, use ssg_broadcast_accounting for the *list-name* argument. For more information about configuring SSG, see the chapter "Configuring Accounting for SSG" in the *Cisco IOS Service Selection Gateway Configuration Guide*, Release 12.4.

Layer 2 LAN Switch Port

You must configure the RADIUS server to perform accounting tasks, such as logging start, stop, and interim-update messages and time stamps. To turn on these functions, enable logging of "Update/Watchdog packets from this AAA client" in your RADIUS server Network Configuration tab. Next, enable "CVS RADIUS Accounting" in your RADIUS server System Configuration tab.

You must enable AAA before you can enter the **aaa accounting** command. To enable AAA and 802.1X (port-based authentication), use the following global configuration mode commands:

- **aaa new-model**
- **aaa authentication dot1x default group radius**

- **dot1x system-auth-control**

Use the **show radius statistics** command to display the number of RADIUS messages that do not receive the accounting response message.

Examples

The following example defines a default commands accounting method list, where accounting services are provided by a TACACS+ security server, set for privilege level 15 commands with a stop-only restriction.

```
aaa accounting commands 15 default stop-only group tacacs+
```

The following example defines a default auth-proxy accounting method list, where accounting services are provided by a TACACS+ security server with a start-stop restriction. The **aaa accounting** command activates authentication proxy accounting.

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization auth-proxy default group tacacs+
aaa accounting auth-proxy default start-stop group tacacs+
```

The following example defines a default system accounting method list, where accounting services are provided by RADIUS security server "server1" with a start-stop restriction. The **aaa accounting** command specifies accounting for vrf "vrf1."

```
aaa accounting system default vrf1 water start-stop group server1
```

The following example defines a default IEEE 802.1x accounting method list, where accounting services are provided by a RADIUS server. The **aaa accounting** command activates IEEE 802.1x accounting.

```
aaa new model
aaa authentication dot1x default group radius
aaa authorization dot1x default group radius
aaa accounting dot1x default start-stop group radius
```

The following example shows how to enable network accounting and send tunnel and tunnel-link accounting records to the RADIUS server. (Tunnel-Reject and Tunnel-Link-Reject accounting records are automatically sent if either start or stop records are configured.)

```
aaa accounting network tunnel start-stop group radius
aaa accounting network session start-stop group radius
```

The following example shows how to enable IEEE 802.1x accounting:

```
aaa accounting dot1x default start-stop group radius
aaa accounting system default start-stop group radius
```

Related Commands

Command	Description
aaa authentication dot1x	Specifies one or more AAA methods for use on interfaces running IEEE 802.1X.
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa group server tacacs+	Groups different server hosts into distinct lists and distinct methods.

Command	Description
aaa new-model	Enables the AAA access control model.
dot1x system-auth-control	Enables port-based authentication.
radius-server host	Specifies a RADIUS server host.
show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.
tacacs-server host	Specifies a TACACS+ server host.

aaa authorization ipmobile

To authorize Mobile IP to retrieve security associations from the AAA server using TACACS+ or RADIUS, use the **aaa authorization ipmobile** command in global configuration mode. To remove authorization, use the **no** form of this command.

aaa authorization ipmobile {[**radius** | **tacacs+**] | **default**} [**group** *server-groupname*]

no aaa authorization ipmobile {[**radius** | **tacacs+**] | **default**} [**group** *server-groupname*]

Syntax Description

radius	Authorization list named radius.
tacacs+	Authorization list named tacacs+.
default	Default authorization list.
group *server-groupname*	(Optional) Name of the server group to use.

Defaults

AAA is not used to retrieve security associations for authentication.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.

Usage Guidelines

Mobile IP requires security associations for registration authentication. The security associations are configured on the router or on a AAA server. This command is not needed for the former; but in the latter case, this command authorizes Mobile IP to retrieve the security associations from the AAA server.

Once the authorization list is named, it can be used in other areas such as login. You can only use one named authorization list; multiple named authorization lists are not supported.

The **aaa authorization ipmobile default group** *server-groupname* command is the most commonly used method to retrieve security associations from the AAA server.

Note The AAA server does not authenticate the user. It stores the security association that is retrieved by the router to authenticate registration.

Examples

The following example uses TACACS+ to retrieve security associations from the AAA server:

```
aaa new-model
aaa authorization ipmobile tacacs+
tacacs-server host 1.2.3.4
tacacs-server key mykey
ip mobile host 10.0.0.1 10.0.0.5 virtual-network 10.0.0.0 255.0.0.0 aaa
```

The following example uses RADIUS as the default group to retrieve security associations from the AAA server:

```
aaa new-model
aaa authentication login default enable
aaa authorization ipmobile default group radius
aaa session-id common
radius-server host 128.107.162.173 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
ip mobile host 10.0.0.1 10.0.0.5 virtual-network 10.0.0.0 255.0.0.0 aaa
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
ip mobile host	Configures the mobile host or mobile node group.
radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
show ip mobile host	Displays mobile node information.
tacacs-server host	Specifies a TACACS host.
tacacs-server key	Sets the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon.

aaa pod server

To enable inbound user sessions to be disconnected when specific session attributes are presented, use the **aaa pod server** command in global configuration mode. To disable this feature, use the **no** form of this command.

aaa pod server [**port** *port number*] [**auth-type** {**any** | **all** | **session-key**}] **server-key** [*encryption-type*] *string*

no aaa pod server

Syntax Description

port *port number*	(Optional) Network access server User Datagram Protocol (UDP) port to use for packet of disconnect (POD) requests. Default value is 1700.
auth-type	(Optional) Type of authorization required for disconnecting sessions. If no authentication type is specified, **auth-type** is the default.
any	(Optional) Session that matches all of the attributes sent in the POD packet is disconnected. The POD packet may contain one or more of four key attributes (user-name, framed-IP-address, session-ID, and session-key).
all	(Optional) Only a session that matches all four key attributes is disconnected. The default is **all**.
session-key	(Optional) Session with a matching session-key attribute is disconnected. All other attributes are ignored.
server-key	Configures the shared-secret text string.
encryption-type	(Optional) Single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Currently defined encryption types are 0, which means that the text immediately following is not encrypted, and 7, which means that the text is encrypted using an encryption algorithm defined by Cisco.
string	Shared-secret text string that is shared between the network access server and the client workstation. This shared-secret string must be the same on both systems.

Defaults

The POD server function is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)XH	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.2(2)XB	The *encryption-type* argument was added, as well as support for the voice applications and the Cisco 3600 series, and Cisco AS5350, and Cisco AS5400 routers.
12.2(2)XB1	Support for the Cisco AS5800 was added.

Release	Modification
12.2(11)T	The *encryption-type* argument and support for the voice applications were added. **Note** Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800 is not included in this release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To disconnect a session, the values in one or more of the key fields in the POD request must match the values for a session on one of the network access server ports. Which values must match depends on the **auth-type** attribute defined in the command. If no **auth-type** attribute is specified, all three values must match. If no match is found, all connections remain intact and an error response is returned. The key fields are as follows:

- An h323-conf-id vendor-specific attribute (VSA) with the same content as received from the gateway for this call.
- An h323-call-origin VSA with the same content as received from the gateway for the leg of interest.
- A 16-byte Message Digest 5 (MD5) hash value that is carried in the *authentication* field of the POD request.

Examples

The following example enables POD and sets the secret key to “xyz123”:

```
aaa pod server server-key xyz123
```

Related Commands

Command	Description
aaa accounting delay-start	Delays generation of the start accounting record until the user IP address is established.
aaa accounting	Enables accounting records.
debug aaa pod	Displays debug messages for POD packets.
radius-server host	Identifies a RADIUS host.

access-list

To configure the access list mechanism for filtering frames by protocol type or vendor code, use the **access-list** command in global configuration mode. To remove the single specified entry from the access list, use the **no** form of this command.

access-list *access-list-number* {**permit** | **deny**} {*type-code wild-mask* | *address mask*}

no access-list *access-list-number* {**permit** | **deny**} {*type-code wild-mask* | *address mask*}

Syntax Description

access-list-number	Integer that identifies the access list. If the *type-code* and *wild-mask* arguments are included, this integer ranges from 200 to 299, indicating that filtering is by protocol type. If the *address* and *mask* arguments are included, this integer ranges from 700 to 799, indicating that filtering is by vendor code.
permit	Permits the frame.
deny	Denies the frame.
type-code	16-bit hexadecimal number written with a leading 0x; for example, 0x6000. Specify either a Link Service Access Point (LSAP) type code for 802-encapsulated packets or a Subnetwork Access Protocol (SNAP) type code for SNAP-encapsulated packets. (LSAP, sometimes called SAP, refers to the type codes found in the DSAP and SSAP fields of the 802 header.)
wild-mask	16-bit hexadecimal number whose ones bits correspond to bits in the *type-code* argument. The *wild-mask* argument indicates which bits in the *type-code* argument should be ignored when making a comparison. (A mask for a DSAP/SSAP pair should always be 0x0101 because these two bits are used for purposes other than identifying the SAP code.)
address	48-bit Token Ring address written as a dotted triple of four-digit hexadecimal numbers. This field is used for filtering by vendor code.
mask	48-bit Token Ring address written as a dotted triple of four-digit hexadecimal numbers. The ones bits in *mask* are the bits to be ignored in *address*. This field is used for filtering by vendor code. For source address filtering, the mask always should have the high-order bit set. This is because the IEEE 802 standard uses this bit to indicate whether a Routing Information Field (RIF) is present, not as part of the source address.

Defaults

No access list is configured.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

For a list of type codes, refer to the "Ethernet Type Codes" appendix of this book.

Examples

In the following example, the access list permits only Novell frames (LSAP 0xE0E0) and filters out all other frame types. This set of access lists would be applied to an interface via the **source-bridge input-lsap list** or **source-bridge input-lsap list** command (described later in this chapter).

```
access-list 201 permit 0xE0E0 0x0101
access-list 201 deny 0x0000 0xFFFF
```

Combine the DSAP/LSAP fields into one number to do LSAP filtering; for example, 0xE0E0—not 0xE0. Note that the deny condition specified in the preceding example is not required; access lists have an implicit deny as the last statement. Adding this statement can serve as a useful reminder, however.

The following access list filters out only SNAP type codes assigned to Digital Equipment Corporation (DEC) (0x6000 to 0x6007) and lets all other types pass. This set of access lists would be applied to an interface using the **source-bridge input-type-list** or **source-bridge output-type-list** command (described later in this chapter).

```
access-list 202 deny 0x6000 0x0007
access-list 202 permit 0x0000 0xFFFF
```

Note Use the last item of an access list to specify a default action; for example, to permit everything else or to deny everything else. If nothing else in the access list matches, the default action is to deny access; that is, filter out all other type codes.

Type code access lists will negatively affect system performance by greater than 30 percent. Therefore, we recommend that you keep the lists as short as possible and use wildcard bit masks whenever possible.

Related Commands

Command	Description
access-expression	Defines an access expression.
source-bridge input-address-list	Applies an access list to an interface configured for source-route bridging, and filters source-routed packets received from the router interface based on the source MAC address.
source-bridge input-lsap-list	Filters, on input, FDDI and IEEE 802-encapsulated packets that include the DSAP and SSAP fields in their frame formats.
source-bridge input-type-list	Filters SNAP-encapsulated packets on input.
source-bridge output-address-list	Applies an access list to an interface configured for SRB, and filters source-routed packets sent to the router interface based on the destination MAC address.
source-bridge output-lsap-list	Filters, on output, FDDI and IEEE 802-encapsulated packets that have DSAP and SSAP fields in their frame formats.
source-bridge output-type-list	Filters SNAP-encapsulated frames by type code on output.

clear ip mobile binding

To remove mobility bindings, use the **clear ip mobile binding** command in privileged EXEC mode.

clear ip mobile binding {**all** [**load** *standby-group-name*] | *ip-address* [**coa** *care-of-address*] | **nai** *string* [**session-id** *string*] | **vrf realm** *realm*} [**synch**]

Syntax Description

all	Clears all mobility bindings.
load *standby-group-name*	(Optional) Downloads mobility bindings for a standby group after a clear operation.
ip-address	IP address of a mobile node or mobile router.
coa *care-of-address*	(Optional) The binding corresponding to the IP address and its care-of address.
nai *string*	Network access identifier (NAI) of the mobile node.
session-id *string*	(Optional) Session identifier. The string value must be fewer than 25 characters in length.
vrf realm *realm*	Specifies the VRF realm.
synch	(Optional) Specifies that the bindings that are administratively cleared on the active home agent are synchronized to the standby home agent, and the bindings will be deleted on the standby home agent.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.1(3)T	The following keywords and argument were added: • **all** • **load** • *standby-group-name*
12.2(2)XC	The **nai** keyword was added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(4)T	The **session-id** keyword was added.
12.4(9)T	The **coa** *care-of-address* keyword and argument combination were added.
12.4(11)T	The **vrf realm** *realm* and **synch** keywords and argument were added.

Usage Guidelines

The home agent creates a mobility binding for each roaming mobile node. Associated with the mobility binding is the tunnel to the visited network and a host route to forward packets destined for the mobile node. Typically, there should be no need to clear the binding because it expires after the lifetime is reached or when the mobile node deregisters.

When the mobility binding is removed through use of this command, the number of users on the tunnel is decremented and the host route is removed from the routing table. The mobile node is not notified.

If the **nai** *string* **session-id** *string* option is specified, only the binding entry with that session identifier is cleared. If the **session-id** keyword is not specified, all binding entries (potentially more than one, with different session identifiers) for that NAI are cleared. You can determine the **session-id** *string* value by using the **show ip mobile binding** command.

When the **synch** option is specified, bindings that are administratively cleared on the active home agent are synchronized to the standby home agent, and the bindings will be deleted on the standby home agent. When the redundancy mode is active-standby, the **synch** option will not take effect if the clear command is issued on the standby home agent.

Use this command with care, because it will disrupt any sessions used by the mobile node. After you use this command, the mobile node will need to reregister to continue roaming.

Examples

The following example administratively stops mobile node 192.168.100.10 from roaming:

```
Router# show ip mobile binding

Mobility Binding List:
Total 1
192.168.100.10:
    Care-of Addr 192.168.6.1, Src Addr 192.168.4.2,
    Lifetime granted 02:46:40 (10000), remaining 02:46:32
    Flags SbdmGvt, Identification B750FAC4.C28F56A8,
    Tunnel100 src 192.168.1.2 dest 192.168.6.1 reverse-allowed
    Routing Options - (G)GRE

Router# clear ip mobile binding 10.2.0.1

Router# show ip mobile binding
```

Related Commands

Command	Description
show ip mobile binding	Displays the mobility binding table.

clear ip mobile host-counters

To clear the mobility counters specific to each mobile node, use the **clear ip mobile host-counters** command in EXEC mode.

clear ip mobile host-counters [[*ip-address* | **nai** *string*] **undo**]]

Syntax Description

ip-address	(Optional) IP address of a mobile node.
nai *string*	(Optional) Network access identifier of the mobile node.
undo	(Optional) Restores the previously cleared counters.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The **nai** keyword was added.
12.2(13)T	The **nai** keyword was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

This command clears the counters that are displayed when you use the **show ip mobile host** command. The **undo** keyword restores the counters (this option is useful for debugging).

Examples

The following example shows how the counters can be used for debugging:

```
Router# show ip mobile host

10.0.0.1:
    Allowed lifetime 10:00:00 (36000/default)
    Roaming status -registered-, Home link on virtual network 20.0.0.0/8
    Accepted 2, Last time 04/13/02 19:04:28
    Overall service time 00:04:42
    Denied 0, Last time -never-
    Last code '-never- (0)'
    Total violations 1
    Tunnel to MN - pkts 0, bytes 0
    Reverse tunnel from MN - pkts 0, bytes 0

    .
Router# clear ip mobile host-counters

Router# show ip mobile host-counters

20.0.0.1:
    Allowed lifetime 10:00:00 (36000/default)
    Roaming status -Unregistered-, Home link on virtual network 20.0.0.0/8
    Accepted 0, Last time -never-
    Overall service time -never-
    Denied 0, Last time -never-
    Last code '-never- (0)'
```

```
Total violations 0
Tunnel to MN - pkts 0, bytes 0
Reverse tunnel from MN - pkts 0, bytes 0
```

Related Commands

Command	Description
show ip mobile host	Displays mobile node counters and information.

clear ip mobile secure

To clear and retrieve remote security associations, use the **clear ip mobile secure** command in EXEC mode.

clear ip mobile secure {**host** *lower* [*upper*] | **nai** *string* | **empty** | **all**} [**load**]

Syntax Description

host	Mobile node host.
lower	IP address of mobile node. Can be used alone, or as lower end of a range of IP addresses.
upper	(Optional) Upper end of a range of IP addresses.
nai *string*	Network access identifier of the mobile node.
empty	Load in only mobile nodes without security associations. Must be used with the **load** keyword.
all	Clears all mobile nodes.
load	(Optional) Reload the security association from the AAA server after security association has been cleared.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The **nai** keyword was added.
12.2(13)T	The **nai** keyword was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Security associations are required for registration authentication. They can be stored on an AAA server. During registration, they may be stored locally after retrieval from the AAA server. The security association on the router may become stale or out of date when the security association on the AAA server changes.

This command clears security associations that have been downloaded from the AAA server.

Note Security associations that are manually configured on the router or not stored on the router after retrieval from the AAA server are not applicable.

Examples

In the following example, the AAA server has the security association for user 10.2.0.1 after registration:

```
Router# show ip mobile secure host 10.2.0.1

Security Associations (algorithm,mode,replay protection,key):
10.2.0.1:
    SPI 300,  MD5, Prefix-suffix, Timestamp +/- 7,
    Key 'oldkey' 1230552d39b7c1751f86bae5205ec0c8
```

If you change the security association stored on the AAA server for this mobile node, the router clears the security association and reloads it from the AAA server:

```
Router# clear ip mobile secure host 10.2.0.1 load

Router# show ip mobile secure host 10.2.0.1

10.2.0.1:
    SPI 300,  MD5, Prefix-suffix, Timestamp +/- 7,
    Key 'newkey' 1230552d39b7c1751f86bae5205ec0c8
```

Related Commands

Command	Description
ip mobile secure	Specifies the mobility security associations for mobile host, visitor, home agent, and foreign agent.

clear ip mobile traffic

To clear counters, use the **clear ip mobile traffic** command in EXEC mode.

clear ip mobile traffic [**undo**]

Syntax Description

undo	(Optional) Restores the previously cleared counters.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.

Usage Guidelines

Mobile IP counters are accumulated during operation. They are useful for debugging and monitoring.

This command clears all Mobile IP counters. The **undo** keyword restores the counters (which is useful for debugging). See the **show ip mobile traffic** command for a description of all counters.

Examples

The following example shows how counters can be used for debugging:

```
Router# show ip mobile traffic
IP Mobility traffic:
Advertisements:
    Solicitations received 0
    Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
    Register 8, Deregister 0 requests
    Register 7, Deregister 0 replied
    Accepted 6, No simultaneous bindings 0
    Denied 1, Ignored 1
    Unspecified 0, Unknown HA 0
    Administrative prohibited 0, No resource 0
    Authentication failed MN 0, FA 0
    Bad identification 1, Bad request form 0
    .
Router# clear ip mobile traffic

Router# show ip mobile traffic
IP Mobility traffic:
Advertisements:
    Solicitations received 0
    Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
    Register 0, Deregister 0 requests
    Register 0, Deregister 0 replied
    Accepted 0, No simultaneous bindings 0
    Denied 0, Ignored 0
    Unspecified 0, Unknown HA 0
    Administrative prohibited 0, No resource 0
    Authentication failed MN 0, FA 0
    Bad identification 0, Bad request form 0
```

Related Commands

Command	Description
show ip mobile traffic	Displays protocol counters.

crypto map (global IPSec)

To enter crypto map configuration mode and create or modify a crypto map entry, to create a crypto profile that provides a template for configuration of dynamically created crypto maps, or to configure a client accounting list, use the **crypto map** command in global configuration mode. To delete a crypto map entry, profile, or set, use the **no** form of this command.

crypto map *map-name seq-num* [**ipsec-manual**]

crypto map *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*]

crypto map *map-name* [**client-accounting-list** *aaalist*]

crypto map *map-name seq-num* [**gdoi**]

no crypto map *map-name seq-num*

Note Issue the **crypto map** *map-name seq-num* command without a keyword to modify an existing crypto map entry.

Syntax Description

map-name	Name that identifies the crypto map set. This is the name assigned when the crypto map was created.
seq-num	Sequence number you assign to the crypto map entry. See additional explanation for using this argument in the "Usage Guidelines" section.
ipsec-manual	(Optional) Indicates that Internet Key Exchange (IKE) will not be used to establish the IP Security (IPSec) security associations (SAs) for protecting the traffic specified by this crypto map entry.
ipsec-isakmp	(Optional) Indicates that IKE will be used to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.
dynamic	(Optional) Specifies that this crypto map entry is to reference a preexisting dynamic crypto map. Dynamic crypto maps are policy templates used in processing negotiation requests from a peer IPSec device. If you use this keyword, none of the crypto map configuration commands will be available.
dynamic-map-name	(Optional) Specifies the name of the dynamic crypto map set that should be used as the policy template.
discover	(Optional) Enables peer discovery. By default, peer discovery is not enabled.
profile	(Optional) Designates a crypto map as a configuration template. The security configurations of this crypto map will be cloned as new crypto maps are created dynamically on demand.
profile-name	(Optional) Name of the crypto profile being created.
client-accounting-list	(Optional) Designates a client accounting list.
aaalist	(Optional) List name.
gdoi	(Optional) Indicates that the key management mechanism is Group Domain of Interpretation (GDOI).

Command Default

No crypto maps exist.
Peer discovery is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
11.3T	The following keywords and arguments were added: • **ipsec-manual** • **ipsec-isakmp** • **dynamic** • *dynamic-map-name*
12.0(5)T	The **discover** keyword was added to support Tunnel Endpoint Discovery (TED).
12.2(4)T	The **profile** *profile-name* keyword and argument combination was added to allow the generation of a crypto map profile that is cloned to create dynamically created crypto maps on demand.
12.2(11)T	This command was implemented on the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
12.2(15)T	The **client-accounting-list** *aaalist* keyword and argument combination was added.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(6)T	The **gdoi** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB without support for the **gdoi** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to create a new crypto map entry, to create a crypto map profile, or to modify an existing crypto map entry or profile.

After a crypto map entry has been created, you cannot change the parameters specified at the global configuration level because these parameters determine which of the configuration commands are valid at the crypto map level. For example, after a map entry has been created using the **ipsec-isakmp** keyword, you cannot change it to the option specified by the **ipsec-manual** keyword; you must delete and reenter the map entry.

After you define crypto map entries, you can assign the crypto map set to interfaces using the **crypto map** (interface IPSec) command.

Crypto Map Functions

Crypto maps provide two functions: filtering and classifying traffic to be protected and defining the policy to be applied to that traffic. The first use affects the flow of traffic on an interface; the second affects the negotiation performed (via IKE) on behalf of that traffic.

IPSec crypto maps define the following:

- What traffic should be protected
- To which IPSec peers the protected traffic can be forwarded—these are the peers with which an SA can be established
- Which transform sets are acceptable for use with the protected traffic
- How keys and SAs should be used or managed (or what the keys are, if IKE is not used)

Multiple Crypto Map Entries with the Same Map Name Form a Crypto Map Set

A crypto map set is a collection of crypto map entries, each with a different *seq-num* argument but the same *map-name* argument. Therefore, for a given interface, you could have certain traffic forwarded to one IPSec peer with specified security applied to that traffic and other traffic forwarded to the same or a different IPSec peer with different IPSec security applied. To accomplish differential forwarding you would create two crypto maps, each with the same *map-name* argument, but each with a different *seq-num* argument. Crypto profiles must have unique names within a crypto map set.

Sequence Numbers

The number you assign to the *seq-num* argument should not be arbitrary. This number is used to rank multiple crypto map entries within a crypto map set. Within a crypto map set, a crypto map entry with a lower *seq-num* is evaluated before a map entry with a higher *seq-num*; that is, the map entry with the lower number has a higher priority.

For example, consider a crypto map set that contains three crypto map entries: mymap 10, mymap 20, and mymap 30. The crypto map set named "mymap" is applied to serial interface 0. When traffic passes through serial interface 0, the traffic is evaluated first for mymap 10. If the traffic matches any access list permit statement entry in the extended access list in mymap 10, the traffic will be processed according to the information defined in mymap 10 (including establishing IPSec SAs when necessary). If the traffic does not match the mymap 10 access list, the traffic will be evaluated for mymap 20, and then mymap 30, until the traffic matches a permit entry in a map entry. (If the traffic does not match a permit entry in any crypto map entry, it will be forwarded without any IPSec security.)

Dynamic Crypto Maps

Refer to the "Usage Guidelines" section of the **crypto dynamic-map** command for a discussion on dynamic crypto maps.

Crypto map entries that reference dynamic map sets should be the lowest priority map entries, allowing inbound SA negotiation requests to try to match the static maps first. Only after the request does not match any of the static maps do you want it to be evaluated against the dynamic map set.

If a crypto map entry references a dynamic crypto map set, make it the lowest priority map entry by giving the it the highest *seq-num* value of all the map entries in a crypto map set.

Create dynamic crypto map entries using the **crypto dynamic-map** command. After you create a dynamic crypto map set, add the dynamic crypto map set to a static crypto map set with the **crypto map** (global IPSec) command using the **dynamic** keyword.

TED

TED is an enhancement to the IPSec feature. Defining a dynamic crypto map allows you to dynamically determine an IPSec peer; however, only the receiving router has this ability. With TED, the initiating router can dynamically determine an IPSec peer for secure IPSec communications.

Dynamic TED helps to simplify IPSec configuration on the individual routers within a large network. Each node has a simple configuration that defines the local network that the router is protecting and the IPSec transforms that are required.

Note TED helps only in discovering peers; otherwise, TED does not function any differently from normal IPSec. Thus, TED does not improve the scalability of IPSec (in terms of performance or the number of peers or tunnels).

Crypto Map Profiles

Crypto map profiles are created using the **profile** *profile-name* keyword and argument combination. Crypto map profiles are used as configuration templates for dynamically creating crypto maps on demand for use with the L2TP Security feature. The relevant SAs in the crypto map profile will be cloned and used to protect IP traffic on the L2TP tunnel.

Note The **set peer** and **match address** commands are ignored by crypto profiles and should not be configured in the crypto map definition.

Examples

The following example shows the minimum required crypto map configuration when IKE will be used to establish the SAs:

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
```

The following example shows the minimum required crypto map configuration when the SAs are manually established:

```
crypto transform-set someset ah-md5-hmac esp-des
crypto map mymap 10 ipsec-manual
 match address 102
 set transform-set someset
 set peer 10.0.0.5
 set session-key inbound ah 256 98765432109876549876543210987654
 set session-key outbound ah 256 fedcbafedcbafedcfedcbafedcbafedc
 set session-key inbound esp 256 cipher 0123456789012345
 set session-key outbound esp 256 cipher abcdefabcdefabcd
```

The following example configures an IPSec crypto map set that includes a reference to a dynamic crypto map set.

Crypto map “mymap 10” allows SAs to be established between the router and either (or both) of two remote IPSec peers for traffic matching access list 101. Crypto map “mymap 20” allows either of two transform sets to be negotiated with the remote peer for traffic matching access list 102.

Crypto map entry “mymap 30” references the dynamic crypto map set “mydynamicmap,” which can be used to process inbound SA negotiation requests that do not match “mymap” entries 10 or 20. In this case, if the peer specifies a transform set that matches one of the transform sets specified in “mydynamicmap,” for a flow permitted by the access list 103, IPSec will accept the request and set up SAs with the remote peer without previously knowing about the remote peer. If the request is accepted, the resulting SAs (and temporary crypto map entry) are established according to the settings specified by the remote peer.

The access list associated with “mydynamicmap 10” is also used as a filter. Inbound packets that match any access list permit statement in this list are dropped for not being IPSec protected. (The same is true for access lists associated with static crypto maps entries.) Outbound packets that match a permit statement without an existing corresponding IPSec SA are also dropped.

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
 set peer 10.0.0.2
crypto map mymap 20 ipsec-isakmp
 match address 102
 set transform-set my_t_set1 my_t_set2
 set peer 10.0.0.3
crypto map mymap 30 ipsec-isakmp dynamic mydynamicmap
!
crypto dynamic-map mydynamicmap 10
 match address 103
 set transform-set my_t_set1 my_t_set2 my_t_set3
```

The following example configures TED on a Cisco router:

```
crypto map testtag 10 ipsec-isakmp dynamic dmap discover
```

The following example configures a crypto profile to be used as a template for dynamically created crypto maps when IPSec is used to protect an L2TP tunnel:

```
crypto map l2tpsec 10 ipsec-isakmp profile l2tp
```

The following example configures a crypto map for a GDOI group member:

```
crypto map diffint 10 gdoi
 set group diffint
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters crypto map configuration command mode.
crypto isakmp profile	Audits IPSec user sessions.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
match address (IPSec)	Specifies an extended access list for a crypto map entry.
set peer (IPSec)	Specifies an IPSec peer in a crypto map entry.
set pfs	Specifies that IPSec should ask for PFS when requesting new SAs for this crypto map entry, or that IPSec requires PFS when receiving requests for new SAs.
set session-key	Specifies the IPSec session keys within a crypto map entry.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPSec)	Displays the crypto map configuration.

crypto map (interface IPSec)

To apply a previously defined crypto map set to an interface, use the **crypto map** command in interface configuration mode. To remove the crypto map set from the interface, use the **no** form of this command.

crypto map *map-name* [**redundancy** *standby-group-name*[**stateful**]]

no crypto map [*map-name*] [**redundancy** *standby-group-name* [**stateful**]]

Syntax Description

map-name	Name that identifies the crypto map set. This is the name assigned when the crypto map was created. When the **no** form of the command is used, this argument is optional. Any value supplied for the argument is ignored.
redundancy	(Optional) Defines a backup IP Security (IPSec) peer. Both routers in the standby group are defined by the redundancy *standby name* and share the same virtual IP address.
standby-group-name	(Optional) Refers to the name of the standby group as defined by Hot Standby Router Protocol (HSRP) standby commands.
stateful	(Optional) Enables IPSec stateful failover for the crypto map.

Defaults

No crypto maps are assigned to interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.1(9)E	The **redundancy** keyword and *standby-name* argument were added.
12.2(8)T	The **redundancy** keyword and *standby-name* argument were integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5800 platforms.
12.2(9)YE	The **redundancy** keyword and *standby-name* argument were integrated into Cisco IOS Release 12.2(9)YE.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.
12.3(11)T	The **stateful** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to assign a crypto map set to an interface. You must assign a crypto map set to an interface before that interface can provide IPSec services. Only one crypto map set can be assigned to an interface. If multiple crypto map entries have the same map name but a different sequence number, they are considered to be part of the same set and will all be applied to the interface. The crypto map entry that has the lowest sequence number is considered the highest priority and will be evaluated first. A single crypto map set can contain a combination of **ipsec-isakmp** and **ipsec-manual crypto map** entries.

Note A crypto map applied to loopback interface is not supported.

The standby name must be configured on all devices in the standby group, and the standby address must be configured on at least one member of the group. If the standby name is removed from the router, the IPSec security associations (SAs) will be deleted. If the standby name is added again, regardless of whether the same name or a different name is used, the crypto map (using the **redundancy** option) will have to be reapplied to the interface.

Note A virtual IP address must be configured in the standby group to enable either stateless or stateful redundancy.

The **stateful** keyword enables stateful failover of IKE and IPSec sessions. Stateful Switchover (SSO) must also be configured for IPSec stateful failover to operate correctly.

Examples

The following example shows how all remote Virtual Private Network (VPN) gateways connect to the router via 192.168.0.3:

```
crypto map mymap 1 ipsec-isakmp
 set peer 10.1.1.1
 reverse-route
 set transform-set esp-3des-sha
 match address 102

Interface FastEthernet 0/0
 ip address 192.168.0.2 255.255.255.0
 standby name group1
 standby ip 192.168.0.3
 crypto map mymap redundancy group1

access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
```

The crypto map on the interface binds this standby address as the local tunnel endpoint for all instances of “mymap” and, at the same time, ensures that stateless HSRP failover is facilitated between an active and standby device that belongs to the same standby group, “group1.”

Reverse route injection (RRI) is also enabled to provide the ability for only the *active* device in the HSRP group to be advertising itself to inside devices as the next hop VPN gateway to the remote proxies. If a failover occurs, routes are deleted on the former active device and created on the new active device.

The following example shows how to configure IPSec stateful failover on the crypto map “to-peer-outside”:

```
crypto map to-peer-outside 10 ipsec-isakmp
 set peer 209.165.200.225
 set transform-set trans1
 match address peer-outside
```

```
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 preempt
 standby 1 name HA-out
 standby 1 track Ethernet1/0
 crypto map to-peer-outside redundancy HA-out stateful
```

Related Commands

Command	Description
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
redundancy inter-device	Configures redundancy and enters inter-device configuration mode.
show crypto map (IPSec)	Displays the crypto map configuration.
standby ip	Assigns an IP address that is to be shared among the members of the HSRP group and owned by the primary IP address.
standby name	Assigns a user-defined group name to the HSRP redundancy group.

debug aaa accounting

To display information on accountable events as they occur, use the **debug aaa accounting** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug aaa accounting

no debug aaa accounting

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Usage Guidelines

The information displayed by the **debug aaa accounting** command is independent of the accounting protocol used to transfer the accounting information to a server. Use the **debug tacacs** and **debug radius** protocol-specific commands to get more detailed information about protocol-level issues.

You can also use the **show accounting** command to step through all active sessions and to print all the accounting records for actively accounted functions. The **show accounting** command allows you to display the active "accountable events" on the system. It provides systems administrators a quick look at what is happening, and may also be useful for collecting information in the event of a data loss of some kind on the accounting server. The **show accounting** command displays additional data on the internal state of the authentication, authorization, and accounting (AAA) security system if **debug aaa accounting** is turned on as well.

Examples

The following is sample output from the **debug aaa accounting** command:

```
Router# debug aaa accounting

16:49:21: AAA/ACCT: EXEC acct start, line 10
16:49:32: AAA/ACCT: Connect start, line 10, glare
16:49:47: AAA/ACCT: Connection acct stop:
task_id=70 service=exec port=10 protocol=telnet address=172.31.3.78 cmd=glare bytes_in=308
bytes_out=76 paks_in=45 paks_out=54 elapsed_time=14
```

Related Commands

Command	Description
debug aaa authentication	Displays information on accountable events as they occur.
debug aaa authorization	Displays information on AAA/TACACS+ authorization.
debug radius	Displays information associated with the RADIUS.
debug tacacs	Displays information associated with the TACACS.

debug aaa pod

To display debug messages related to packet of disconnect (POD) packets, use the **debug aaa pod** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug aaa pod

no debug aaa pod

Syntax Description

This command has no keywords or arguments.

Defaults

Debugging for POD packets is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB	Support for the voice applications as well as support for the Cisco AS5350, Cisco AS5400 and the Cisco 3600 series was added.
12.2(2)XB1	Support for the Cisco AS5800 was added.
12.2(11)T	Support for the Cisco AS5850 was added. This command was integrated into Cisco IOS Release 12.2(11)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example shows output from a successful POD request when using the **show debug** command:

```
Router# debug aaa pod

AAA POD packet processing debugging is on

Router# show debug

General OS:
  AAA POD packet processing debugging is on
Router#
Apr 25 17:15:59.318:POD:172.19.139.206 request queued
Apr 25 17:15:59.318:voice_pod_request:
Apr 25 17:15:59.318:voip_populate_pod_attr_list:
Apr 25 17:15:59.318:voip_pod_get_guid:
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr_len=50
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr=h323-conf-id
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr_len=50 value_len=35
Apr 25 17:15:59.318:voip_pod_get_guid:conf-id=FFA7785F F7F607BB
00000000 993FB1F4 n_bytes=35
Apr 25 17:15:59.318:voip_pod_get_guid:GUID = FFA7785F F7F607BB 00000000
993FB1F4
```

```
Apr 25 17:15:59.318:voip_populate_pod_attr_list:
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr_len=23
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr=h323-originate
Apr 25 17:15:59.318:voip_pod_get_vsa_attr_val:attr_len=23 value_len=6
Apr 25 17:15:59.318:voip_get_call_direction:
Apr 25 17:15:59.318:voip_get_call_direction:returning answer
Apr 25 17:15:59.318:voip_eval_pod_attr:
Apr 25 17:15:59.318:cc_api_trigger_disconnect:
Apr 25 17:15:59.322:POD:Sending ACK to 172.19.139.206/1700
Apr 25 17:15:59.322:voip_pod_clean:
```

Related Commands

Command	Description
aaa pod server	Enables the POD feature.

debug condition

To filter debugging output for certain **debug** commands on the basis of specified conditions, use the **debug condition** command in privileged EXEC mode. To remove the specified condition, use the **no** form of this command.

debug condition {**called** *dial-string* | **caller** *dial-string* | **calling** *tid/imsi string* | **domain** *domain-name* | **ip** *ip-address* | **mac-address** *hexadecimal-MAC-address* | **portbundle ip** *ip-address* **bundle** *bundle-number* | **session-id** *session-number* | **username** *username* | **vcid** *vc-id*}

no debug condition {*condition-id* | **all**}

Syntax Description

called *dial-string*	Filters output on the basis of the called party number.
caller *dial-string*	Filters output on the basis of the calling party number.
calling *tid/imsi string*	Filters debug messages for general packet radio service (GPRS) tunneling protocol (GTP) processing on the gateway GPRS support node (GGSN) based on the tunnel identifier (TID) or international mobile system identifier (IMSI) in a Packet Data Protocol (PDP) Context Create Request message.
domain *domain-name*	Filters output on the basis of the specified domain.
ip *ip-address*	Filters output on the basis of the specified IP address.
mac-address *hexadecimal-MAC-address*	Filters messages on the specified MAC address.
portbundle ip *IP-address*	Filters output on the basis of the port-bundle host key (PBHK) that uniquely identifies the session.
bundle *bundle-number*	Specifies the port bundle.
session-id *session-number*	Filters output on the specified Intelligent Service Architecture (ISA) session identifier.
username *username*	Filters output on the basis of the specified username.
vcid *vc-id*	Filters output on the basis of the specified VC ID.
condition-id	Removes the condition indicated.
all	Removes all debugging conditions, and conditions specified by the **debug condition interface** command. Use this keyword to disable conditional debugging and reenable debugging for all interfaces.

Defaults

All debugging messages for enabled protocol-specific **debug** commands are generated.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S. This command was updated with the **vcid** and **ip** keywords to support the debugging of Any Transport over MPLS (AToM) messages.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Relese 12.2(15)T.
12.3(2)XB	This command was introduced on the GGSN.
12.3(8)T	The **calling** keyword and *tid/imsi string* argument were added.
12.2(28)SB	The ability to filter output on the following conditions was added: domain, MAC address, PBHK, and ISA session ID.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **debug condition** command to restrict the debug output for some commands. If any **debug condition** commands are enabled, output is generated only for interfaces associated with the specified keyword. In addition, this command enables debugging output for conditional debugging events. Messages are displayed as different interfaces meet specific conditions.

If multiple **debug condition** commands are enabled, output is displayed if at least one condition matches. All the conditions do not need to match.

The **no** form of this command removes the debug condition specified by the condition identifier. The condition identifier is displayed after you use a **debug condition** command or in the output of the **show debug condition** command. If the last condition is removed, debugging output resumes for all interfaces. You will be asked for confirmation before removing the last condition or all conditions.

Not all debugging output is affected by the **debug condition** command. Some commands generate output whenever they are enabled, regardless of whether they meet any conditions.

The following components are supported for Intelligent Service Architecture (ISA) distributed conditional debugging:

- Authentication, authorization, and accounting (AAA) and RADIUS
- ATM components
- Feature Manager
- Policy Manager
- PPP
- PPP over Ethernet (PPPoE)
- Session Manager
- Virtual Private Dialup Network (VPDN)

Ensure that you enable TID/IMSI-based conditional debugging by entering **debug condition calling** before configuring **debug gprs gtp** and **debug gprs charging**. In addition, ensure that you disable the **debug gprs gtp** and **debug gprs charging** commands using the **no debug all** command before disabling conditional debugging using the **no debug condition** command. This will prevent a flood of debugging messages when you disable conditional debugging.

Examples

Example 1

In the following example, the router displays debugging messages only for interfaces that use a username of "user1". The condition identifier displayed after the command is entered identifies this particular condition.

```
Router# debug condition username user1

Condition 1 set
```

Example 2

The following example specifies that the router should display debugging messages only for VC 1000:

```
Router# debug condition vcid 1000

Condition 1 set
01:12:32: 1000 Debug: Condition 1, vcid 1000 triggered, count 1
01:12:32: 1000 Debug: Condition 1, vcid 1000 triggered, count 1
```

The following example enables other debugging commands. These debugging commands will only display information for VC 1000.

```
Router# debug mpls l2transport vc event

AToM vc event debugging is on

Router# debug mpls l2transport vc fsm

AToM vc fsm debugging is on
```

The following commands shut down the interface on which VC 1000 is established.

```
Router(config)# interface s3/1/0
Router(config-if)# shut
```

The debugging output shows the change to the interface where VC 1000 is established.

```
01:15:59: AToM MGR [13.13.13.13, 1000]: Event local down, state changed from established
to remote ready
01:15:59: AToM MGR [13.13.13.13, 1000]: Local end down, vc is down
01:15:59: AToM SMGR [13.13.13.13, 1000]: Processing imposition update, vc_handle 6227BCF0,
update_action 0, remote_vc_label 18
01:15:59: AToM SMGR [13.13.13.13, 1000]: Imposition Disabled
01:15:59: AToM SMGR [13.13.13.13, 1000]: Processing disposition update, vc_handle
6227BCF0, update_action 0, local_vc_label 755
01:16:01:%LINK-5-CHANGED: Interface Serial3/1/0, changed state to administratively down
01:16:02:%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/1/0, changed state to
down
```

Related Commands

Command	Description
debug condition interface	Limits output for some debugging commands based on the interfaces.

debug ip mobile

To display IP mobility activities, use the **debug ip mobile** command in privileged EXEC mode.

debug ip mobile [**advertise** | **host** [*access-list-number*] | **local-area** | **redundancy** | **udp-tunneling**]

Syntax Description

advertise	(Optional) Advertisement information.
host	(Optional) The mobile node host.
access-list-number	(Optional) The number of an IP access list.
local-area	(Optional) The local area.
redundancy	(Optional) Redundancy activities.
udp-tunneling	(Optional) User Datagram Protocol (UDP) tunneling activities.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.0(2)T	The **standby** keyword was added.
12.2(8)T	The **standby** keyword was replaced by the **redundancy** keyword.
12.2(13)T	This command was enhanced to display information about foreign agent reverse tunnels and the mobile networks attached to the mobile router.
12.3(8)T	The **udp-tunneling** keyword was added and the command was enhanced to display information about NAT traversal using UDP tunneling.
12.3(7)XJ	This command was enhanced to include the Resource Management capability.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **debug ip mobile redundancy** command to troubleshoot redundancy problems.

No per-user debugging output is shown for mobile nodes using the network access identifier (NAI) for the **debug ip mobile host** command. Debugging of specific mobile nodes using an IP address is possible through the access list.

Examples

The following is sample output from the **debug ip mobile** command when foreign agent reverse tunneling is enabled:

```
MobileIP:MN 14.0.0.30 deleted from ReverseTunnelTable of Ethernet2/1(Entries 0)
```

The following is sample output from the **debug ip mobile advertise** command:

```
Router# debug ip mobile advertise

MobileIP: Agent advertisement sent out Ethernet1/2: type=16, len=10, seq=1,
lifetime=36000,
flags=0x1400(rbhFmGv-rsv-),
Care-of address: 68.0.0.31
Prefix Length ext: len=1 (8 )
FA Challenge value:769C808D
```

Table 2 describes the significant fields shown in the display.

Table 2 debug ip mobile advertise Field Descriptions

Field	Description
type	Type of advertisement.
len	Length of extension (in bytes).
seq	Sequence number of this advertisement.
lifetime	Lifetime (in seconds).
flags	Capital letters represent bits that are set; lowercase letters represent unset bits.
Care-of address	IP address.
Prefix Length ext	Number of prefix lengths advertised. This is the bits in the mask of the interface sending this advertisement. Used for roaming detection.
FA Challenge value	Foreign Agent challenge value (randomly generated by the foreign agent.)

The following is sample output from the **debug ip mobile host** command:

```
Router# debug ip mobile host

MobileIP: HA received registration for MN 20.0.0.6 on interface Ethernet1 using COA
68.0.0.31 HA 66.0.0.5 lifetime 30000 options sbdmgvT
MobileIP: Authenticated FA 68.0.0.31 using SPI 110 (MN 20.0.0.6)
MobileIP: Authenticated MN 20.0.0.6 using SPI 300

MobileIP: HA accepts registration from MN 20.0.0.6
MobileIP: Mobility binding for MN 20.0.0.6 updated
MobileIP: Roam timer started for MN 20.0.0.6, lifetime 30000
MobileIP: MH auth ext added (SPI 300) in reply to MN 20.0.0.6
MobileIP: HF auth ext added (SPI 220) in reply to MN 20.0.0.6

MobileIP: HA sent reply to MN 20.0.0.6
```

The following is sample output from the **debug ip mobile redundancy** command. In this example, the active home agent receives a registration request from mobile node 20.0.0.2 and sends a binding update to peer home agent 1.0.0.2:

```
MobileIP:MN 20.0.0.2 - sent BindUpd to HA 1.0.0.2 HAA 20.0.0.1
MobileIP:HA standby maint started - cnt 1
MobileIP:MN 20.0.0.2 - sent BindUpd id 3780410816 cnt 0 elapsed 0
adjust -0 to HA 1.0.0.2 in grp 1.0.0.10 HAA 20.0.0.1
```

In this example, the standby home agent receives a binding update for mobile node 20.0.0.2 sent by the active home agent:

```
MobileIP:MN 20.0.0.2 - HA rcv BindUpd from 1.0.0.3 HAA 20.0.0.1
```

The following is sample output from the **debug ip mobile udp-tunneling** command and displays the registration, authentication, and establishment of UDP tunneling of a mobile node (MN) with a foreign agent (FA):

```
Dec 31 12:34:25.707: UDP: rcvd src=10.10.10.10(434),dst=10.30.30.1(434), length=54
Dec 31 12:34:25.707: MobileIP: ParseRegExt type MHAE(32) addr 2000FEEC end 2000FF02
Dec 31 12:34:25.707: MobileIP: ParseRegExt skipping 10 to next
Dec 31 12:34:25.707: MobileIP: FA rcv registration for MN 10.10.10.10 on Ethernet2/2 using
 COA 10.30.30.1 HA 10.10.10.100 lifetime 65535 options sbdmg-T-identification
 C1BC0D4FB01AC0D8
Dec 31 12:34:25.707: MobileIP: Ethernet2/2 glean 10.10.10.10 accepted
Dec 31 12:34:25.707: MobileIP: Registration request byte count = 74
Dec 31 12:34:25.707: MobileIP: FA queued MN 10.10.10.10 in register table
Dec 31 12:34:25.707: MobileIP: Visitor registration timer started for MN 10.10.10.10,
 lifetime 120
Dec 31 12:34:25.707: MobileIP:  Adding UDP Tunnel req extension
Dec 31 12:34:25.707: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:25.707: MobileIP: MN 10.10.10.10 FHAE added to HA 10.10.10.100 using SPI 1000
Dec 31 12:34:25.707: MobileIP: FA forwarded registration for MN 10.10.10.10 to HA
 10.10.10.100
Dec 31 12:34:25.715: UDP: rcvd src=10.10.10.100(434), dst=10.30.30.1(434), length=94
Dec 31 12:34:25.715: MobileIP: ParseRegExt type NVSE(134) addr 20010B28 end 20010B6A
Dec 31 12:34:25.715: MobileIP: ParseRegExt type MN-config NVSE(14) subtype 1 (MN prefix
 length) prefix length (24)
Dec 31 12:34:25.715: MobileIP: ParseRegExt skipping 12 to next
Dec 31 12:34:25.715: MobileIP: ParseRegExt type MHAE(32) addr 20010B36 end 20010B6A
Dec 31 12:34:25.715: MobileIP: ParseRegExt skipping 10 to next
Dec 31 12:34:25.715: MobileIP: ParseRegExt type UDPTUNREPE(44) addr 20010B4C end 20010B6A
Dec 31 12:34:25.715: Parsing UDP Tunnel Reply Extension - length 6
Dec 31 12:34:25.715: MobileIP: ParseRegExt skipping 6 to next
Dec 31 12:34:25.715: MobileIP: ParseRegExt type FHAE(34) addr 20010B54 end 20010B6A
Dec 31 12:34:25.715: MobileIP: ParseRegExt skipping 20 to next
Dec 31 12:34:25.715: MobileIP: FA rcv accept (0) reply for MN 10.10.10.10 on Ethernet2/3
 using HA 10.10.10.100 lifetime 65535
Dec 31 12:34:25.719: MobileIP: Authenticating HA 10.10.10.100 using SPI 1000
Dec 31 12:34:25.719: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:25.719: MobileIP: Authenticated HA 10.10.10.100 using SPI 1000 and 16 byte
 key
Dec 31 12:34:25.719: MobileIP: HA accepts UDP Tunneling
Dec 31 12:34:25.719: MobileIP: Update visitor table for MN 10.10.10.10
Dec 31 12:34:25.719: MobileIP: Enabling UDP Tunneling
Dec 31 12:34:25.719: MobileIP: Tunnel0 (MIPUDP/IP) created with src 10.30.30.1 dst
 10.10.10.100
Dec 31 12:34:25.719: MobileIP: Setting up UDP Keep-Alive Timer for tunnel 10.30.30.1:0 -
 10.10.10.100:0 with keep-alive 30
Dec 31 12:34:25.719: MobileIP: Starting the tunnel keep-alive timer
Dec 31 12:34:25.719: MobileIP: ARP entry for MN 10.10.10.10 using 10.10.10.10 inserted on
 Ethernet2/2
Dec 31 12:34:25.719: MobileIP: FA route add 10.10.10.10 successful. Code = 0
Dec 31 12:34:25.719: MobileIP: MN 10.10.10.10 added to ReverseTunnelTable of Ethernet2/2
 (Entries 1)
Dec 31 12:34:25.719: MobileIP: FA dequeued MN 10.10.10.10 from register table
Dec 31 12:34:25.719: MobileIP: MN 10.10.10.10 using 10.10.10.10 visiting on Ethernet2/2
Dec 31 12:34:25.719: MobileIP: Reply in for MN 10.10.10.10 using 10.10.10.10, accepted
Dec 31 12:34:25.719: MobileIP: registration reply byte count = 84
Dec 31 12:34:25.719: MobileIP: FA forwarding reply to MN 10.10.10.10 (10.10.10.10 mac
 0060.70ca.f021)
Dec 31 12:34:26.095: MobileIP: agent advertisement byte count = 48
Dec 31 12:34:26.095: MobileIP: Agent advertisement sent out Ethernet2/2: type=16, len=10,
 seq=55, lifetime=65535, flags=0x1580(rbhFmG-TU),
Dec 31 12:34:26.095: Care-of address: 10.30.30.1
Dec 31 12:34:26.719: MobileIP: swif coming up Tunnel0
```

```
!
Dec 31 12:34:35.719: UDP: sent src=10.30.30.1(434), dst=10.10.10.100(434)
Dec 31 12:34:35.719: UDP: rcvd src=10.10.10.100(434), dst=10.30.30.1(434), length=32d0
```

The following is sample output from the **debug ip mobile udp-tunneling** command and displays the registration, authentication, and establishment of UDP tunneling of a MN with a home agent (HA):

```
Dec 31 12:34:26.167: MobileIP: ParseRegExt skipping 20 to next
Dec 31 12:34:26.167: MobileIP: ParseRegExt type UDPTUNREQE(144) addr 2001E762 end 2001E780
Dec 31 12:34:26.167: MobileIP: Parsing UDP Tunnel Request Extension - length 6
Dec 31 12:34:26.167: MobileIP: ParseRegExt skipping 6 to next
Dec 31 12:34:26.167: MobileIP: ParseRegExt type FHAE(34) addr 2001E76A end 2001E780
Dec 31 12:34:26.167: MobileIP: ParseRegExt skipping 20 to next
Dec 31 12:34:26.167: MobileIP: HA 167 rcv registration for MN 10.10.10.10 on Ethernet2/1
 using HomeAddr 10.10.10.10 COA 10.30.30.1 HA 10.10.10.100 lifetime 65535 options
 sbdmg-T-identification C1BC0D4FB01AC0D8
Dec 31 12:34:26.167: MobileIP: NAT detected SRC:10.10.10.50 COA: 10.30.30.1
Dec 31 12:34:26.167: MobileIP: UDP Tunnel Request accepted 10.10.10.50:434
Dec 31 12:34:26.167: MobileIP: Authenticating FA 10.30.30.1 using SPI 1000
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and truncated key
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.167: MobileIP: Authenticated FA 10.30.30.1 using SPI 1000 and 16 byte key
Dec 31 12:34:26.167: MobileIP: Authenticating MN 10.10.10.10 using SPI 1000
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and truncated key
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.167: MobileIP: Authenticated MN 10.10.10.10 using SPI 1000 and 16 byte key
Dec 31 12:34:26.167: MobileIP: Mobility binding for MN 10.10.10.10 created
Dec 31 12:34:26.167: MobileIP: NAT detected for MN 10.10.10.10. Terminating tunnel on
 10.10.10.50
Dec 31 12:34:26.167: MobileIP: Tunnel0 (MIPUDP/IP) created with src 10.10.10.100 dst
 10.10.10.50
Dec 31 12:34:26.167: MobileIP: Setting up UDP Keep-Alive Timer for tunnel 10.10.10.100:0 -
 10.10.10.50:0 with keep-alive 30
Dec 31 12:34:26.167: MobileIP: Starting the tunnel keep-alive timer
Dec 31 12:34:26.167: MobileIP: MN 10.10.10.10 Insert route for 10.10.10.10/255.255.255.255
 via gateway 10.10.10.50 on Tunnel0
Dec 31 12:34:26.167: MobileIP: MN 10.10.10.10 is now roaming
Dec 31 12:34:26.171: MobileIP: Gratuitous ARPs sent for MN 10.10.10.10 MAC 0002.fca5.bc39
Dec 31 12:34:26.171: MobileIP: Mask for address is 24
Dec 31 12:34:26.171: MobileIP: HA accepts registration from MN 10.10.10.10
Dec 31 12:34:26.171: MobileIP: Dynamic and Static Network Extension Length 0 - 0
Dec 31 12:34:26.171: MobileIP: Composed mobile network extension length:0
Dec 31 12:34:26.171: MobileIP: Added prefix length vse in reply
Dec 31 12:34:26.171: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.171: MobileIP: MN 10.10.10.10 MHAE added to MN 10.10.10.10 using SPI 1000
Dec 31 12:34:26.171: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.171: MobileIP: MN 10.10.10.10 FHAE added to FA 10.10.10.50 using SPI 1000
Dec 31 12:34:26.171: MobileIP: MN 10.10.10.10 - HA sent reply to 10.10.10.50
Dec 31 12:34:26.171: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.171: MobileIP: MN 10.10.10.10 HHAE added to HA 10.10.10.3 using SPI 1000
Dec 31 12:34:26.175: MobileIP: ParseRegExt type CVSE(38) addr 2000128C end 200012AE
Dec 31 12:34:26.175: MobileIP: ParseRegExt type HA red. version CVSE(6)
Dec 31 12:34:26.175: MobileIP: ParseRegExt skipping 8 to next
Dec 31 12:34:26.175: MobileIP: ParseRegExt type HHAE(35) addr 20001298 end 200012AE
Dec 31 12:34:26.175: MobileIP: ParseRegExt skipping 20 to next
Dec 31 12:34:26.175: MobileIP: Authenticating HA 10.10.10.3 using SPI 1000
Dec 31 12:34:26.175: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.175: MobileIP: Authentication algorithm MD5 and truncated key
Dec 31 12:34:26.175: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.175: MobileIP: Authenticated HA 10.10.10.3 using SPI 1000 and 16 byte key
Dec 31 12:34:27.167: MobileIP: swif coming up Tunnel0d0
```

debug ip mobile advertise

The **debug ip mobile advertise** command was consolidated with the **debug ip mobile** command. See the description of the **debug ip mobile** command in the "Debug Commands" chapter for more information.

To display advertisement information, use the **debug ip mobile advertise** EXEC command .

debug ip mobile advertise

no debug ip mobile advertise

Syntax Description

This command has no arguments or keywords.

Defaults

No default values.

Command Modes

EXEC mode

Command History

Release	Modification
12.0(1)T	This command was introduced.

Examples

The following is sample output from the **debug ip mobile advertise** command. Table 3 describes significant fields shown in the display.

```
Router# debug ip mobile advertise

MobileIP: Agent advertisement sent out Ethernet1/2: type=16, len=10, seq=1,
lifetime=36000,
flags=0x1400(rbhFmGv-rsv-),
Care-of address: 14.0.0.31
Prefix Length ext: len=1 (8 )
```

Table 3 Debug IP Mobile Advertise Field Descriptions

Field	Description
type	Type of advertisement.
len	Length of extension in bytes.
seq	Sequence number of this advertisement.
lifetime	Lifetime in seconds.
flags	Capital letters represent bits that are set, lower case letters represent unset bits.
Care-of address	IP address.
Prefix Length ext	Number of prefix lengths advertised. This is the bits in the mask of the interface sending this advertisement. Used for roaming detection.

debug ip mobile host

The **debug ip mobile host** command was consolidated with the **debug ip mobile** command. See the description of the **debug ip mobile** command in the "Debug Commands" chapter for more information.

Use the **debug ip mobile host** EXEC command to display IP mobility events.

debug ip mobile host [[*access-list-number*]**|[nai {*NAI username* | *username@realm*}]**

no debug ip mobile host [[*access-list-number*]**|[nai {*NAI username* | *username@realm*}]**

Syntax Description

host [*access-list-number*]	(Optional) The mobile node host.
nai **{*NAI username* | *username@realm*}**	(Optional) Mobile host identified by NAI.

Defaults

No default values.

Command History

Release	Modification
12.0(1)T	This command was introduced.

Examples

The following is sample output from the **debug ip mobile host** command:

```
Router# debug ip mobile host

MobileIP: HA received registration for MN 10.0.0.6 on interface Ethernet1 using COA
14.0.0.31 HA 15.0.0.5 lifetime 30000 options sbdmgvT
MobileIP: Authenticated FA 15.0.0.31 using SPI 110 (MN 20.0.0.6)
MobileIP: Authenticated MN 11.0.0.6 using SPI 300

MobileIP: HA accepts registration from MN 11.0.0.6
MobileIP: Mobility binding for MN 11.0.0.6 updated
MobileIP: Roam timer started for MN 11.0.0.6, lifetime 30000
MobileIP: MH auth ext added (SPI 300) in reply to MN 11.0.0.6
MobileIP: HF auth ext added (SPI 220) in reply to MN 11.0.0.6

MobileIP: HA sent reply to MN 11.0.0.6
```

debug ip mobile redundancy

The **debug ip mobile redundancy** command was consolidated with the **debug ip mobile** command. See the description of the **debug ip mobile** command in the "Debug Commands" chapter for more information.

Use the **debug ip mobile redundancy** EXEC command to display IP mobility events.

debug ip mobile redundancy

no debug ip mobile redundancy

Syntax Description

This command has no keywords or arguments.

Defaults

No default values.

Command History

Release	Modification
12.0(1)T	This command was introduced.

Examples

The following is sample output from the debug ip mobile redundancy command:

```
Router# debug ip mobile redundancy

00:19:21: MobileIP: Adding MN service flags to bindupdate
00:19:21: MobileIP:  Adding MN service flags 0 init registration flags 1
00:19:21: MobileIP: Adding a hared version cvse - bindupdate
00:19:21: MobileIP: HARelayBindUpdate version number 2MobileIP: MN 14.0.0.20 - sent
BindUpd to HA 11.0.0.3 HAA 11.0.0.4
00:19:21: MobileIP: HA standby maint started - cnt 1
00:19:21: MobileIP: MN 14.0.0.20 - HA rcv BindUpdAck accept from 11.0.0.3 HAA 11.0.0.4
00:19:22: MobileIP: HA standby maint started - cnt 1
```

debug radius

To display information associated with RADIUS, use the **debug radius** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug radius [**brief** | **hex**]

no debug radius [**brief** | **hex**]

Syntax Description

brief	(Optional) Displays abbreviated debug output.
hex	(Optional) Displays debugging output in hexadecimal notation.

Defaults

Debugging output in ASCII format is enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2(1)T	This command was introduced.
12.2(11)T	The **brief** and **hex** keywords were added. The default output format became ASCII rather than hexadecimal.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

RADIUS is a distributed security system that secures networks against unauthorized access. Cisco supports RADIUS under the authentication, authorization, and accounting (AAA) security system. When RADIUS is used on the router, you can use the **debug radius** command to display detailed debugging and troubleshooting information in ASCII format. Use the **debug radius brief** command for abbreviated output displaying client/server interaction and minimum packet information. Use the **debug radius hex** command to display packet dump information that has not been truncated in hex format.

Examples

The following is sample output from the **debug radius** command:

```
Router# debug radius

Radius protocol debugging is on
Radius packet hex dump debugging is off
Router#
00:02:50: RADIUS: ustruct sharecount=3
00:02:50: Radius: radius_port_info() success=0 radius_nas_port=1
00:02:50: RADIUS: Initial Transmit ISDN 0:D:23 id 0 10.0.0.1:1824, Accounting-Request, len
358
00:02:50: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.0
00:02:50: RADIUS:  Vendor, Cisco       [26]  19  VT=02 TL=13 ISDN 0:D:23
00:02:50: RADIUS:  NAS-Port-Type       [61]  6   Async
00:02:50: RADIUS:  User-Name           [1]   12  "4085554206"
00:02:50: RADIUS:  Called-Station-Id   [30]  7   "52981"
```

```
00:02:50: RADIUS:  Calling-Station-Id  [31]  12  "4085554206"
00:02:50: RADIUS:  Acct-Status-Type    [40]  6   Start
00:02:50: RADIUS:  Service-Type        [6]   6   Login
00:02:50: RADIUS:  Vendor, Cisco       [26]  27  VT=33 TL=21 h323-gw-id=5300_43.
00:02:50: RADIUS:  Vendor, Cisco       [26]  55  VT=01 TL=49
h323-incoming-conf-id=8F3A3163 B4980003 0 29BD0
00:02:50: RADIUS:  Vendor, Cisco       [26]  31  VT=26 TL=25 h323-call-origin=answer
00:02:50: RADIUS:  Vendor, Cisco       [26]  32  VT=27 TL=26 h323-call-type=Telephony
00:02:50: RADIUS:  Vendor, Cisco      [26]  57  VT=25 TL=51 h323-setup-time=*16:02:48.681
PST Fri Dec 31 1999
00:02:50: RADIUS:  Vendor, Cisco       [26]  46  VT=24 TL=40 h323-conf-id=8F3A3163
B4980003 0 29BD0
00:02:50: RADIUS:  Acct-Session-Id     [44]  10  "00000002"
00:02:50: RADIUS:  Delay-Time          [41]  6   0
00:02:51: RADIUS: Received from id 0 1.7.157.1:1824, Accounting-response, len 20
00:02:51: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to 4085274206
00:03:01: RADIUS: ustruct sharecount=3
00:03:01: Radius: radius_port_info() success=0 radius_nas_port=1
00:03:01: RADIUS: Initial Transmit ISDN 0:D:23 id 1 1.7.157.1:1823, Access-Request, len
171
00:03:01: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.0
00:03:01: RADIUS:  Vendor, Cisco       [26]  19  VT=02 TL=13 ISDN 0:D:23
00:03:01: RADIUS:  NAS-Port-Type       [61]  6   Async
00:03:01: RADIUS:  User-Name           [1]   8   "123456"
00:03:01: RADIUS:  Vendor, Cisco       [26]  46  VT=24 TL=40 h323-conf-id=8F3A3163
B4980003 0 29BD0
00:03:01: RADIUS:  Calling-Station-Id  [31]  12  "4085554206"
00:03:01: RADIUS:  User-Password       [2]   18  *
00:03:01: RADIUS:  Vendor, Cisco       [26]  36  VT=01 TL=30 h323-ivr-out=transactionID:0
00:03:01: RADIUS: Received from id 1 1.7.157.1:1823, Access-Accept, len 115
00:03:01: RADIUS:  Service-Type        [6]   6   Login
00:03:01: RADIUS:  Vendor, Cisco       [26]  29  VT=101 TL=23 h323-credit-amount=45
00:03:01: RADIUS:  Vendor, Cisco       [26]  27  VT=102 TL=21 h323-credit-time=33
00:03:01: RADIUS:  Vendor, Cisco       [26]  26  VT=103 TL=20 h323-return-code=0
00:03:01: RADIUS:  Class               [25]  7   6C6F63616C
00:03:01: RADIUS: saved authorization data for user 62321E14 at 6233D258
00:03:13: %ISDN-6-DISCONNECT: Interface Serial0:22  disconnected from 4085274206, call
lasted 22 seconds
00:03:13: RADIUS: ustruct sharecount=2
00:03:13: Radius: radius_port_info() success=0 radius_nas_port=1
00:03:13: RADIUS: Sent class "local" at 6233D2C4 from user 62321E14
00:03:13: RADIUS: Initial Transmit ISDN 0:D:23 id 2 1.7.157.1:1824, Accounting-Request,
len 775
00:03:13: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.0
00:03:13: RADIUS:  Vendor, Cisco       [26]  19  VT=02 TL=13 ISDN 0:D:23
00:03:13: RADIUS:  NAS-Port-Type       [61]  6   Async
00:03:13: RADIUS:  User-Name           [1]   8   "123456"
00:03:13: RADIUS:  Called-Station-Id   [30]  7   "52981"
00:03:13: RADIUS:  Calling-Station-Id  [31]  12  "4085274206"
00:03:13: RADIUS:  Acct-Status-Type    [40]  6   Stop
00:03:13: RADIUS:  Class               [25]  7   6C6F63616C
00:03:13: RADIUS:  Undebuggable        [45]  6   00000001
00:03:13: RADIUS:  Service-Type        [6]   6   Login
00:03:13: RADIUS:  Vendor, Cisco       [26]  27  VT=33 TL=21 h323-gw-id=5300_43.
00:03:13: RADIUS:  Vendor, Cisco       [26]  55  VT=01 TL=49
h323-incoming-conf-id=8F3A3163 B4980003 0 29BD0
00:03:13: RADIUS:  Vendor, Cisco       [26]  31  VT=26 TL=25 h323-call-origin=answer
00:03:13: RADIUS:  Vendor, Cisco       [26]  32  VT=27 TL=26 h323-call-type=Telephony
00:03:13: RADIUS:  Vendor, Cisco      [26]  57  VT=25 TL=51 h323-setup-time=*16:02:48.681
PST Fri Dec 31 1999
00:03:13: RADIUS:  Vendor, Cisco       [26]  59  VT=28 TL=53
h323-connect-time=*16:02:48.946 PST Fri Dec 31 1999
00:03:13: RADIUS:  Vendor, Cisco       [26]  62  VT=29 TL=56in=0
00:03:13: RADIUS:  Vendor, Cisco       [26]  23  VT=01 TL=17 pre-bytes-out=0
```

```
00:03:13: RADIUS:  Vendor, Cisco       [26]  21  VT=01 TL=15 pre-paks-in=0
00:03:13: RADIUS:  Vendor, Cisco       [26]  22  VT=01 TL=16 pre-paks-out=0
00:03:13: RADIUS:  Vendor, Cisco       [26]  22  VT=01 TL=16 nas-rx-speed=0
00:03:13: RADIUS:  Vendor, Cisco       [26]  22  VT=01 TL=16 nas-tx-speed=0
00:03:13: RADIUS:  Delay-Time          [41]  6   0
00:03:13: RADIUS: Received from id 2 1.7.157.1:1824, Accounting-response, len 20
h323-disconnect-time=*16:03:11.306 PST Fri Dec 31 1999
00:03:13: RADIUS:  Vendor, Cisco       [26]  32  VT=30 TL=26 h323-disconnect-cause=10
00:03:13: RADIUS:  Vendor, Cisco       [26]  28  VT=31 TL=22 h323-voice-quality=0
00:03:13: RADIUS:  Vendor, Cisco       [26]  46  VT=24 TL=40 h323-conf-id=8F3A3163
B4980003 0 29BD0
00:03:13: RADIUS:  Acct-Session-Id     [44]  10  "00000002"
00:03:13: RADIUS:  Acct-Input-Octets   [42]  6   0
00:03:13: RADIUS:  Acct-Output-Octets  [43]  6   88000
00:03:13: RADIUS:  Acct-Input-Packets  [47]  6   0
00:03:13: RADIUS:  Acct-Output-Packets [48]  6   550
00:03:13: RADIUS:  Acct-Session-Time   [46]  6   22
00:03:13: RADIUS:  Vendor, Cisco       [26]  30  VT=01 TL=24 subscriber=RegularLine
00:03:13: RADIUS:  Vendor, Cisco       [26]  35  VT=01 TL=29 h323-ivr-out=Tariff:Unknown
00:03:13: RADIUS:  Vendor, Cisco       [26]  22  VT=01 TL=16 pre-bytes-
```

The following is sample output from the **debug radius brief** command:

```
Router# debug radius brief

Radius protocol debugging is on
Radius packet hex dump debugging is off
Radius protocol in brief format debugging is on
00:05:21: RADIUS: Initial Transmit ISDN 0:D:23 id 6 10.0.0.1:1824, Accounting-Request, len
358
00:05:21: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to 4085274206
00:05:26: RADIUS: Retransmit id 6
00:05:31: RADIUS: Tried all servers.
00:05:31: RADIUS: No valid server found. Trying any viable server
00:05:31: RADIUS: Tried all servers.
00:05:31: RADIUS: No response for id 7
00:05:31: RADIUS: Initial Transmit ISDN 0:D:23 id 8 10.0.0.0:1823, Access-Request, len 171
00:05:36: RADIUS: Retransmit id 8
00:05:36: RADIUS: Received from id 8 1.7.157.1:1823, Access-Accept, len 115
00:05:47: %ISDN-6-DISCONNECT: Interface Serial0:22 disconnected from 4085274206, call
lasted 26 seconds
00:05:47: RADIUS: Initial Transmit ISDN 0:D:23 id 9 10.0.0.1:1824, Accounting-Request, len
775
00:05:47: RADIUS: Received from id 9 1.7.157.1:1824, Accounting-response, len 20
```

The following example shows **debug radius hex** output:

```
Router# debug radius hex

Radius protocol debugging is on
Radius packet hex dump debugging is on
Router#
17:26:52: RADIUS: ustruct sharecount=3
17:26:52: Radius: radius_port_info() success=0 radius_nas_port=1
17:26:52: RADIUS: Initial Transmit ISDN 0:D:23 id 10 10.0.0.1:1824, Accounting-Request,
len 361
17:26:52:         Attribute 4 6 01081D03
17:26:52:         Attribute 26 19 00000009020D4953444E20303A443A3233
17:26:52:         Attribute 61 6 00000000
17:26:52:         Attribute 1 12 34303835323734323036
17:26:52:         Attribute 30 7 3532393831
17:26:52:         Attribute 31 12 34303835323734323036
17:26:52:         Attribute 40 6 00000001
17:26:52:         Attribute 6 6 00000001
```

```
17:26:52:         Attribute 26 27 0000000921156833323332D67772D69643D353330305F34332E
17:26:52:         Attribute 26 57
0000000901336833323332D696E636F6D696E672D636F6E662D69643D3846334133313633204234393830303046
203020334245373142 38
17:26:52:         Attribute 26 31
000000091A19683332332D63616C6C2D6F726967696E3D616E73776572
17:26:52:         Attribute 26 32
000000091B1A683332332D63616C6C2D747970653D54656C6570686F6E79
17:26:52:         Attribute 26 56
0000000919326833323332D73657475702D74696D653D2A30393A32363A35322E383830205053542053617420204A
616E20312032303030
17:26:52:         Attribute 26 48
00000009182A683332332D636F6E662D69643D3846334133313633204234393830303046203020334245373142
38
17:26:52:         Attribute 44 10 3030303030303035
17:26:52:         Attribute 41 6 00000000
17:26:52: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to 4085274206
17:26:52: RADIUS: Received from id 10 10.0.0.1:1824, Accounting-response, len 20
17:27:01: RADIUS: ustruct sharecount=3
17:27:01: Radius: radius_port_info() success=0 radius_nas_port=1
17:27:01: RADIUS: Initial Transmit ISDN 0:D:23 id 11 10.0.0.0:1823, Access-Request, len
173
17:27:01:         Attribute 4 6 01081D03
17:27:01:         Attribute 26 19 00000009020D4953444E20303A443A3233
17:27:01:         Attribute 61 6 00000000
17:27:01:         Attribute 1 8 313233343536
17:27:01:         Attribute 26 48
00000009182A683332332D636F6E662D69643D3846334133313633204234393830303046203020334245373142
38
17:27:01:         Attribute 31 12 34303835323734323036
17:27:01:         Attribute 2 18 C980D8D0E9A061B3D783C61AA6F27214
17:27:01:         Attribute 26 36
00000009011E683332332D6976722D6F75743D7472616E73616374696F6E49443A33
17:27:01: RADIUS: Received from id 11 1.7.157.1:1823, Access-Accept, len 115
17:27:01:         Attribute 6 6 00000001
17:27:01:         Attribute 26 29 0000000965176833323332D6372656469742D616D6F756E743D3435
17:27:01:         Attribute 26 27 000000096615683332332D6372656469742D74696D653D3333
17:27:01:         Attribute 26 26 00000009671468333233 32D72657475726E2D636F64653D30
17:27:01:         Attribute 25 7 6C6F63616C
17:27:01: RADIUS: saved authorization data for user 61AA0698 at 6215087C
17:27:09: %ISDN-6-DISCONNECT: Interface Serial0:22  disconnected from 4085554206, call
lasted 17 seconds
17:27:09: RADIUS: ustruct sharecount=2
17:27:09: Radius: radius_port_info() success=0 radius_nas_port=1
17:27:09: RADIUS: Sent class "local" at 621508E8 from user 61AA0698
17:27:09: RADIUS: Initial Transmit ISDN 0:D:23 id 12 1.7.157.1:1824, Accounting-Request,
len 776
17:27:09:         Attribute 4 6 01081D03
17:27:09:         Attribute 26 19 00000009020D4953444E20303A443A3233
17:27:09:         Attribute 61 6 00000000
17:27:09:         Attribute 1 8 313233343536
17:27:09:         Attribute 30 7 3532393831
17:27:09:         Attribute 31 12 34303835323734323036
17:27:09:         Attribute 40 6 00000002
17:27:09:         Attribute 25 7 6C6F63616C
17:27:09:         Attribute 45 6 00000001
17:27:09:         Attribute 6 6 00000001
17:27:09:         Attribute 26 27 0000000921156833323332D67772D69643D353330305F34332E
17:27:09:         Attribute 26 57
0000000901336833323332D696E636F6D696E672D636F6E662D69643D3846334133313633204234393830303046
203020334245373142 38
17:27:09:         Attribute 26 31
000000091A19683332332D63616C6C2D6F726967696E3D616E73776572
```

```
17:27:09:         Attribute 26 32
000000091B1A683332332D63616C6C2D747970653D54656C6570686F6E79
17:27:09:         Attribute 26 56
0000000919326833323332D73657475702D74696D653D2A30393A32363A35322E38383020505354205361742
616E20312032303030
17:27:09:         Attribute 26 58
000000091C34683332332D636F6E6E6563742D74696D653D2A30393A32363A35322E393037205053542053617
204A616E20312032303030
17:27:09:         Attribute 26 61
000000091D37683332332D646973636F6E6E6563742D74696D653D2A30393A32373A31302E3133372050535420
536174204A616E20312032303030
17:27:09:         Attribute 26 32
000000091E1A683332332D646973636F6E6E6563742D63617573653D3130
17:27:09:         Attribute 26 28 000000091F16683332332D766F6963652D7175616C6974793D30
17:27:09:         Attribute 26 48
00000009182A683332332D636F6E662D69643D3846334133313633204234393830303046203020334245373142
38
17:27:09:         Attribute 44 10 3030303030303035
17:27:09:         Attribute 42 6 00000000
17:27:09:         Attribute 43 6 00012CA0
17:27:09:         Attribute 47 6 00000000
17:27:09:         Attribute 48 6 000001E1
17:27:09:         Attribute 46 6 00000011
17:27:09:         Attribute 26 30 0000000901187375627363726962657 23D526567756C61724C696E65
17:27:09:         Attribute 26 35
00000009011D683332332D6976722D6F75743D5461726966663A556E6B6E6F776E
17:27:09:         Attribute 26 22 00000009011070726 52D62797465732D696E3D30
17:27:09:         Attribute 26 23 00000009011170726 52D62797465732D6F75743D30
17:27:09:         Attribute 26 21 00000009010F7072652D70616B732D696E3D30
17:27:09:         Attribute 26 22 00000009011070726 52D70616B732D6F75743D30
17:27:09:         Attribute 26 22 0000000901106E61732D72782D73706565643D30
17:27:09:         Attribute 26 22 0000000901106E61732D74782D73706565643D30
17:27:09:         Attribute 41 6 00000000
17:27:09: RADIUS: Received from id 12 10.0.0.1:1824, Accounting-response, len 20
```

Related Commands

Command	Description
debug aaa accounting	Displays information on accountable events as they occur.
debug aaa authentication	Displays information on AAA/TACACS+ authentication.

debug tacacs

To display information associated with TACACS, use the **debug tacacs** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug tacacs

no debug tacacs

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Usage Guidelines

TACACS is a distributed security system that secures networks against unauthorized access. Cisco supports TACACS under the authentication, authorization, and accounting (AAA) security system.

Use the **debug aaa authentication** command to get a high-level view of login activity. When TACACS is used on the router, you can use the **debug tacacs** command for more detailed debugging information.

Examples

The following is sample output from the **debug aaa authentication** command for a TACACS login attempt that was successful. The information indicates that TACACS+ is the authentication method used.

```
Router# debug aaa authentication

14:01:17: AAA/AUTHEN (567936829): Method=TACACS+
14:01:17: TAC+: send AUTHEN/CONT packet
14:01:17: TAC+ (567936829): received authen response status = PASS
14:01:17: AAA/AUTHEN (567936829): status = PASS
```

The following is sample output from the **debug tacacs** command for a TACACS login attempt that was successful, as indicated by the status PASS:

```
Router# debug tacacs

14:00:09: TAC+: Opening TCP/IP connection to 192.168.60.15 using source 10.116.0.79
14:00:09: TAC+: Sending TCP/IP packet number 383258052-1 to 192.168.60.15 (AUTHEN/START)
14:00:09: TAC+: Receiving TCP/IP packet number 383258052-2 from 192.168.60.15
14:00:09: TAC+ (383258052): received authen response status = GETUSER
14:00:10: TAC+: send AUTHEN/CONT packet
14:00:10: TAC+: Sending TCP/IP packet number 383258052-3 to 192.168.60.15 (AUTHEN/CONT)
14:00:10: TAC+: Receiving TCP/IP packet number 383258052-4 from 192.168.60.15
14:00:10: TAC+ (383258052): received authen response status = GETPASS
14:00:14: TAC+: send AUTHEN/CONT packet
14:00:14: TAC+: Sending TCP/IP packet number 383258052-5 to 192.168.60.15 (AUTHEN/CONT)
14:00:14: TAC+: Receiving TCP/IP packet number 383258052-6 from 192.168.60.15
14:00:14: TAC+ (383258052): received authen response status = PASS
14:00:14: TAC+: Closing TCP/IP connection to 192.168.60.15
```

The following is sample output from the **debug tacacs** command for a TACACS login attempt that was unsuccessful, as indicated by the status FAIL:

```
Router# debug tacacs

13:53:35: TAC+: Opening TCP/IP connection to 192.168.60.15 using source
192.48.0.79
13:53:35: TAC+: Sending TCP/IP packet number 416942312-1 to 192.168.60.15
(AUTHEN/START)
13:53:35: TAC+: Receiving TCP/IP packet number 416942312-2 from 192.168.60.15
13:53:35: TAC+ (416942312): received authen response status = GETUSER
13:53:37: TAC+: send AUTHEN/CONT packet
13:53:37: TAC+: Sending TCP/IP packet number 416942312-3 to 192.168.60.15
(AUTHEN/CONT)
13:53:37: TAC+: Receiving TCP/IP packet number 416942312-4 from 192.168.60.15
13:53:37: TAC+ (416942312): received authen response status = GETPASS
13:53:38: TAC+: send AUTHEN/CONT packet
13:53:38: TAC+: Sending TCP/IP packet number 416942312-5 to 192.168.60.15
(AUTHEN/CONT)
13:53:38: TAC+: Receiving TCP/IP packet number 416942312-6 from 192.168.60.15
13:53:38: TAC+ (416942312): received authen response status = FAIL
13:53:40: TAC+: Closing TCP/IP connection to 192.168.60.15
```

Related Commands

Command	Description
debug aaa accounting	Displays information on accountable events as they occur.
debug aaa authentication	Displays information on AAA/TACACS+ authentication.

ip mobile home-agent

To enable and control home agent (HA) services, use the **ip mobile home-agent** command in global configuration mode. To disable these services, use the **no** form of this command.

ip mobile home-agent [**address** *ip-address*] [**broadcast**] [**care-of-access** *access-list*] [**lifetime** *seconds*] [**nat-detect**] [**replay** *seconds*] [**reverse-tunnel** {**off** | **private-address**}] [**roam-access** *access-list*] [**strip-realm**] [**suppress-unreachable**] [**local-timezone**] [**unknown-ha** [**accept** [**reply**] | **deny**]] [**send-mn-address**]

no ip mobile home-agent [**address** *ip-address*] [**broadcast**] [**care-of-access** *access-list*] [**lifetime** *seconds*] [**nat-detect**] [**replay** *seconds*] [**reverse-tunnel** {**off** | **private-address**}] [**roam-access** *access-list*] [**strip-realm**] [**suppress-unreachable**] [**local-timezone**] [**unknown-ha** [**accept** [**reply**] | **deny**]] [**send-mn-address**]

Syntax Description

address *ip-address*	(Optional) Specifies the IP address of the HA. **Note** This option is only applicable when HA redundancy is used for virtual networks.
broadcast	(Optional) Enables forwarding of broadcast datagrams to the mobile node (MN). By default, broadcasting is disabled.
care-of-access *access-list*	(Optional) Controls which care-of addresses (CoAs) in registration requests are permitted by the HA. By default, all CoAs are permitted. The *access-list* argument can be a string or number from 1 to 99.
lifetime *seconds*	(Optional) Specifies the global registration lifetime for an MN in seconds. Range is from 3 to 65535 (infinity). Default is 36000 (10 hours). **Note** This configuration can be overridden by the individual MN configuration. Registrations requesting a lifetime greater than this value will still be accepted, but will use this lifetime value.
nat-detect	(Optional) Allows the HA to detect registration requests from a MN traversing a Network Address Translation (NAT)-enabled device and apply a tunnel to reach the MN. By default, NAT detection is disabled.
replay *seconds*	(Optional) Sets the replay protection time-stamp value in seconds. A registration received within the router clock time plus or minus 7 is valid.
reverse-tunnel {**off** | **private-address**}	(Optional) Enables support of reverse tunnel by the HA. By default, reverse tunnel support is enabled. The keywords are as follows: • **off**—Disables support of reverse tunnel. • **private-address**—Reverse tunnel mandatory for private Mobile IP addresses.
roam-access *access-list*	(Optional) Controls which MNs are permitted or denied to roam. By default, all specified MNs can roam.
strip-realm	(Optional) Strips the realm part of the Network access identifier (NAI) before authentication is performed. This option is useful if the majority of MNs have the identical realm, for example, in the case of enterprise networks.
suppress-unreachable	(Optional) Disables sending Internet Control Message Protocol (ICMP) unreachable messages to the source when an MN on the virtual network is not registered. By default, ICMP unreachable messages are sent.

local-timezone	(Optional) Uses the local time zone to generate identification fields.
unknown-ha [**accept** [**reply**] | **deny**]	Accepts or denies an unknown HA registration request. The keywords are as follows: • **accept**—(Optional) HA accepts the registration request with an HA address different from the IP destination of the registration request. The HA address set in the registration reply is that of the IP destination address. • **reply**—(Optional) HA uses the received HA address in reply. • **deny**—(Optional) HA denies the registration request with an HA address different from the IP destination of the registration request with error code Unknown HomeAgent. The HA address set in the reject registration reply is that of the IP destination address.  **Note** This command option can be used in a testing environment when the home agent is in private addressing space behind a NAT gateway.
send-mn-address	Sends the home address as received in the registration request and in the access request messages for the HA Challenge Handshake Authentication Protocol (CHAP). **Note** You must configure this keyword in the HA to send **radius-server vsa send authentication 3gpp2** attributes. This keyword is available only on PDSN platforms running specific PDSN code images.

Defaults

The command is disabled. Broadcasting is disabled. Reverse tunnel support is enabled. ICMP unreachable messages are sent. NAT detection is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The **strip-nai-realm** and **local-timezone** keywords were added.
12.2(13)T	The **nat-detect** keyword was added.
12.3(4)T	The **unknown-ha**, **accept**, **reply**, **deny** and **send-mn-address** keywords were added.

Usage Guidelines

This command enables and controls HA services on a router. Changes to service take effect immediately; however, broadcast and lifetime settings for previously registered MNs are unaffected. Tunnels are shared by MNs registered with the same endpoints, so the **reverse-tunnel-off** keyword also affects registered MNs.

The HA processes registration requests from the MN and sets up tunnels and routes to the CoA. Packets to the MN are forwarded to the visited network.

The HA will forward broadcast packets to MNs if the MNs are registered with the service. However, heavy broadcast traffic uses the CPU of the router.

The HA can control where the MNs roam by the **care-of-access** keyword, and which MN is allowed to roam by the **roam-access** keyword.

When a registration request comes in, the HA ignores requests when HA service is not enabled or the security association of the MN is not configured. The latter condition occurs because the security association must be available for the MH authentication extension in the reply. If a security association exists for the FA (IP source address or CoA in the request), the FA is authenticated, and then the MN is authenticated. The Identification field is verified to protect against replay attack. The HA checks the validity of the request (see Table 4) and sends a reply. (Reply codes are listed in Table 5.) A security violation is logged when FA authentication, MH authentication, or identification verification fails. (The violation reasons are listed in Table 6.)

After registration is accepted, the HA creates or updates the mobility binding of the MN, which contains the expiration timer. If no binding existed before this registration, a virtual tunnel is created, a host route to the MN via the care-of address is added to the routing table, and gratuitous ARPs are sent out. For deregistration, the host route is removed from the routing table, the virtual tunnel interface is removed (if no MNs are using it), and gratuitous ARP messages are sent out if the MN is back home. Mobility binding is removed (along with its associated host route and tunnel) when registration lifetime expires or deregistration is accepted.

By default, the HA uses the entire NAI string as the username for authentication (which may be with local security association or retrieved from the AAA server). The **strip-nai-realm** keyword instructs the HA to strip off the realm part of NAI (if it exists) before performing authentication. Basically, the MN is identified by only the user name part of the NAI. This option is useful if the majority of MNs belong to the same realm, for example, in the case of enterprise networks.

When the packet destined for the MN arrives on the HA, the HA encapsulates the packet and tunnels it to the care-of address. If the Don't Fragment (DF) bit is set in the packet via the **ip mobile tunnel path-mtu-discovery** global configuration command, the HA will copy the DF bit from the original packet to the new tunnel IP header. This allows the path MTU discovery to set the MTU of the tunnel. Subsequent packets greater than the MTU of the tunnel will be dropped and an ICMP datagram too big message will be sent to the source (correspondent node). If the HA loses the route to the tunnel endpoint, the host route to the MN will be removed from the routing table until the tunnel route is available. Packets destined for the MN without a host route will be sent out the interface (home network) or to the virtual network (see the description of the **suppress-unreachable** keyword). For subnet-directed broadcasts to the home link, the HA will send a copy to all MNs registered with the broadcast routing option.

Some companies block ICMP datagram too big messages. If the message does not reach the original correspondent node sending the packet, the correspondent node will simply resend the same size packet. To work around this problem, turn off Path MTU Discovery with the **no ip mobile tunnel path-mtu-discovery** command. The DF bit will not be copied from the original packet and the tunnel packet can be fragmented.

The **ip mobile home-agent nat-detect** option is supported for MNs using a collocated care-of address and registering through the FA. The MN will use the NAT inside address as the collocated care-of address used in its registration requests. If a MN is using a FA CoA address, the MN can be detected behind a NAT gateway.

The **ip mobile home-agent unknown-ha** option can be useful in a testing environment when the HA is using a private address behind a NAT gateway. A MN would need to access the HA through the NAT box while it is on a public network domain. However, NAT will translate the destination IP address of the

registration request to the private address of the HA. When the HA checks the HA field in the registration request, it does not match one of the interfaces. The packet can not be processed properly and the tunnels are not set up properly. The **ip mobile home-agent unknown-ha** command allows the HA to accept the unknown (translated) address and process the registration request.

The **send-mn-address** keyword is available only on PDSN platforms running specific PDSN code images; consult Feature Navigator for your Cisco IOS software release.

The MN requests services from the HA by setting bits in the registration request. Table 4 shows the services the MN can request.

Table 4 HA Registration Bitflags

Bit Set	Definition
S	Accept with code 1 (no simultaneous binding).
B	Accept. Broadcast can be enabled or disabled.
D	Accept. Tunnel endpoint is a colocated care-of address.
M	Deny. Minimum IP encapsulation is not supported.
G	Accept. GRE encapsulation is supported.
V	Deny if this bit is set.
T	Accept if the **reverse-tunnel-off** parameter is not set.
reserved	Deny. Reserved bit must not be set.

Table 5 lists the HA registration reply codes. The codes tell the MN whether the registration was accepted or denied. If registration is denied, the reply code gives the reason.

Table 5 HA Registration Reply Codes

Code	Reason
0	Accept.
1	Accept. No simultaneous bindings.
128	Reason unspecified.
129	Administratively prohibited.
130	Insufficient resource.
131	MN failed authentication.
132	FA failed authentication.
133	Registration identification mismatched (timestamp is off).
134	Poorly formed request.
136	Unknown HA address.
137	Reverse tunnel is unavailable.
138	Reverse tunnel is mandatory and T bit not set.
139	Unsupported encapsulation.
140	Unsupported vendor id or unable to interpret registration request extensions sent by the MN to the home agent.

Table 5 HA Registration Reply Codes (continued)

Code	Reason
141	Unsupported vendor id or unable to interpret registration request extensions sent by the FA to the home agent.
142	Active home agent failed authentication.

Table 6 lists security violation codes.

Table 6 Security Violation Codes

Code	Reason
1	No mobility security association.
2	Bad authenticator.
3	Bad identifier.
4	Bad SPI.
5	Missing security extension.
6	Other.
7	Stale request.

Examples

The following example enables broadcast routing and specifies a global registration lifetime of 7200 seconds (2 hours):

```
ip mobile home-agent broadcast lifetime 7200
```

Related Commands

Command	Description
ip mobile tunnel	Specifies the setting of tunnels created by Mobile IP.
show ip mobile binding	Displays the mobility binding table.
show ip mobile globals	Displays global information for mobile agents.

ip mobile home-agent accounting

To enable home agent accounting services on the router, use the **ip mobile home-agent accounting** command in global configuration mode. To disable these services, use the **no** form of this command.

ip mobile home-agent accounting {**default** | *list-name*}

no ip mobile home-agent accounting {**default** | *list-name*}

Syntax Description

default	Uses the listed accounting methods that follow this argument as the default list of methods for accounting services.
list-name	Character string used to name the list of at least one of the accounting methods.

Defaults

The command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

This command enables and controls home agent accounting services on the router. First, use the **aaa accounting** global configuration command to define the accounting method list. Next, apply the same accounting method list on the home agent using the **ip mobile home-agent accounting** global configuration command.

Examples

The following example enables home agent accounting for the list named mobile-list:

```
ip mobile home-agent accounting mobile-list
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.

ip mobile home-agent dynamic-address

To set the home agent address field in a Registration Response packet, use the **ip mobile home-agent dynamic-address** command in global configuration. To disable this functionality, or to reset the field use the **no** form of this command.

ip mobile home-agent dynamic-address *ip-address*

no ip mobile home-agent dynamic-address *ip-address*

Syntax Description

ip-address	The IP address of the Home Agent.

Defaults

The Home Agent Address field will be set to the values specified by the *ip-address* argument.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)YF	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Examples

In the following example, the dynamic home-agent address is set to 10.1.1.1:

```
Router# ip mobile home-agent dynamic-address 10.1.1.1
```

ip mobile home-agent redundancy

To configure the home agent for redundancy by using the Hot Standby Router Protocol (HSRP) group name, use the **ip mobile home-agent redundancy** command in global configuration mode. To remove the address, use the **no** form of this command.

ip mobile home-agent redundancy *hsrp-group-name* [[**virtual-network***]* **address** *address*] [**mode active-standby***]* [**swact-notification**]

no ip mobile home-agent redundancy *hsrp-group-name* [[**virtual-network**] **address** *address*] [**mode active-standby***]* [**swact-notification**]

Syntax Description

hsrp-group-name	Specifies the HSRP group name.
virtual-network	(Optional) Specifies that the HSRP group is used to support virtual networks.
address *address*	(Optional) Home agent address.
mode active-standby	(Optional) Allows the bindings to come up (with local pool addressing for virtual-networks) with the home agent IP address specified under the loopback interface.
swact-notification	(Optional) Notifies the RADIUS server of a home agent failover.

Defaults

No global home agent addresses are specified.

Command Modes

Global configuration

Command History

Release	Modification
12.0(2)T	This command was introduced.
12.2(8)T	The command changed from **ip mobile home-agent standby** to **ip mobile home-agent redundancy**.
12.4(11)T	The **mode active-standby** and **swact-notification** keywords were added.

Usage Guidelines

The **virtual-network** keyword specifies that the HSRP group supports virtual networks.

Note Redundant home agents must have identical Mobile IP configurations. You can use a standby group to provide HA redundancy for either physical or virtual networks, but not both at the same time.

When Mobile IP standby is configured, the home agent can request mobility bindings from the peer home agent. When Mobile IP standby is deconfigured, the home agent can remove mobility bindings. Operation of home agent redundancy on physical and virtual networks is described as follows:

- **Physical network**—Only the active home agent will receive registrations on a physical network. It updates the standby home agent. The standby home agent requests the mobility binding table from the active home agent. When Mobile IP standby is deconfigured, the standby home agent removes all bindings, but the active home agent keeps all bindings.
- **Virtual network**—Both active and standby home agents receive registrations if the loopback interface is used; each will update the peer after accepting a registration. Otherwise, the active home agent receives registrations. Both active and standby home agents request mobility binding tables from each other. When Mobile IP standby is deconfigured, the standby or active home agent removes all bindings.

Note The **swact-notification** option notifies the RADIUS server of a home agent failover. This is achieved by including the cisco-avpair radius attribute “mobileip-rfswat=1” in RADIUS accounting records. This attribute is included only in the first accounting record of a binding generated after a failover, and if that binding was created before the failover.

Examples

The following example specifies an HSRP group named SanJoseHA:

```
ip mobile home-agent redundancy SanJoseHA
```

Related Commands

Command	Description
show ip mobile globals	Displays global information for mobile agents.

ip mobile home-agent redundancy periodic-sync

To synchronize the byte and packet counters for each binding to the standby unit using an accounting update event, use the **ip mobile home-agent redundancy periodic-sync** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip mobile home-agent redundancy *hsrp-group-name* [[**virtual-network**] **address** *address*] **periodic-sync**

no ip mobile home-agent redundancy *hsrp-group-name* [[**virtual-network**] **address** *address*] **periodic-sync**

Syntax Description

hsrp-group-name	Specifies the HSRP group name.
virtual-network	(Optional) Specifies that the HSRP group is used to support virtual networks.
address *address*	(Optional) Home agent address.

Defaults

There are no default values for this command.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YX	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

The byte and packet counters for each binding are synchronized to the standby unit using an accounting update event only if the byte counts have changed since the last synchronization.

Examples

In the following example, the byte and packet counters for each binding will be periodically synchronized between the active and standby unit:

```
Router# ip mobile home-agent redundancy group1 periodic-sync
```

ip mobile home-agent reject-static-addr

To configure the HA to reject Registration Requests from MNs under certain conditions, use the **ip mobile home-agent reject-static-addr** sub-command under the **ip mobile home-agent** global configuration command.

ip mobile home-agent reject-static-addr

Syntax Description

This command has not arguments or keywords

Command Modes

Sub-command of the **ip mobile home-agent** global configuration command.

Command History

Release	Modification
12.2(8)BY	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

You must first configure the **ip mobile home-agent** command to use this sub-command.

If an MN that has a binding to the HA with a static address tries to register with the same static address again, then the HA rejects the second RRQ from the MN.

Examples

The following example illustrates the **ip mobile home-agent reject-static-addr** command:

```
Router# ip mobile home-agent reject-static-addr
```

ip mobile home-agent resync-sa

To configure the home agent to clear out the old cached security associations and requery the AAA server for a new security association when the mobile node fails authentication, use the **ip mobile home-agent resync-sa** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip mobile home-agent resync-sa *seconds*

no ip mobile home-agent resync-sa *seconds*

Syntax Description

seconds	Specifies the time in which the home agent will wait to initiate a resynchronization.

Defaults

This command is off by default. The normal behavior of the home agent is to never requery the AAA server for a new security association.

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

You must enable security association caching for the **ip mobile home-agent resync-sa** command to work. Use the **ip mobile host aaa load-sa** global configuration command to enable caching of security associations retrieved from a AAA server.

When a security association is downloaded for a mobile node from a AAA server, the security association is time stamped. If the mobile node fails reregistration and the time interval since the security association was cached is greater than *sec* seconds, the home agent will clear out the old security association and requery the AAA server. If the time period is less than the *sec* value, the home agent will not requery the AAA server for the security association of the mobile node.

The *sec* value represents the number of seconds the home agent will consider the downloaded security association synchronized with the AAA server. After that time period, it is considered old and can be replaced by a new security association from the AAA server.

This time-based resynchronization process helps prevent denial-of-service attacks on the AAA server and provides a way to synchronize the home agent's cached security association entry when a change to the security association for the mobile node is made at the AAA server and on the mobile node. By using this process, once the mobile node fails reregistration with the old cached security association, the home agent will clear the cache for that mobile node, and resynchronize with the AAA server.

Examples

In the following example, if a registration fails authentication, the home agent retrieves a new security association from the AAA server if the existing security association was downloaded more than 10 seconds ago:

```
ip mobile home-agent resync-sa 10
```

Related Commands

Command	Description
ip mobile host	Configures the mobile node or mobile host group.

ip mobile home-agent revocation

To enable support for MIPv4 registration revocation on the home agent, use the **ip mobile home-agent revocation** command in global configuration mode. To disable support for registration revocation, use the **no** form of the command.

ip mobile home-agent revocation [**timeout** *seconds*] [**retransmit** *retries*] [**timestamp msec**]

no ip mobile home-agent revocation [**timeout** *seconds*] [**retransmit** *retries*] [**timestamp msec**]

Syntax Description

timeout *seconds*	(Optional) Configures the time interval (in seconds) between retransmission of MIPv4 registration revocation message. The **no** version restores the time interval between retransmission of MIPv4 registration revocation Message to the default value. The default is 3 seconds. The range is from 1 to 100 seconds
retransmit *retries*	(Optional) Configures the number of times MIPv4 registration revocation messages are retransmitted. The **no** version of this command restores the retransmit number to the default value. The default is 3 retransmissions. The range is from 1 to 100 retransmissions.
timestamp msec	(Optional) Configures the units in which the timestamp value in the revocation support extension and revocation message should be encoded. By default the timestamp value will be sent as seconds. If the **msec** option is specified, the values will be encoded in milliseconds.

Command Default

The home agent does not support registration revocation.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)XJ	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Examples

In the following example, the MIPv4 registration message will be retransmitted a maximum of 5 times with a time interval of 4 seconds in between retransmissions:

```
Router(config)#ip mobile home-agent revocation timeout 4 retransmit 5
```

ip mobile home-agent template tunnel

To configure a home agent to use the template tunnel, use the **ip mobile home-agent template tunnel** command in global configuration. To disable the use of the template tunnel, use the **no** form of the command.

ip mobile home-agent template tunnel *interface-id* **address** *ha-address*

no ip mobile home-agent template tunnel *interface-id* **address** *ha-address*

Syntax Description

interface-id	Specifies the template tunnel interface ID from which to apply ACLs.
address ha-address	Specifies the home agent address. ACLs will be applied to tunnels with *ha-address* as the local end point.

Command Default

The home agent does not use a template tunnel.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XJW	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Examples

In the following example, the home agent is configured to use the template tunnel:

```
Router(config)# interface tunnel 10
!
Router(config)# ip mobile home-agent template tunnel 10 address 10.0.0.1
```

ip mobile host

To configure the mobile host or mobile node group, use the **ip mobile host** command in global configuration mode. To disable these services, use the **no** form of this command.

ip mobile host {*lower* [*upper*] | **nai** *string* [**static-address** {*addr1* [*addr2*] [*addr3*] [*addr4*] [*addr5*] | **local-pool** *name*}] [**address** {*addr* | **pool** {**local** *name* | **dhcp-proxy-client** [**dhcp-server** *addr*]}]} {**interface** *name* | **virtual-network** *network-address mask*} [**aaa** [**load-sa** [**permanent**]]] [**authorized-pool** *name*] [**skip-aaa-reauthentication**][**care-of-access** *access-list*] [**lifetime** *seconds*]

no ip mobile host {*lower* [*upper*] | **nai** *string* [**static-address** {*addr1* [*addr2*] [*addr3*] [*addr4*] [*addr5*] | **local-pool** *name*}] [**address** {*addr* | **pool** {**local** *name* | **dhcp-proxy-client** [**dhcp-server** *addr*]}]} {**interface** *name* | **virtual-network** *network-address mask*} [**aaa** [**load-sa** [**permanent**]]] [**authorized-pool** *name*] [**skip-aaa-reauthentication**] [**care-of-access** *access-list*] [**lifetime** *seconds*]

Syntax Description

lower [*upper*]	One or a range of mobile host or mobile node group IP addresses. The upper end of the range is optional.
nai *string*	Network access identifier. The NAI can be a unique identifier (username@realm) or a group identifier (@realm).
static-address	(Optional) Indicates that a static IP address is to be assigned to the flows on this NAI. This parameter is not valid if the NAI is a realm.
addr1, addr2, ...	(Optional) One to a maximum of five IP addresses to be assigned using the **static-address** keyword.
local-pool *name*	(Optional) Name of the local pool of addresses to use for assigning a static IP address to this NAI.
address	(Optional) Indicates that a dynamic IP address is to be assigned to the flows on this NAI.
addr	(Optional) IP address to be assigned using the **address** keyword.
pool	(Optional) Indicates that a pool of addresses is to be used in assigning a dynamic IP address.
local *name*	(Optional) The name of the local pool to use in assigning addresses.
dhcp-proxy-client	(Optional) Indicates that the DHCP request should be sent to a DHCP server on behalf of the mobile node.
dhcp-server *addr*	(Optional) IP address of the DHCP server.
interface *name*	When used with DHCP, specifies the gateway address from which the DHCP server should select the address.
virtual-network *network-address mask*	Indicates that the mobile station resides in the specified virtual network, which was created using the **ip mobile virtual-network** command.
aaa	(Optional) Retrieves security associations from a AAA (TACACS+ or RADIUS) server. Allows the home agent to download address configuration details from the AAA server.
load-sa	(Optional) Caches security associations after retrieval by loading the security association into RAM. See Table 8 for details on how security associations are cached for NAI hosts and non-NAI hosts.

permanent	(Optional) Caches security associations in memory after retrieval permanently. Use this optional keyword only for NAI hosts.
authorized-pool *name*	(Optional) Verifies the IP address assigned to the mobile node if it is within the pool specified by the *name* argument.
skip-aaa-reauthentication	(Optional) When configured, the home agent does not send an access request for authentication for mobile IP re-registration requests. When disabled, the home agent sends an access request for all Mobile IP registration requests.
care-of-access *access-list*	(Optional) Access list. This can be a named access list or standard access list. The range is from 1 to 99. Controls where mobile nodes roam—the acceptable care-of addresses.
lifetime *seconds*	(Optional) Lifetime (in seconds). The lifetime for each mobile node (group) can be set to override the global value. The range is from 3 to 65535 (infinite).

Defaults

No host is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The **nai** keyword and associated parameters were added.
12.2(13)T	The **permanent** keyword was added and the command was integrated into Cisco IOS Release 12.2(13)T.
12.3(4)T	The **authorized-pool** *and* **skip-aaa-reauthentication** keywords were added.

Usage Guidelines

This command configures the mobile host or mobile node group (ranging from *lower* address to *upper* address) to be supported by the home agent. These mobile nodes belong to the network on an interface or a virtual network (via the **ip mobile virtual-network** command). The security association for each mobile host must be configured using the **ip mobile secure** command or downloaded from a AAA server.

All hosts must have security associations for registration authentication. Mobile nodes can have more than one security association. The memory consumption calculations shown in Table 7 are based on the assumption of one security association per mobile node. Caching behavior of security associations differs between NAI and non-NAI hosts as described in Table 8.

The **nai** keyword allows you to specify a particular mobile node or range of mobile nodes. The mobile node can request a static IP address (**static-address** keyword), which is configured using the *addr1* variable (for a specific address) or the **local-pool** keyword (for an IP address from an address pool; the requested address must be in the pool). Or, the mobile node can request a dynamic address (**address** keyword), which is configured using the *addr* variable (for a specific address) or the **pool** keyword (for an IP address from a pool or DHCP server). If this command is used with the Packet Data Serving Node (PDSN) proxy Mobile IP feature and a realm is specified in the **ip mobile proxy-host nai** command, then only a pool of addresses can be specified in this command.

The address pool can be defined by a local pool or by use of a DHCP proxy client. For DHCP, the **interface** *name* keyword and argument combination specifies the gateway address from which the DHCP server should select the address and the **dhcp-server** keyword specifies the DHCP server address. The NAI is sent in the client-id option of the DHCP packet and can be used to provide dynamic DNS services.

You can also use this command to configure the static IP address or address pool for multiple flows with the same NAI. A flow is a set of {NAI, IP address}.

Security associations can be stored by using one of three methods:

- On the router
- On the AAA server, retrieve security association each time registration comes in (**aaa** optional keyword)
- On the AAA server, retrieve and cache security association (**aaa load-sa** option)

Each method has advantages and disadvantages, which are described in Table 7.

Table 7 Methods for Storing Security Associations

Storage Method	Advantage	Disadvantage
On the router	• Security association is in router memory, resulting in fast lookup. • For home agents supporting fewer than 1500 mobile nodes, this provides optimum authentication performance and security (keys never leave router).	• NVRAM of router is limited, cannot store many security associations. Each security association configuration takes about 80 bytes. For 125 KB NVRAM, you can store about 1500 security associations on a home agent.
On the AAA server, retrieve security association each time registration comes in	• Central administration and storage of security association on AAA server. • If keys change constantly, administration is simplified to one server, latest keys always retrieved during registration. • Router memory (DRAM) is conserved. Router will need memory only to load in a security association, and then release the memory when done.	• Requires network to retrieve security association, slower than other storage methods, and dependent on network and server performance. • Multiple home agents that use one AAA server, which can become the bottleneck, can get slow response. • Key can be snooped if packets used to retrieve from AAA are not encrypted (for example, using RADIUS or unencrypted TACACS+ mode).

Table 7 Methods for Storing Security Associations (continued)

Storage Method	Advantage	Disadvantage
On the AAA server, retrieve and store security association	• AAA acts as an offload configuration server, security associations are loaded into router DRAM, which is more abundant (for example, 16 MB, 32 MB, 64 MB) when the first registration comes in. Each security association takes only about 50 bytes of DRAM, so 10,000 mobile nodes will use up 0.5 MB. • If keys remain fairly constant, once security associations are loaded, home agent authenticates as fast as when stored on the router. • Only security associations that are needed are loaded into router memory. Mobile nodes that never register will not waste memory.	• If keys change on the AAA server after the mobile node registered, then you need to use **clear ip mobile secure** command to clear and load in new security association from AAA, otherwise the security association of the router is stale.

The caching behavior of security associations for NAI hosts and non-NAI hosts is described in Table 8.

Table 8 Caching Behavior for Security Associations

Keyword Option	NAI Hosts	Non-NAI Hosts
aaa	Security associations are deleted after authentication and are not cached.	Security associations are deleted after authentication and are not cached.
aaa load-sa	The security association is cached while the mobile node is registered. If the mobile node's registration is deleted, the security association is removed.	Security associations are cached permanently.
aaa load-sa permanent	Security associations are cached permanently after being retrieved from the AAA server.	—

Note On the Mobile Wireless Home Agent, the following conditions apply:

If the **aaa load-sa** option is configured, the Home Agent caches the SA locally on first registration. In this case the Home Agent will not invoke the RADIUS authorization procedure for re-registration.

If **aaa load-sa skip-aaa-reauthentication** is configured, the Home Agent caches the SA locally on first registration; however, the Home Agent will not invoke HA-CHAP procedure for re-registration.

The **aaa load-sa permanent** option is not supported on the Mobile Wireless Home Agent, and should not be configured.

Examples

The following example configures a mobile node group to reside on virtual network 20.0.0.0 and retrieve mobile node security associations from a AAA server every time the mobile node registers:

```
ip mobile host 20.0.0.1 20.0.0.3 virtual-network 20.0.0.0 aaa
```

The following example configures a mobile node group to reside on virtual network 10.99.1.0 and retrieve and cache mobile node security associations from a AAA server. The cached security association is then used for subsequent registrations.

```
ip mobile host 10.99.1.1 10.99.1.100 virtual-network 10.99.1.0 aaa load-sa
```

The following example configures a local pool of dynamic addresses to be used in assigning IP addresses to mobile nodes in the cisco.com domain:

```
ip mobile host nai @cisco.com address pool local mobilenodes virtual-network 9.0.0.0
255.0.0.0 aaa lifetime 180
```

The following example configures a local pool of dynamic addresses to be used in assigning IP addresses to mobile nodes in the cisco.com domain. The security associations that are retrieved from the AAA server are cached as long as the binding is present and are deleted on the home agent when the binding is removed (due to manual clearing of the binding or lifetime expiration).

```
ip mobile host nai @cisco.com address pool local mobilenodes virtual-network 10.2.0.0
255.255.0.0 aaa load-sa lifetime 180
```

The following example configures a local pool of static addresses to be used in assigning IP addresses to mobile nodes in the cisco.com domain:

```
ip mobile host nai @cisco.com static-address local-pool mobilenodes
```

The following example configures a local pool of dynamic addresses to be used in assigning IP addresses to mobile nodes in the cisco.com domain. The security associations that are retrieved from the AAA server are cached permanently until cleared manually.

```
ip mobile host nai @cisco.com address pool local mobilenodes virtual network 10.2.0.0
255.255.0.0 aaa load-sa permanent lifetime 180
```

The following example configures the DHCP proxy client to use a DHCP server located at 10.1.2.3 to allocate a dynamic home address:

```
ip mobile host nai @dhcppool.com address pool dhcp-proxy-client dhcp-server 10.1.2.3
interface FastEthernet 0/0
```

Related Commands

Command	Description
aaa authorization ipmobile	Authorizes Mobile IP to retrieve security associations from the AAA server using TACACS+ or RADIUS.
clear ip mobile secure	Clears and retrieves remote security associations.
ip mobile proxy-host	Locally configures the proxy Mobile IP attributes
ip mobile secure	Specifies the mobility security associations for mobile host, visitor, home agent, and foreign agent.
show ip mobile host	Displays mobile node counters and information.

ip mobile radius disconnect

To enable the home agent to process Radius Disconnect messages, use the **ip mobile radius disconnect** command in global configuration mode. To disable the processing of Radius Disconnect messages on the home agent, use the **no** form of this command.

ip mobile radius disconnect

no ip mobile radius disconnect

Syntax Description

This command has no arguments or keywords.

Command Default

Radius Disconnect messages are not processed by the home agent.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)XJ	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

In order for packet of disconnect (POD) requests to be processed by AAA, you need to configure the **aaa server radius dynamic-author** global configuration command.

You must configure **radius-server attribute 32 include-in-access-req** for the home agent to send the fully qualified domain name (FQDN) in the access request.

Examples

The following example enables the home agent to process Radius Disconnect messages:

```
Router(config)# ip mobile radius disconnect
```

ip mobile realm

To enable inbound user sessions to be disconnected when specific session attributes are presented, use the **ip mobile realm** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip mobile realm @xyz.com **vrf** vrf-name **ha-addr** ip-address [**aaa-group** [**accounting** aaa-acct-group | **authentication** aaa-auth-group]] [**dns dynamic-update method** word] [**dns server** primary dns server address secondary dns server address [**assign**]] [**hotline**]

no ip mobile realm ip mobile realm *@xyz.com* **vrf** *vrf-name* **ha-addr** *ip-address* [**aaa-group** [**accounting** *aaa-acct-group*] [**dns dynamic-update method** *word*] [**dns server** *primary dns server address secondary dns server address* [**assign**]] [**hotline**]

Syntax Description

realm	Name of the specified realm.
vrf *vrf name*	Enables VRF support for a specific group.
ha-addr *ip-address*	IP address of the Home Agent.
aaa-group	(Optional) Denotes a AAA group.
accounting *aaa-acct-group*	(Optional) Specifies a AAA accounting group.
authentication *aaa-auth-group*	(Optional) Specifies a AAA authentication group.
dns dynamic-update method *word*	(Optional) Enables the DNS Update procedure for the specified realm. *word* is the dynamic DNS update method name.
dns server *primary dns server address secondary dns server address*	(Optional) Enables you to locally configure the DNS Server address.
assign	(Optional) Enables this feature for the specified realm.
hotline	(Optional) Enables Hotlining of the mobile hosts.

Defaults

There are no default values for this command.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)XJ.	This command was introduced.
12.3(14)YX	The dns server assign, and dns dynamic-update method variables were introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

This CLI defines the VRF for the domain "@xyz.com". The IP address of the Home Agent corresponding to the VRF is also defined, at which the MOIP tunnel will terminate. The IP address of the Home Agent should be a routable IP address on the box. Optionally, the AAA accounting and/or authentication server groups can be defined per VRF. If a AAA accounting server group is defined, all accounting records for the users of the realm will be sent to the specified group. If a AAA authentication server group is defined, HA-CHAP is sent to the server(s) defined in the group.

Examples

The following example identifies the DNS **dynamic update** keyword:

```
router(config)#ip mobile realm @ispxyz1.com dns ?
dynamic-update Enable 3GPP2 IP reachability
server DNS server configuration
```

The following example identifies the **hotlining** and **vrf** keywords:

```
router(config)# ip mobile realm @ispxyz1.com ?
dns Configure DNS details
hotline Hotlining of the mobile hosts
vrf VRF for the realm
```

ip mobile secure

To specify the mobility security associations for the mobile host, visitor, home agent, foreign agent, and proxy-host, use the **ip mobile secure** command in global configuration mode. To remove the mobility security associations, use the **no** form of this command.

ip mobile secure {**aaa-download** | **host** | **visitor** | **home-agent** | **foreign-agent** | **proxy-host**} {*lower-address [upper-address]* | **nai** *string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key hex** *string* [**replay timestamp** [*number*] **algorithm** {**md5** | **hmac-md5**} **mode prefix-suffix**]

no ip mobile secure {**aaa-download** | **host** | **visitor** | **home-agent** | **foreign-agent** | **proxy-host**} {*lower-address [upper-address]* | **nai** *string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key hex** *string* [**replay timestamp** [*number*] **algorithm** {**md5** | **hmac-md5**} **mode prefix-suffix**]

Syntax Description

aaa-download	Downloads security association from AAA at every timer interval.
host	Security association of the mobile host on the home agent.
visitor	Security association of the mobile host on the foreign agent.
home-agent	Security association of the remote home agent on the foreign agent.
foreign-agent	Security association of the remote foreign agent on the home agent.
proxy-host	Security association of the proxy Mobile IP users. This keyword is only available on Packet Data Serving Node (PDSN) platforms.
lower-address	IP address of a host or lower range of IP address pool.
upper-address	(Optional) Upper range of an IP address pool. If specified, security associations for multiple hosts are configured. The value used in the *upper-address* argument must be greater than that used in the *lower-address* argument.
nai *string*	Network access identifier of the mobile node. The **nai** *string* is valid only for a host, visitor, and proxy host.
inbound-spi *spi-in*	Security parameter index used for authenticating inbound registration packets. Range is from 0x100 to 0xffffffff.
outbound-spi *spi-out*	Security parameter index used for calculating the authenticator in outbound registration packets. Range is from 0x100 to 0xffffffff.
spi *spi*	Bidirectional SPI. Range is from 0x100 to 0xffffffff.
key hex *string*	ASCII string of hexadecimal values. No spaces are allowed.
replay	(Optional) Specifies replay protection used on registration packets.
timestamp	(Optional) Validates incoming packets to ensure that they are not being "replayed" by a spoofer using the timestamp method.
number	(Optional) Number of seconds. Registration is valid if received within the router's clock +/- 7 seconds. This means the sender and receiver are in time synchronization (NTP can be used).
algorithm	(Optional) Algorithm used to authenticate messages during registration.
md5	(Optional) Message Digest 5.
hmac-md5	(Optional) Hash-based message authentication code (HMAC) message digest 5.

mode	(Optional) Mode used to authenticate during registration.
prefix-suffix	(Optional) The key is used to wrap the registration information for authentication (for example, key registration information key) to calculate the message digest.

Defaults

No security association is specified.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2	The *lower-address* and *upper-address* arguments were added.
12.2(2)XC	The **nai** keyword was added.
12.2(13)T	The **hmac-md5** keyword was added and this command was integrated into Cisco IOS Release 12.2(13)T.
12.3(4)T	The **proxy-host** keyword was added for PDSN platforms.

Usage Guidelines

The security association consists of the entity address, SPI, key, replay protection method, authentication algorithm, and mode.

The SPI is the 4-byte index that selects the specific security parameters to be used to authenticate the peer. The security parameters consist of the authentication algorithm and mode, replay attack protection method, timeout, and IP address.

The HMAC-MD5 authentication algorithm is mandatory for mobile-home authentication (MHAE), mobile-foreign authentication (MFAE), and foreign-home authentication (FHAE)

On a home agent, the security association of the mobile host is mandatory for mobile host authentication. If desired, configure a foreign agent security association on your home agent. On a foreign agent, the security association of the visiting mobile host and security association of the home agent are optional. Multiple security associations for each entity can be configured.

If registration fails because the **timestamp** value is out of bounds, the time stamp of the home agent is returned so that the mobile node can reregister with the time-stamp value closer to that of the home agent, if desired.

The **nai** keyword is valid only for a host, visitor, and proxy host.

The **proxy-host** keyword is available only on PDSN platforms running specific PDSN code images; consult Feature Navigator for your Cisco IOS software release.

Note NTP is not required for operation but NTP can be used to synchronize time for all parties.

Examples

The following example shows mobile node 10.0.0.4, which has a key that is generated by the MD5 hash of the string:

```
ip mobile secure host 10.0.0.4 spi 100 key hex 12345678123456781234567812345678
```

Related Commands

Command	Description
ip mobile host	Configures the mobile host or mobile node group.
ip mobile proxy-host	Configures the proxy Mobile IP attributes.
ntp server	Allows the system clock to be synchronized by a time server.
show ip mobile secure	Displays the mobility security associations for mobile host, mobile visitor, foreign agent, or home agent.

ip mobile tunnel

To specify the settings of tunnels created by Mobile IP, use the **ip mobile tunnel** command in global configuration mode. To disable the setting of tunnels created by Mobile IP, use the **no** form of this command.

ip mobile tunnel {**crypto map** *map-name* | **route-cache** [**cef**] | **path-mtu-discovery** [**age-timer** {*minutes* | **infinite**}] | **nat** {**inside** | **outside**} | **route-map** *map-tag*}

no ip mobile tunnel {**crypto map** *map-name* | **route-cache** [**cef**] | **path-mtu-discovery** [**age-timer** {*minutes* | **infinite**}] | **nat** {**inside** | **outside**} | **route-map** *map-tag*}

Syntax DescriptionI

crypto map	Enables encryption or decryption on new tunnels. This keyword is only available on platforms running specific Packet Data Serving Node (PDSN) code images.
map-name	The name of the crypto map. This argument is available only on platforms running specific PDSN code images.
route-cache	Sets tunnels to fast-switching mode.
cef	Sets tunnels to Cisco Express Forwarding (CEF) switching mode if CEF is enabled on the router.
path-mtu-discovery	Specifies when the tunnel MTU should expire if set by Path MTU Discovery.
age-timer *minutes*	(Optional) Time interval in minutes after which the tunnel reestimates the path MTU.
infinite	(Optional) Turns off the age timer.
nat	Applies Network Address Translation (NAT) on the tunnel interface.
inside	Sets the dynamic tunnel as the inside interface for NAT.
outside	Sets the dynamic tunnel as the outside interface for NAT.
route-map *map-tag*	Defines a meaningful name for the route map.

Defaults

Disabled.

If enabled, default value for the *minutes* argument is 10 minutes.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.1(1)T	The **nat**, **inside**, and **outside** keywords were added.
12.2T	The **cef** keyword was added.
12.2(13)T	The **route-map** keyword and *map-tag* argument were added.
12.3(4)T	The **crpto map** keyword and *map-name* argument were added for PDSN platforms.

Usage Guidelines

Path MTU Discovery is used by end stations to find a packet size that does not need to be fragmented when being sent between the end stations. Tunnels must adjust their MTU to the smallest MTU interior to achieve this condition, as described in RFC 2003.

The discovered tunnel MTU should be aged out periodically to possibly recover from a case where suboptimum MTU existed at time of discovery. It is reset to the outgoing MTU of the interface.

The **no ip mobile tunnel route-cache** command disables fast switching and CEF switching (if CEF is enabled) on Mobile IP tunnels. The **no ip mobile tunnel route-cache cef** command disables CEF switching only.

CEF switching is currently not supported on a foreign agent when reverse tunneling is enabled. If reverse tunneling is enabled at the foreign agent, disable CEF on the foreign agent using the **no ip cef** global configuration command. If the foreign agent does not support reverse tunneling, there is no need to disable CEF at the global configuration level.

The **crypto map** *map-name* keyword and argument combination are available only on platforms running specific PDSN code images; consult Feature Navigator for your Cisco IOS software release.

Examples

The following example sets the discovered tunnel MTU to expire in 10 minutes (600 seconds):

```
ip mobile tunnel path-mtu-discovery age-timer 600
```

Related Commands

Command	Description
ip cef	Enables CEF on the RP card.
show ip mobile tunnel	Displays active tunnels.

ip mobile virtual-network

To define a virtual network, use the **ip mobile virtual-network** command in global configuration mode. To remove the virtual network, use the **no** form of this command.

ip mobile virtual-network *net mask* [**address** *address*]

no ip mobile virtual-network *net mask*

Syntax Description

net	Network associated with the IP address of the virtual network.
mask	Mask associated with the IP address of the virtual network.
address address	(Optional) IP address of a home agent on a virtual network.

Defaults

No home agent addresses are specified.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.0(2)T	The **address** keyword and *address* argument were added.

Usage Guidelines

This command inserts the virtual network into the routing table to allow mobile nodes to use the virtual network as their home network. The network is propagated when redistributed to other routing protocols.

Note You may need to include virtual networks when configuring the routing protocols. If this is the case, use the **redistribute mobile** router configuration command to redistribute routes from one routing domain to another.

Examples

The following example adds the virtual network 20.0.0.0 to the routing table and specifies that the home agent IP address is configured on the loopback interface for that virtual network:

```
interface ethernet 0
 ip address 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA

interface loopback 0
 ip address 20.0.0.1 255.255.255.255

ip mobile home-agent
 ip mobile virtual-network 20.0.0.0 255.255.0.0 address 20.0.0.1
 ip mobile home-agent standby SanJoseHA virtual-network
 ip mobile secure home-agent 1.0.0.2 spi 100 hex 00112233445566778899001122334455
```

Related Commands

Command	Description
ip mobile host	Configures the mobile host or mobile node group.
redistribute mobile	Redistributes routes from one routing domain into another routing domain.

radius-server attribute 32 include-in-access-req

To send RADIUS attribute 32 (NAS-Identifier) in an access-request or accounting-request, use the **radius-server attribute 32 include-in-access-req** command in global configuration mode. To disable sending RADIUS attribute 32, use the **no** form of this command.

radius-server attribute 32 include-in-access-req [*format*]

no radius-server attribute 32 include-in-access-req

Syntax Description

format	(Optional) A string sent in attribute 32 containing an IP address (%i), a hostname (%h), or a domain name (%d).

Defaults

RADIUS attribute 32 is not sent in access-request or accounting-request packets.

Command Modes

Global configuration

Command History

Release	Modification
12.1 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Using the **radius-server attribute 32 include-in-access-req** command makes it possible to identify the network access server (NAS) manufacturer to the RADIUS server by sending RADIUS attribute 32 (NAS-Identifier) in an access-request or accounting-request. If you configure the format argument, the string sent in attribute 32 will include an IP address, a hostname, or a domain name; otherwise, the Fully Qualified Domain Name (FQDN) is sent by default.

Examples

The following example shows a configuration that sends RADIUS attribute 32 in the access-request with the format configured to identify a Cisco NAS:

```
radius-server attribute 32 include-in-access-req format cisco %h.%d %i
! The following string will be sent in attribute 32 (NAS-Identifier).
"cisco router.nlab.cisco.com 10.0.1.67"
```

radius-server host

To specify a RADIUS server host, use the **radius-server host** command in global configuration mode. To delete the specified RADIUS host, use the **no** form of this command.

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*]

no radius-server host {*hostname* | *ip-address*}

Syntax Description

hostname	Domain Name System (DNS) name of the RADIUS server host.
ip-address	IP address of the RADIUS server host.
test username	(Optional) Turns on the automated testing feature for RADIUS server load balancing.
user-name	(Optional) Test user ID username. • Must be used if the **test username** keyword is used. **Caution** It is recommended that a test user, one that is not defined on the RADIUS server, be used for RADIUS server automated testing to protect against security issues that may arise if the test user is not correctly configured.
auth-port	(Optional) Specifies the UDP destination port for authentication requests.
port-number	(Optional) Port number for authentication requests; the host is not used for authentication if set to 0. If unspecified, the port number defaults to 1645.
ignore-auth-port	(Optional) Turns off the automated testing feature for RADIUS server load balancing on the authentication port.
acct-port	(Optional) Specifies the UDP destination port for accounting requests.
port-number	(Optional) Port number for accounting requests; the host is not used for accounting if set to 0. If unspecified, the port number defaults to 1646.
ignore-acct-port	(Optional) Turns off the automated testing feature for RADIUS server load balancing on the accounting port.
timeout	(Optional) The time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the **radius-server timeout** command. If no timeout value is specified, the global value is used. Enter a value in the range 1 to 1000.
seconds	(Optional) Specifies the **timeout** value. Enter a value in the range 1 to 1000. If no **timeout** value is specified, the global value is used.
retransmit	(Optional) The number of times a RADIUS request is re-sent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the **radius-server retransmit** command.
retries	(Optional) Specifies the retransmit value. Enter a value in the range 1 to 100. If no retransmit value is specified, the global value is used.

key	(Optional) Specifies the authentication and encryption key used between the router and the RADIUS daemon running on this RADIUS server. This key overrides the global setting of the **radius-server key** command. If no key string is specified, the global value is used. The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command syntax. This is because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
string	(Optional) Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS server. This key must match the encryption used on the RADIUS daemon. All 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.
alias	(Optional) Allows up to eight aliases per line for any given RADIUS server.
idle-time	(Optional) Specifies the time the server remains idle before it is quarantined and test packets are sent out.
seconds	(Optional) Length of idle time. • Default is 3600 seconds (1 hour). The valid range is 1–35791 seconds.

Defaults

No RADIUS host is specified; use global **radius-server** command values.

RADIUS server load balancing automated testing is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.0(5)T	This command was modified to add options for configuring timeout, retransmission, and key values per RADIUS server.
12.1(3)T	The **alias** keyword was added on the Cisco AS5300 and AS5800 universal access servers.
12.2(28)SB	The following keywords and arguments were added for configuring RADIUS server load balancing automated testing functionality: **test username** *user-name*, **ignore-auth-port**, **ignore-acct-port**, and **idle-time** *seconds*.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can use multiple **radius-server host** commands to specify multiple hosts. The software searches for hosts in the order in which you specify them.

If no host-specific timeout, retransmit, or key values are specified, the global values apply to each host.

RADIUS Server Automated Testing

When using the **radius-server host** command to enable automated testing for RADIUS server load balancing:

The authentication port is checked by default. If not specified, the default port of 1645 is used. If you wish to not check the authentication port, the **ignore-auth-port** keyword must be specified.

The accounting port is checked by default. If not specified, the default port of 1645 is used. If you wish to not check the accounting port, the **ignore-acct-port** keyword must be specified.

Examples

The following example specifies *host1* as the RADIUS server and uses default ports for both accounting and authentication:

```
radius-server host host1
```

The following example specifies port 1612 as the destination port for authentication requests and port 1616 as the destination port for accounting requests on the RADIUS host named host1:

```
radius-server host host1 auth-port 1612 acct-port 1616
```

Because entering a line resets all the port numbers, you must specify a host and configure accounting and authentication ports on a single line.

The following example specifies the host with IP address 192.0.2.46 as the RADIUS server, uses ports 1612 and 1616 as the authorization and accounting ports, sets the timeout value to 6, sets the retransmit value to 5, and sets “rad123” as the encryption key, matching the key on the RADIUS server:

```
radius-server host 192.0.2.46 auth-port 1612 acct-port 1616 timeout 6 retransmit 5 key
rad123
```

To use separate servers for accounting and authentication, use the zero port value as appropriate.

The following example specifies that RADIUS server host1 be used for accounting but not for authentication, and that RADIUS server host2 be used for authentication but not for accounting:

```
radius-server host host1.example.com auth-port 0
radius-server host host2.example.com acct-port 0
```

The following example specifies four aliases on the RADIUS server with IP address 192.0.2.1:

```
radius-server host 192.0.2.1 acct-port 1645 auth-port 1646
radius-server host 192.0.2.1 alias 192.0.2.2 192.0.2.3 192.0.2.4
```

The following example shows how to enable RADIUS server automated testing for load balancing with the authorization and accounting ports specified:

```
radius-server host 192.0.2.176 test username test1 auth-port 1645 acct-port 1646
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication ppp	Specifies one or more AAA authentication method for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict network access to a user.
debug aaa test	Shows when the idle-timer or dead-timer has expired for RADIUS server load balancing.
load-balance	Enables RADIUS server load balancing for named RADIUS server groups.
ppp	Starts an asynchronous connection using PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server load-balance	Enables RADIUS server load balancing for the global RADIUS server group.
radius-server retransmit	Specifies how many times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Sets the interval a router waits for a server host to reply.
test aaa group	Tests RADIUS load balancing server response manually.
username	Establishes a username-based authentication system, such as PPP CHAP and PAP.

router mobile

To enable Mobile IP on the router, use the **router mobile** command in global configuration mode. To disable Mobile IP, use the **no** form of this command.

router mobile

no router mobile

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.

Usage Guidelines

This command must be used in order to run Mobile IP on the router, as either a home agent or a foreign agent. The process is started, and counters begin. Disabling Mobile IP removes all related configuration commands, both global and interface.

Examples

The following example enables Mobile IP:

```
router mobile
```

Related Commands

Command	Description
show ip mobile globals	Displays global information for mobile agents.
show ip protocols	Displays the parameters and current state of the active routing protocol process.
show processes	Displays information about the active processes.

show ip mobile binding

To display the mobility binding table on the home agent (HA), use the **show ip mobile binding** command in privileged EXEC mode.

show ip mobile binding [**home-agent** *ip-address* | **nai** *string* [**session-id** *string*] | **summary**]

Syntax Description

home-agent	(Optional) Mobility bindings for a specific home agent (HA).
ip-address	(Optional) IP address for the HA.
nai *string*	(Optional) Mobile node (MN) identified by the network access identifier (NAI).
session-id *string*	(Optional) Session identifier. The *string* argument must be fewer than 25 characters in length.
summary	(Optional) Total number of bindings in the table.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.0(2)T	The **home-agent** keyword and *ip-address* argument were added.
12.1(2)T	The **summary** keyword was added.
12.2(2)XC	The **nai** keyword was added.
12.2(13)T	This command was enhanced to display the service options field and to include information about the mobile networks registered on the home agent.
12.3(4)T	The **session-id** keyword was added.
12.3(8)T	The output was enhanced to display UDP tunneling information.
12.4(9)T	The output was enhanced to display multipath support.

Usage Guidelines

You can display a list of all bindings if you press enter. You can also specify an IP address for a specific home agent using the **show ip mobile binding home-agent** *ip-address* command.

If the **session-id** *string* combination is specified, only the binding entry for that session identifier is displayed. A session identifier is used to uniquely identify a Mobile IP flow. A Mobile IP flow is the set of {NAI, IP address}. The flow allows a single NAI to be associated with one or multiple IP addresses, for example, {NAI, ipaddr1}, {NAI, ipaddr2}, and so on. A single user can have multiple sessions for example, when logging through different devices such as a PDA, cellular phone, or laptop. If the session identifier is present in the initial registration, it must be present in all subsequent registration renewals from that MN.

Examples

The following is sample output from the **show ip mobile binding** command:

```
Router# show ip mobile binding

Mobility Binding List:
```

```
Total 1
10.0.0.1:
 Care-of Addr 10.0.0.31, Src Addr 10.0.0.31,
 Lifetime granted 02:46:40 (10000), remaining 02:46:32
 Flags SbdmGvt, Identification B750FAC4.C28F56A8,
 Tunnel100 src 10.0.0.5 dest 10.0.0.31 reverse-allowed
 Routing Options - (G)GRE
  Service Options:
  NAT detect
```

The following is sample output from the **show ip mobile binding** command when mobile networks are configured or registered on the home agent:

```
Router# show ip mobile binding

Mobility Binding List:
Total 1
10.0.4.1:
 Care-of Addr 10.0.0.5, Src Addr 10.0.0.5
 Lifetime granted 00:02:00 (120), remaining 00:01:56
 Flags sbDmgvT, Identification B7A262C5.DE43E6F4
 Tunnel0 src 10.0.0.3 dest 10.0.0.5 reverse-allowed
 MR Tunnel1 src 10.0.0.3 dest 10.0.4.1 reverse-allowed
 Routing Options - (D)Direct-to-MN (T)Reverse-tunnel
 Mobile Networks: 10.0.0.0/255.255.255.0(S)
  10.0.0.0/255.255.255.0 (D)
  10.0.0.0/255.0.0.0(D)
```

The following is sample output from the **show ip mobile binding** command with session identifier information:

```
Router# show ip mobile binding

Mobility Binding List:
Total 1
 10.100.100.19:
 Care-of Addr 10.70.70.2, Src Addr 10.100.100.1,
 Lifetime granted 00:33:20 (20000), remaining 00:30:56
 Flags SbdmGvt, Identification BC1C2A04.EA42659C,
 Tunnel0 src 10.100.100.100 dest 10.70.70.2 reverse-allowed
 Routing Options
 Session identifier 998811234
 SPI 333 (decimal 819) MD5, Prefix-suffix, Timestamp +/-255, root key
 Key 38a38987ad0a399cb80940835689da66
 SPI 334 (decimal 820) MD5, Prefix-suffix, Timestamp +/-255, session key
 Key 34c7635a313038611dec8c16681b55e0
```

The following sample output shows that the home agent is configured to detect network address translation (NAT):

```
Router# show ip mobile binding nai mn@cisco.com

Mobility Binding List:

 mn@cisco.com (Bindings 1):
 Home Addr 10.99.101.1
 Care-of Addr 192.168.1.202, Src Addr 192.168.157.1
 Lifetime granted 00:03:00 (180), remaining 00:02:20
 Flags sbDmg-T-, Identification BCF5F7FF.92C1006F
 Tunnel0 src 192.168.202.1 dest 192.168.157.1 reverse-allowed
 Routing Options - (D)Direct-to-MN (T)Reverse-tunnel
 Service Options:
 NAT detect
```

The following sample output shows that multipath support is enabled:

```
Router# show ip mobile binding

Mobility Binding List:
Total 1
10.1.1.1:
    Care-of Addr 10.1.1.11, Src Addr 10.1.1.11
    Lifetime granted 10:00:00 (36000), remaining 09:52:40
    Flags sbDmg-T-, Identification C5441314.61D36B14
    Tunnel1 src 12.1.1.10 dest 10.1.1.11 reverse-allowed
    MR Tunnel1 src 12.1.1.10 dest 10.1.1.11 reverse-allowed
    Routing Options - (D)Direct-to-MN (T)Reverse-tunnel
    Mobile Networks: 10.38.0.0/255.255.0.0 (D)
    Roaming IF Attributes: BW 10000 Kbit, ID 3247
     Description First Lan Interface
    Multi-path Metric bandwidth
```

Table 9 describes the significant fields shown in the display.

Table 9 show ip mobile binding Field Descriptions

Field	Description
Total	Total number of mobility bindings.
<IP Address>	Home IP address of the mobile node. The NAI is displayed if configured.
Care-of Addr	Care-of address of the mobile node.
Src Addr	IP source address of the registration request as received by the home agent. Will be either the colocated care-of address of a mobile node or an address on the foreign agent or the active HA address. If it is the active HA address, then this is a binding update from the active HA to the standby HA and not a registration directly received from the MN or FA.
Lifetime granted	The lifetime (in hh:mm:ss) granted to the mobile node for this registration. Number of seconds appears in parentheses.
remaining	The time (in hh:mm:ss) remaining until the registration expires. It has the same initial value as lifetime granted and is counted down by the home agent.
Flags	Services requested by the mobile node. The mobile node requests these services by setting bits in the registration request. Uppercase characters denote bit set.
Identification	Identification used in that binding by the mobile node. This field has two purposes: unique identifier for each request and replay protection.
Tunnel	The tunnel used by the mobile node is characterized by the source and destination addresses and reverse-allowed or reverse-off for reverse tunnel. The default encapsulation is IP-in-IP. The mobile node can request GRE.
Routing Options	Routing options identify the services that the home agent is currently providing. The mobile node must request these services in its registration request by setting the services flag (see Flags field description). For example, the V bit may have been requested by the mobile node (shown in the Flags field), but the home agent will not provide such service. Possible options are B (broadcast), D (direct-to-mobile node), G (GRE), and T (reverse-tunnel).
Service Options	Service options configured.
NAT detect	Indicates that the mobile node is registering from behind a NAT-enabled router.

Table 9 show ip mobile binding Field Descriptions (continued)

Field	Description
Mobile Networks	Mobile networks configured or registered on the home agent. D denotes dynamic (registered) mobile networks, and S denotes static (configured) mobile networks.
Session identifier	The ID used to uniquely identify a Mobile IP flow.
SPI	The security parameter index (SPI) is the 4-byte opaque index within the mobility security association that selects the specific security parameters to be used to authenticate the peer.
MD5	Message Digest 5 authentication algorithm. HMAC-MD5 is displayed if configured.
Prefix-suffix	Authentication mode.
Timestamp	Replay protection method.
root key	Dynamic key based on the Microsoft Windows password shared between the mobile node and AAA or Windows domain controller or active directory. Once a mobile node registers, this key is established until the binding persists on the home agent. Subsequent registration requests can be authenticated using the root key.
session key	Dynamic key that is derived using the root key. This key can be refreshed, and the refreshed keys are based off the root key. Subsequent registration renewal messages can be authenticated using the session key. The period or frequency for the session key refresh is determined by the mobile node. Registration requests that also request session key refresh are authenticated using the root key.
Roaming IF Attributes	Attributes associated with the roaming interface. BW denotes the bandwidth of the roaming interface.
Description	Description of the roaming interface on the mobile router.
Multi-path Metric bandwidth	Metric that the mobile router uses for multipath support.

Related Commands

Command	Description
debug ip mobile	Displays IP mobility activities.
ip mobile foreign-agent nat traversal	Enables NAT UDP traversal support for Mobile IP foreign agents.
ip mobile home-agent nat traversal	Enables NAT UDP traversal support for Mobile IP HAs.
show ip mobile globals	Displays global information about Mobile IP home agents, foreign agents, and mobile nodes.
show ip mobile tunnel	Displays information about UDP tunneling.
show ip mobile visitor	Displays the table that contains a visitor list of foreign agents.

show ip mobile binding

To display the mobility binding table, use the **show ip mobile binding** EXEC command.

show ip mobile binding [ip address | **home-agent** *address* | ***nai*** *string* | **summary** | **vrf [realm** ***vrf-realm*****] [summary]**]

Syntax Description

ip address	IP address of the Home agent
home-agent *address*	(Optional) IP address of mobile node.
nai string	(Optional) Network access identifier.
summary	(Optional) Displays the total number of bindings that are VRF-enabled.
vrf	(Optional) VRF of the user.
realm	(Optional) Displays the vrf realm.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.0(2)T	The following keyword and argument were added: • **home-agent** *address*
12.1(2)T	The **summary** keyword was added.
12.2(2)XC	The **nai** keyword was added.
12.3(7)XJ	This command was modified to display VRF related info if the realm of the NAI is under a VRF.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

The Home Agent updates the mobility binding table in response to registration events from mobile nodes. If the *address* argument is specified, bindings are shown for only that mobile node.

Examples

The following is sample output from the **show ip mobile binding** command:

```
Router# show ip mobile binding

Mobility Binding List:
Total 1
mwts-mip-r20sit-haslb@ispxyz.com (Bindings 1):
    Home Addr 40.0.0.2
    Care-of Addr 20.20.210.10, Src Addr 20.20.210.10
    Lifetime granted 00:05:00 (300), remaining 00:04:11
    Flags sBdmg-T-, Identification C70D0890.10000
    Tunnel0 src 20.20.202.102 dest 20.20.210.10 reverse-allowed
    Tunnel0 Input ACL: mipinacl
    Tunnel0 Output ACL: mipoutacl
```

```
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Service Options:
        Dynamic HA assignment
    Revocation negotiated - I-bit set
    Acct-Session-Id: 43
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Radius Disconnect Enabled
    DNS Address primary 10.77.155.10 secondary 6.6.6.6
    DNS Address Assignment enabled with entity Configured at Homeagent(3)
    Dynamic DNS update to server enabled
ha2#
```

If the DNS server configs configured locally are used then the show output will include the following:

```
router# show ip mobile binding
Mobility Binding List:
    Total 1
    mwts-mip-r20sit-haslb@ispxyz20.com (Bindings 1):
    Home Addr 40.0.0.2
    Care-of Addr 20.20.210.10, Src Addr 20.20.210.10
    Lifetime granted 00:03:00 (180), remaining 00:02:32
    Flags sBdmg-T-, Identification C6ACD1D7.10000
    Tunnel0 src 20.20.202.102 dest 20.20.210.10 reverse-allowed
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Service Options:
    Dynamic HA assignment
    Revocation negotiated - I-bit set
    Acct-Session-Id: 23
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    DNS Address primary 10.77.155.10 secondary 5.5.5.5
    DNS Address Assignment enabled with entity Configured at Homeagent(3)
```

If the DNS server addresses downloaded using a DNS server VSA from HAAA, then the show output will include the following:

```
router# show ip mobile binding
Mobility Binding List:
    Total 1
    mwts-mip-r20sit-haslb@ispxyz30.com (Bindings 1):
    Home Addr 40.0.0.3
    Care-of Addr 20.20.210.10, Src Addr 20.20.210.10
    Lifetime granted 00:03:00 (180), remaining 00:02:05
    Flags sBdmg-T-, Identification C6ACD910.10000
    Tunnel0 src 20.20.202.102 dest 20.20.210.10 reverse-allowed
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Service Options:
    Dynamic HA assignment
    Revocation negotiated - I-bit set
    Acct-Session-Id: 31
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    DNS Address primary 10.77.155.10 secondary 10.77.155.9
    DNS Address Assignment enabled with entity From Home AAA(1)
```

Note If the DNS server address is configured both locally and downloaded from AAA, then preference will be given to the local configuration on the HA.

ACLs Applied to a Mobility Binding and Accounting Session ID and Accounting Counters

```
router# show ip mobile binding 44.0.0.1
Mobility Binding List:
    44.0.0.1:
    Care-of Addr 55.0.0.11, Src Addr 55.0.0.11
    Lifetime granted 00:01:30 (90), remaining 00:00:51
    Flags sbDmg-T-, Identification C661D5A0.4188908
    Tunnel1 src 46.0.0.3 dest 55.0.0.11 reverse-allowed
    Tunnel1 Input ACL: inaclname
    Tunnel1 Output ACL: outaclname - Empty list or not configured.
    MR Tunnel1 src 46.0.0.3 dest 55.0.0.11 reverse-allowed
    Routing Options - (D)Direct-to-MN (T)Reverse-tunnel
    Mobile Networks: 111.0.0.0/255.0.0.0 (S)
    Acct-Session-Id: 0
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes

router# show ip mobile tunnel

Mobile Tunnels:
    Total mobile ip tunnels 1
    Tunnel0:
    src 46.0.0.3, dest 55.0.0.11
    encap IP/IP, mode reverse-allowed, tunnel-users 1
    Input ACL users 1, Output ACL users 1
    IP MTU 1480 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Ethernet1/0
    HA created, fast switching enabled, ICMP unreachable enabled
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 drops
    0 packets output, 0 bytes
```

The following is sample output from the **show ip mobile binding vrf summary** command:

```
router# show ip mobile binding vrf summary
Mobility Binding List:
Total number of VRF bindings is 1
```

If the VRF name downloaded from the HAAA and what is configured locally matches , then the **show ip mobile binding vrf realm** command will display the ouput below:

```
router# show ip mobile binding vrf realm @ispxyz1.com
Mobility Binding List:
Total bindings for realm @ispxyz1.com under VRF ispxyz-vrf1 is 1
mwts-mip-r20sit-haslb1@ispxyz1.com (Bindings 1):
Home Addr 50.0.0.2
Care-of Addr 20.20.210.10, Src Addr 20.20.210.10
Lifetime granted 00:05:00 (300), remaining 00:03:59
Flags sBdmg-T-, Identification C6DF047C.10000
Tunnel0 src 20.20.204.2 dest 20.20.210.10 reverse-allowed
Routing Options - (B)Broadcast (T)Reverse-tunnel
Service Options:
Dynamic HA assignment
Revocation negotiated - I-bit set
VRF ispxyz-vrf1
Acct-Session-Id: 17
Sent on tunnel to MN: 0 packets, 0 bytes
Received on reverse tunnel from MN: 0 packets, 0 bytes
Radius Disconnect Enabled
DNS Address primary 10.77.155.10 secondary 1.1.1.1
```

```
DNS Address Assignment enabled with entity Configured at Homeagent(3)
Dynamic DNS update to server enabled
```

If VRF is not configured locally, then the **show** output will be as below:

```
router# show ip mobile binding vrf realm @ispxyz1.com summary
Mobility Binding List:
%VRF is not enabled locally for realm @ispxyz1.com
```

Table 10 describes the significant fields shown in the display.

Table 10 show ip mobile binding Field Descriptions

Field	Description
Total	Total number of mobility bindings.
IP address	Home IP address of the mobile node.
Care-of Addr	Care-of address of the mobile node.
Src Addr	IP source address of the Registration Request as received by the Home Agent. Will be either the collocated care-of address of a mobile node or an address of the Foreign Agent.
Lifetime granted	The lifetime granted to the mobile node for this registration. Number of seconds in parentheses.
Lifetime remaining	The time remaining until the registration is expired. It has the same initial value as lifetime granted, and is counted down by the Home Agent.
Flags	Registration flags sent by mobile node. Uppercase characters denote bit set.
Identification	Identification used in that binding by the mobile node. This field has two purposes: unique identifier for each request, and replay protection.
Tunnel	The tunnel used by the mobile node is characterized by the source and destination addresses, and reverse-allowed or reverse-off for reverse tunnel. The default is IPIP encapsulation, otherwise GRE will be displayed in the Routing Options field.
Routing Options	Routing options list all Home Agent-accepted services. For example, the V bit may have been requested by the mobile node (shown in the Flags field), but the Home Agent will not provide such service. Possible options are B (broadcast), D (direct-to-mobile node), G (GRE), and T (reverse-tunnel).

show ip mobile binding

To display the mobility binding table, use the **show ip mobile binding** EXEC command.

show ip mobile binding [ip address | **home-agent** *address* | ***nai*** *string* | **summary** | **vrf [realm** ***vrf-realm*****] [summary]**]

Syntax Description

ip address	IP address of the Home agent
home-agent *address*	(Optional) IP address of mobile node.
nai string	(Optional) Network access identifier.
summary	(Optional) Displays the total number of bindings that are VRF-enabled.
vrf	(Optional) VRF of the user.
realm	(Optional) Displays the vrf realm.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.0(2)T	The following keyword and argument were added: • **home-agent** *address*
12.1(2)T	The **summary** keyword was added.
12.2(2)XC	The **nai** keyword was added.
12.3(7)XJ	This command was modified to display VRF related info if the realm of the NAI is under a VRF.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

The Home Agent updates the mobility binding table in response to registration events from mobile nodes. If the *address* argument is specified, bindings are shown for only that mobile node.

Examples

The following is sample output from the **show ip mobile binding** command:

```
Router# show ip mobile binding

Mobility Binding List:
Total 1
mwts-mip-r20sit-haslb@ispxyz.com (Bindings 1):
    Home Addr 40.0.0.2
    Care-of Addr 20.20.210.10, Src Addr 20.20.210.10
    Lifetime granted 00:05:00 (300), remaining 00:04:11
    Flags sBdmg-T-, Identification C70D0890.10000
    Tunnel0 src 20.20.202.102 dest 20.20.210.10 reverse-allowed
    Tunnel0 Input ACL: mipinacl
    Tunnel0 Output ACL: mipoutacl
```

```
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Service Options:
        Dynamic HA assignment
    Revocation negotiated - I-bit set
    Acct-Session-Id: 43
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Radius Disconnect Enabled
    DNS Address primary 10.77.155.10 secondary 6.6.6.6
    DNS Address Assignment enabled with entity Configured at Homeagent(3)
    Dynamic DNS update to server enabled
ha2#
```

If the DNS server configs configured locally are used then the show output will include the following:

```
router# show ip mobile binding
Mobility Binding List:
    Total 1
    mwts-mip-r20sit-haslb@ispxyz20.com (Bindings 1):
    Home Addr 40.0.0.2
    Care-of Addr 20.20.210.10, Src Addr 20.20.210.10
    Lifetime granted 00:03:00 (180), remaining 00:02:32
    Flags sBdmg-T-, Identification C6ACD1D7.10000
    Tunnel0 src 20.20.202.102 dest 20.20.210.10 reverse-allowed
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Service Options:
    Dynamic HA assignment
    Revocation negotiated - I-bit set
    Acct-Session-Id: 23
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    DNS Address primary 10.77.155.10 secondary 5.5.5.5
    DNS Address Assignment enabled with entity Configured at Homeagent(3)
```

If the DNS server addresses downloaded using a DNS server VSA from HAAA, then the show output will include the following:

```
router# show ip mobile binding
Mobility Binding List:
    Total 1
    mwts-mip-r20sit-haslb@ispxyz30.com (Bindings 1):
    Home Addr 40.0.0.3
    Care-of Addr 20.20.210.10, Src Addr 20.20.210.10
    Lifetime granted 00:03:00 (180), remaining 00:02:05
    Flags sBdmg-T-, Identification C6ACD910.10000
    Tunnel0 src 20.20.202.102 dest 20.20.210.10 reverse-allowed
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Service Options:
    Dynamic HA assignment
    Revocation negotiated - I-bit set
    Acct-Session-Id: 31
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    DNS Address primary 10.77.155.10 secondary 10.77.155.9
    DNS Address Assignment enabled with entity From Home AAA(1)
```

Note If the DNS server address is configured both locally and downloaded from AAA, then preference will be given to the local configuration on the HA.

ACLs Applied to a Mobility Binding and Accounting Session ID and Accounting Counters

```
router# show ip mobile binding 44.0.0.1
Mobility Binding List:
    44.0.0.1:
    Care-of Addr 55.0.0.11, Src Addr 55.0.0.11
    Lifetime granted 00:01:30 (90), remaining 00:00:51
    Flags sbDmg-T-, Identification C661D5A0.4188908
    Tunnel1 src 46.0.0.3 dest 55.0.0.11 reverse-allowed
    Tunnel1 Input ACL: inaclname
    Tunnel1 Output ACL: outaclname - Empty list or not configured.
    MR Tunnel1 src 46.0.0.3 dest 55.0.0.11 reverse-allowed
    Routing Options - (D)Direct-to-MN (T)Reverse-tunnel
    Mobile Networks: 111.0.0.0/255.0.0.0 (S)
    Acct-Session-Id: 0
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes

router# show ip mobile tunnel

Mobile Tunnels:
    Total mobile ip tunnels 1
    Tunnel0:
    src 46.0.0.3, dest 55.0.0.11
    encap IP/IP, mode reverse-allowed, tunnel-users 1
    Input ACL users 1, Output ACL users 1
    IP MTU 1480 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Ethernet1/0
    HA created, fast switching enabled, ICMP unreachable enabled
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 drops
    0 packets output, 0 bytes
```

The following is sample output from the **show ip mobile binding vrf summary** command:

```
router# show ip mobile binding vrf summary
Mobility Binding List:
Total number of VRF bindings is 1
```

If the VRF name downloaded from the HAAA and what is configured locally matches , then the **show ip mobile binding vrf realm** command will display the ouput below:

```
router# show ip mobile binding vrf realm @ispxyz1.com
Mobility Binding List:
Total bindings for realm @ispxyz1.com under VRF ispxyz-vrf1 is 1
mwts-mip-r20sit-haslb1@ispxyz1.com (Bindings 1):
Home Addr 50.0.0.2
Care-of Addr 20.20.210.10, Src Addr 20.20.210.10
Lifetime granted 00:05:00 (300), remaining 00:03:59
Flags sBdmg-T-, Identification C6DF047C.10000
Tunnel0 src 20.20.204.2 dest 20.20.210.10 reverse-allowed
Routing Options - (B)Broadcast (T)Reverse-tunnel
Service Options:
Dynamic HA assignment
Revocation negotiated - I-bit set
VRF ispxyz-vrf1
Acct-Session-Id: 17
Sent on tunnel to MN: 0 packets, 0 bytes
Received on reverse tunnel from MN: 0 packets, 0 bytes
Radius Disconnect Enabled
DNS Address primary 10.77.155.10 secondary 1.1.1.1
```

```
DNS Address Assignment enabled with entity Configured at Homeagent(3)
Dynamic DNS update to server enabled
```

If VRF is not configured locally, then the **show** output will be as below:

```
router# show ip mobile binding vrf realm @ispxyz1.com summary
Mobility Binding List:
```
%VRF is not enabled locally for realm @ispxyz1.com

Table 11 describes the significant fields shown in the display.

Table 11 show ip mobile binding Field Descriptions

Field	Description
Total	Total number of mobility bindings.
IP address	Home IP address of the mobile node.
Care-of Addr	Care-of address of the mobile node.
Src Addr	IP source address of the Registration Request as received by the Home Agent. Will be either the collocated care-of address of a mobile node or an address of the Foreign Agent.
Lifetime granted	The lifetime granted to the mobile node for this registration. Number of seconds in parentheses.
Lifetime remaining	The time remaining until the registration is expired. It has the same initial value as lifetime granted, and is counted down by the Home Agent.
Flags	Registration flags sent by mobile node. Uppercase characters denote bit set.
Identification	Identification used in that binding by the mobile node. This field has two purposes: unique identifier for each request, and replay protection.
Tunnel	The tunnel used by the mobile node is characterized by the source and destination addresses, and reverse-allowed or reverse-off for reverse tunnel. The default is IPIP encapsulation, otherwise GRE will be displayed in the Routing Options field.
Routing Options	Routing options list all Home Agent-accepted services. For example, the V bit may have been requested by the mobile node (shown in the Flags field), but the Home Agent will not provide such service. Possible options are B (broadcast), D (direct-to-mobile node), G (GRE), and T (reverse-tunnel).

show ip mobile globals

To display global information for mobile agents, use the **show ip mobile globals** command in privileged EXEC mode.

show ip mobile globals

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(13)T	This command was enhanced to display the NAT detect field and the Strip realm domain field.
12.2(15)T	This command was enhanced to display the HA Accounting field.
12.3(7)T	This command was enhanced to display information about foreign agent route optimization.
12.3(8)T	This command was enhanced to display information about UDP tunneling.
12.4(9)T	This command was enhanced to display information about multipath support.

Usage Guidelines

This command shows the services provided by the home agent or foreign agent. Note the deviation from RFC 3344: the foreign agent will not display busy or registration required information. Both are handled on a per-interface basis (see the **show ip mobile interface** command), not at the global foreign agent level.

Examples

The following is sample output from the **show ip mobile globals** command:

```
Router# show ip mobile globals

IP Mobility global information:

Home Agent

    Registration lifetime: 10:00:00 (36000 secs)
    Broadcast enabled
    Replay protection time: 7 secs
    Reverse tunnel enabled
    ICMP Unreachable enabled
    Strip realm enabled
    NAT detect disabled
    HA Accounting enabled using method list: mylist
    Address 1.1.1.1
    Virtual networks
        10.0.0.0/8
```

```
Foreign Agent

    Pending registrations expire after 120 seconds
    Care-of address advertised
    Mobile network route injection enabled
    Mobile network route redistribution disabled
    Mobile network route injection access list mobile-net-list
    Ethernet2/2 (10.10.10.1) - up

Mobility Agent

1 interfaces providing service
Encapsulations supported: IPIP and GRE
Tunnel fast switching enabled, cef switching enabled
Discovered tunnel MTU aged out after 1:00:00
```

The following example shows that home agent UDP tunneling is enabled with a keepalive timer set at 60 seconds and forced UDP tunneling enabled.

```
Router# show ip mobile globals

IP Mobility global information:

Home agent

 Registration lifetime: 10:00:00 (36000 secs)
 Broadcast disabled
 Replay protection time: 7 secs
 Reverse tunnel enabled
 ICMP Unreachable enabled
 Strip realm disabled
 NAT Traversal disabled
 HA Accounting disabled
 NAT UDP Tunneling support enabled
 UDP Tunnel Keepalive 60
 Forced UDP Tunneling enabled
 Virtual networks
 10.99.101.0/24

Foreign agent is not enabled, no care-of address

0 interfaces providing service
Encapsulations supported: IPIP and GRE
Tunnel fast switching enabled, cef switching enabled
Tunnel path MTU discovery aged out after 10 min
```

The following example shows that NAT UDP tunneling support is enabled on the foreign agent with a keepalive timer set at 110 seconds and forced UDP tunneling disabled.

```
Router# show ip mobile globals

IP Mobility global information:

Foreign Agent

Pending registrations expire after 120 secs
Care-of addresses advertised
Mobile network route injection disabled

Ethernet2/2 (10.30.30.1) - up
```

```
1 interface providing service
Encapsulations supported: IPIP and GRE
Tunnel fast switching enabled, cef switching enabled
Tunnel path MTU discovery aged out after 10 min
NAT UDP Tunneling support enabled
UDP Tunnel Keepalive 110
Forced UDP Tunneling disabled
```

The following example output shows that multipath support is enabled:

```
Router# show ip mobile globals

IP Mobility global information:

Home Agent

    Registration lifetime: 10:00:00 (36000 secs)
    Broadcast disabled
    Replay protection time: 7 secs
    ….
    UDP Tunnel Keepalive 110
    Forced UDP Tunneling disabled
    Multiple Path Support enabled
```

Table 12 describes the significant fields shown in the sample output.

Table 12 show ip mobile globals Field Descriptions

Field	Description
Home Agent	
Registration lifetime	Default lifetime (in hh:mm:ss) for all mobile nodes. Number of seconds given in parentheses.
Roaming access list	Determines which mobile nodes are allowed to roam. Displayed if defined.
Care-of access list	Determines which care-of addresses are allowed to be accepted. Displayed if defined.
Broadcast	Whether broadcast is enabled or disabled.
Replay protection time	Time, in seconds, that the time stamp on a registration request (RRQ) from a mobile node may differ from the router's internal clock.
Reverse tunnel	Whether reverse tunnel is enabled or disabled.
ICMP Unreachable	Sends ICMP unreachable messages, which are enabled or disabled for the virtual network.
Strip realm	Whether strip realm is enabled or disabled.
NAT detect	Whether NAT detect is enabled or disabled. If NAT detect is enabled, the home agent can detect a registration request that has traversed a NAT-enabled device and can apply a tunnel to reach the Mobile IP client.
HA Accounting	Whether home agent accounting is enabled or disabled.
NAT UDP Tunneling support	Whether NAT UDP tunneling is enabled or disabled on the home agent.
UDP Tunnel Keepalive	Keepalive interval, in seconds, configured on the home agent that avoids a NAT translation entry on a NAT device from expiring when there is no active Mobile IP data traffic going through the UDP tunnel.

Table 12 show ip mobile globals Field Descriptions (continued)

Field	Description
Forced UDP Tunneling	Whether the home agent is configured to accept forced UDP tunneling.
Address	Home agent address.
Virtual networks	Lists virtual networks serviced by the home agent. Displayed if defined.
Multiple Path Support	Whether multiple path support is enabled or disabled.
Foreign Agent	
Pending registrations expire after	The amount of time, in seconds, before a pending registration will time out.
Care-of addresses advertised	Displayed if care-of addresses are defined.
Mobile network route injection	Mobile network route injection can be enabled or disabled.
Mobile network route redistribution	Mobile network route redistribution can be enabled or disabled.
Mobile network route injection access list	The name of the access list used if mobile network route injection is enabled.
NAT UDP Tunneling support	Whether NAT UDP tunneling is enabled or disabled on the foreign agent
UDP Tunnel Keepalive	Keepalive interval, in seconds, configured on the foreign agent that avoids a NAT translation entry on a NAT device from expiring when there is no active Mobile IP data traffic going through the UDP tunnel.
Forced UDP Tunneling	Whether the foreign agent is configured to force UDP tunneling.
up, interface-only, transmit-only	Up status is displayed if the foreign agent is configured to function in an asymmetric link environment. Interface-only status is displayed if the foreign agent is configured to advertise only its own address as the care-of address in an asymmetric link environment. Transmit-only status is displayed if the foreign agent is configured to transmit only from the interface in an asymmetric link environment.
Mobility Agent	
Number of interfaces providing service	See the **show ip mobile interface** command for more information on the interfaces providing service. Agent advertisements are sent when ICMP Router Discovery Protocol (IRDP) is enabled.
Encapsulations supported	The encapsulation types that are supported. Possible encapsulation types are IPIP and GRE.
Tunnel fast switching	Whether tunnel fast switching is enabled or disabled.

Table 12 show ip mobile globals Field Descriptions (continued)

Field	Description
cef switching	Whether CEF switching is enabled or disabled.
Discovered tunnel MTU	Aged out after amount of time (in hh:mm:ss).

Related Commands

Command	Description
show ip mobile interface	Displays advertisement information for interfaces that are providing foreign agent service or that are home links for mobile nodes.

show ip mobile host

To display mobile node information, use the **show ip mobile host** command in privileged EXEC mode.

show ip mobile host [*address* | **interface** *interface* | **network** *address* | **nai** *string* | **group** | **summary**]

Syntax Description

address	(Optional) IP address of specific mobile node. If not specified, information for all mobile nodes is displayed.
interface *interface*	(Optional) Displays all mobile nodes whose home network is on this interface.
network *address*	(Optional) Displays all mobile nodes residing on this network or virtual network.
nai *string*	(Optional) Network access identifier.
group	(Optional) Displays all mobile node groups configured using the **ip mobile host** command.
summary	(Optional) Displays all values in the table.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The **nai** keyword was added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Examples

The following is sample output from the **show ip mobile host** command:

```
Router# show ip mobile host

10.34.253.147:
   Allowed lifetime 10:00:00 (36000/default)
   Roam status -Registered-, Home link on virtual network 10.34.253.128 /26
   Accepted 2082, Last time 02/13/03 01:03:24
   Overall service time 1w0d
   Denied 32, Last time 01/03/03 21:13:43
   Last code 'registration id mismatch (133)'
   Total violations 32
   Tunnel to MN - pkts 0, bytes 0
   Reverse tunnel from MN - pkts 0, bytes 0
```

The following is sample output from the **show ip mobile host nai** *string* command:

```
Router# show ip mobile host nai jane@cisco.com

jane@cisco.com
   Allowed lifetime 10:00:00 (36000/default)
   Roam status -Registered-, Home link on interface Loopback0
   Bindings 10.34.253.205
   Accepted 3705, Last time 02/13/03 01:02:37
   Overall service time 6d05h
```

```
Denied 4918, Last time 01/30/03 20:59:14
Last code 'administratively prohibited (129)'
Total violations 262
Tunnel to MN - pkts 0, bytes 0
Reverse tunnel from MN - pkts 0, bytes 0
```

Table 13 describes the significant fields shown in the display.

Table 13 show ip mobile host Field Descriptions

Field	Description
IP address	Home IP address of the mobile node. The network access identifier (NAI) is displayed if configured.
Allowed lifetime	Allowed lifetime (in hh:mm:ss) of the mobile node. By default, it is set to the global lifetime (**ip mobile home-agent lifetime** command). Setting this lifetime will override global value.
Roaming status	When the mobile node is registered, the roaming status is - Registered - ; otherwise, it is - Unregistered -. Use the **show ip mobile binding** command for more information when the user is registered.
Home link	Interface or virtual network.
Accepted	Total number of service requests for the mobile node accepted by the home agent.
Last time	The time at which the most recent registration request was accepted by the home agent for this mobile node.
Overall service time	Overall service time that has accumulated for the mobile node since the router has booted or cleared.
Denied	Total number of service requests for the mobile node denied by the home agent (sum of all registrations denied with Code 128 through Code 159).
Last time	The time at which the most recent registration request was denied by the home agent for this mobile node.
Last code	The code indicating the reason why the most recent registration request for this mobile node was rejected by the home agent.
Total violations	Total number of security violations.
Tunnel to mobile node	Number of packets and bytes tunneled to mobile node.
Reverse tunnel from mobile node	Number of packets and bytes reverse tunneled from mobile node.
NAI string	NAI associated with the mobile node.
Bindings	Addresses currently assigned to the NAI.

The following is sample output from the **show ip mobile host group** command for groups configured with the **ip mobile host** command:

```
Router# show ip mobile host group

20.0.0.1 - 20.0.0.20:
    Home link on virtual network 20.0.0.0 /8, Care-of ACL -none-
    Security associations on router, Allowed lifetime 10:00:00 (36000/default)
```

Table 14 describes the significant fields shown in the display.

Table 14 show ip mobile host group Field Descriptions

Field	Description
IP address	Mobile host IP address or grouping of addresses.
Home link	Interface or virtual network.
Care-of ACL	Care-of address access list.
Security association	Router or AAA server.
Allowed lifetime	Allowed lifetime for mobile host or group.

Related Commands

Command	Description
clear ip mobile host-counters	Clears the mobile node counters.
show ip mobile binding	Displays the mobility binding table.

show ip mobile secure

To display the mobility security associations for the mobile host, mobile visitor, foreign agent, home agent, or proxy Mobile IP host, use the **show ip mobile secure** command in privileged EXEC mode.

show ip mobile secure {**host** | **visitor** | **foreign-agent** | **home-agent** | **proxy-host** | **summary**} {*ip-address* | **nai** *string*}

Syntax Description

host	Displays security association of the mobile host on the home agent.
visitor	Displays security association of the mobile visitor on the foreign agent.
foreign-agent	Displays security association of the remote foreign agents on the home agent.
home-agent	Displays security association of the remote home agent on the foreign agent.
proxy-host	Displays security association of the proxy mobile user. This keyword is only available on Packet Data Serving Node (PDSN) platforms running specific PDSN code images.
summary	Displays number of security associations in table.
ip-address	IP address.
nai *string*	Network access identifier (NAI).

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The **nai** keyword was added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(4)T	The **proxy-host** keyword was added for PDSN platforms.

Usage Guidelines

Multiple security associations can exist for each entity.

The **proxy-host** keyword is only available on PDSN platforms running specific PDSN code images; consult Feature Navigator for your Cisco IOS software release.

Examples

The following is sample output from the **show ip mobile secure** command:

```
Router# show ip mobile secure

Security Associations (algorithm,mode,replay protection,key):
10.0.0.6
    SPI 300,  MD5, Prefix-suffix, Timestamp +/- 7,
    Key 00112233445566778899001122334455
```

Table 15 describes the significant fields shown in the display.

Table 15 show ip mobile secure Field Descriptions

Field	Description
10.0.0.6	IP address. The NAI is displayed if configured.
In/Out SPI	The SPI is the 4-byte opaque index within the mobility security association that selects the specific security parameters to be used to authenticate the peer. Allows either "SPI" or "In/Out SPI." The latter specifies an inbound and outbound SPI pair. If an inbound SPI is received, then outbound SPI will be used when a response is sent.
MD5	Message Digest 5 authentication algorithm. HMAC-MD5 id displayed if configured.
Prefix-suffix	Authentication mode.
Timestamp	Replay protection method.
Key	The shared secret key for the security associations, in hexadecimal format.

show ip mobile traffic

To display protocol counters, use the **show ip mobile traffic** command in privileged EXEC mode.

show ip mobile traffic

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(13)T	This command was enhanced to display successful registration requests with NAT detect and to display information about foreign agent reverse tunnels and foreign agent challenge and response extensions.
12.3(14)T	The command output was enhanced to display the count of UDP Port 434 input packets that were dropped by UDP.

Usage Guidelines

Counters can be reset to zero using the **clear ip mobile traffic** command, which also allows you to undo the reset.

Examples

The following is sample output from the **show ip mobile traffic** command:

```
Router# show ip mobile traffic

IP Mobility traffic:
UDP:
    Port: 434 (Mobile IP) input drops: 0
Advertisements:
    Solicitations received 0
    Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
    Register 0, Deregister 0 requests
    Register 0, Deregister 0 replied
    Accepted 0, No simultaneous bindings 0
    Denied 0, Ignored 0
    Unspecified 0, Unknown HA 0
    Administrative prohibited 0, No resource 0
    Authentication failed MN 0, FA 0
    Bad identification 0, Bad request form 0
    Unavailable encap 0, reverse tunnel 0
    Reverse tunnel mandatory 0
    Binding updates received 0, sent 0 total 0 fail 0
    Binding update acks received 0, sent 0
    Binding info request received 0, sent 0 total 0 fail 0
    Binding info reply received 0 drop 0, sent 0 total 0 fail 0
    Binding info reply acks received 0 drop 0, sent 0
    Gratuitous 0, Proxy 0 ARPs sent
    Total incoming requests using NAT detect 1
```

```
Foreign Agent Registrations:
    Request in 0,
    Forwarded 0, Denied 0, Ignored 0
    Unspecified 0, HA unreachable 0
    Administrative prohibited 0, No resource 0
    Bad lifetime 0, Bad request form 0
    Unavailable encapsulation 0, Compression 0
    Unavailable reverse tunnel 0
    Reverse tunnel mandatory
    Replies in 0
    Forwarded 0, Bad 0, Ignored 0
    Authentication failed MN 0, HA 0
    Received challenge/gen. authentication extension, feature not enabled 0
    Route Optimization Binding Updates received 0, acks sent 0 neg acks sent 0
    Unknown challenge 1, Missing challenge 0, Stale challenge 0
```

Table 16 describes the significant fields shown in the display.

Table 16 show ip mobile traffic Field Descriptions

Field	Description
Port: 434 (Mobile IP) input drops	Total number of UDP Port 434 (Mobile IP) packets dropped by UDP processing due to a full input queue. These packets are not processed by the home agent or foreign agent and so are not otherwise counted or displayed by Mobile IP. This count is the same count displayed by using the **show ip socket detail** command.
Solicitations received	Total number of solicitations received by the mobility agent.
Advertisements sent	Total number of advertisements sent by the mobility agent.
response to solicitation	Total number of advertisements sent by the mobility agent in response to mobile node solicitations.
Home Agent	
Register requests	Total number of registration requests received by the home agent.
Deregister requests	Total number of registration requests received by the home agent with a lifetime of zero (requests to deregister).
Register replied	Total number of registration replies sent by the home agent.
Deregister replied	Total number of registration replies sent by the home agent in response to requests to deregister.
Accepted	Total number of registration requests accepted by the home agent (Code 0).
No simultaneous bindings	Total number of registration requests accepted by the home agent—simultaneous mobility bindings unsupported (Code 1).
Denied	Total number of registration requests denied by the home agent.
Ignored	Total number of registration requests ignored by the home agent.
Unspecified	Total number of registration requests denied by the home agent—reason unspecified (Code 128).
Unknown HA	Total number of registration requests denied by the home agent—unknown home agent address (Code 136).
Administrative prohibited	Total number of registration requests denied by the home agent—administratively prohibited (Code 129).

Table 16 show ip mobile traffic Field Descriptions (continued)

Field	Description
No resource	Total number of registration requests denied by the home agent—insufficient resources (Code 130).
Authentication failed MN	Total number of registration requests denied by the home agent—mobile node failed authentication (Code 131).
Authentication failed FA	Total number of registration requests denied by the home agent—foreign agent failed authentication (Code 132).
Bad identification	Total number of registration requests denied by the home agent—identification mismatch (Code 133).
Bad request form	Total number of registration requests denied by the home agent—poorly formed request (Code 134).
Unavailable encap	Total number of registration requests denied by the home agent—unavailable encapsulation (Code 139).
Reverse tunnel mandatory	Total number of registration requests denied by the home agent—reverse tunnel is mandatory and the "T" bit is not set (Code 138).
Unavailable reverse tunnel	Total number of registration requests denied by the home agent—reverse tunnel unavailable (Code 137).
Binding updates	A Mobile IP standby message sent from the active router to the standby router when a registration request comes into the active router.
Binding update acks	A Mobile IP standby message sent from the standby router to the active router to acknowledge the reception of a binding update.
Binding info request	A Mobile IP standby message sent from a router coming up from reboot/or a down interface. The message is a request to the current active router to send the entire Mobile IP binding table.
Binding info reply	A reply from the active router to the standby router that has part or all of the binding table (depending on size).
Binding info reply acks	An acknowledge message from the standby router to the active router that it has received the binding info reply.
Gratuitous ARP	Total number of gratuitous ARPs sent by the home agent on behalf of mobile nodes.
Proxy ARPs sent	Total number of proxy ARPs sent by the home agent on behalf of mobile nodes.
Total incoming registration requests...	Total number incoming registration requests using NAT detect.
Foreign Agent	
Request in	Total number of registration requests received by the foreign agent.
Forwarded	Total number of registration requests relayed to the home agent by the foreign agent.
Denied	Total number of registration requests denied by the foreign agent.
Ignored	Total number of registration requests ignored by the foreign agent.
Unspecified	Total number of registration requests denied by the foreign agent—reason unspecified (Code 64).

Table 16 show ip mobile traffic Field Descriptions (continued)

Field	Description
HA unreachable	Total number of registration requests denied by the foreign agent—home agent unreachable (Codes 80-95).
Administrative prohibited	Total number of registration requests denied by the foreign agent—administratively prohibited (Code 65).
No resource	Total number of registration requests denied by the home agent—insufficient resources (Code 66).
Bad lifetime	Total number of registration requests denied by the foreign agent—requested lifetime too long (Code 69).
Bad request form	Total number of registration requests denied by the home agent—poorly formed request (Code 70).
Unavailable encapsulation	Total number of registration requests denied by the home agent—unavailable encapsulation (Code 72).
Unavailable compression	Total number of registration requests denied by the foreign agent—requested Van Jacobson header compression unavailable (Code 73).
Unavailable reverse tunnel	Total number of registration requests denied by the home agent—reverse tunnel unavailable (Code 74).
Reverse tunnel mandatory	Total number of registration requests denied by the foreign agent—reverse tunnel is mandatory and the “T” bit is not set (Code 75).
Replies in	Total number of well-formed registration replies received by the foreign agent.
Forwarded	Total number of valid registration replies relayed to the mobile node by the foreign agent.
Bad	Total number of registration replies denied by the foreign agent—poorly formed reply (Code 71).
Ignored	Total number of registration replies ignored by the foreign agent.
Authentication failed MN	Total number of registration requests denied by the home agent—mobile node failed authentication (Code 67).
Authentication failed HA	Total number of registration replies denied by the foreign agent—home agent failed authentication (Code 68).
Received challenge/gen. authentication extension, feature not enabled	Total number of registration requests dropped by the foreign agent—received challenge/generalized-authentication extension in registration request but Mobile IP foreign agent challenge/response extension is not enabled.
Unknown challenge	Total number of registration requests denied by the foreign agent—unknown challenge (Code 104).
Missing Challenge	Total number of registration requests denied by the foreign agent—missing challenge (Code 105).
Stale Challenge	Total number of registration requests denied by the foreign agent—stale challenge (Code 106).

show ip mobile tunnel

To display active tunnels, use the **show ip mobile tunnel** command in EXEC mode.

show ip mobile tunnel [*interface*]

Syntax Description

interface	(Optional) Displays a particular tunnel interface. The *interface* argument is tunnel *x*.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(13)T	The output was enhanced to display route maps configured on the home agent.
12.2(15)T	The output was enhanced to display tunnel templates for multicast configured on the home agent or mobile router.
12.3(8)T	The output was enhanced to display UDP tunneling.
12.4(9)T	The command was enhanced to display information about multipath support.

Usage Guidelines

This command displays active tunnels created by Mobile IP. When no more users are on the tunnel, the tunnel is released.

Examples

The following is sample output from the **show ip mobile tunnel** command:

```
Router# show ip mobile tunnel

Mobile Tunnels:

Tunnel0:
 src 10.0.0.32, dest 10.0.0.48
 encap IP/IP, mode reverse-allowed, tunnel-users 1
 IP MTU 1480 bytes
 HA created, fast switching enabled, ICMP unreachable enabled
 0 packets input, 0 bytes, 0 drops
 1591241 packets output, 1209738478 bytes
 Route Map is: MoIPMap
Running template configuration for this tunnel:
ip pim sparse-dense-mode
```

The following is sample output from the **show ip mobile tunnel** command that verifies that UDP tunneling is established:

```
Router# show ip mobile tunnel

Mobile Tunnels:
Total mobile ip tunnels 1
Tunnel0:
```

```
    src 10.30.30.1, dest 10.10.10.100
    src port 434, dest port 434
    encap MIPUDP/IP, mode reverse-allowed, tunnel-users 1
    IP MTU 1480 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Ethernet2/3
    FA created, fast switching disabled, ICMP unreachable enabled
    5 packets input, 600 bytes, 0 drops
    7 packets output, 780 bytes
```

The following is sample output from the **show ip mobile tunnel** command that shows that the mobile node-home agent tunnel is still IP-in-IP, but that the foreign agent-home agent tunnel is UDP:

```
Router# show ip mobile tunnel

Mobile Tunnels:
Total mobile ip tunnels 2
Tunnel0:
 src 10.2.1.1, dest 10.99.100.2
 encap IP/IP, mode reverse-allowed, tunnel-users 1
 IP MTU 1460 bytes
 Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
 outbound interface Tunnel1
 HA created, fast switching enabled, ICMP unreachable enabled
 11 packets input, 1002 bytes, 0 drops
 5 packets output, 600 bytes

Tunnel1:
 src 10.2.1.1, dest 100.3.1.5
 src port 434, dest port 434
 encap MIPUDP/IP, mode reverse-allowed, tunnel-users 1
 IP MTU 1480 bytes
 Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
 outbound interface GigabitEthernet0/2
 HA created, fast switching disabled, ICMP unreachable enabled
 11 packets input, 1222 bytes, 0 drops
 7 packets output, 916 bytes
```

The following is sample output from the **show ip mobile tunnel** command that shows that the mobile node has UDP tunneling established with the home agent:

```
Router# show ip mobile tunnel

Total mobile ip tunnels 1
Tunnel0:
 src 10.10.10.100, dest 10.10.10.50
 src port 434, dest port 434
 encap MIPUDP/IP, mode reverse-allowed, tunnel-users 1
 IP MTU 1480 bytes
 Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
 outbound interface Ethernet2/1
 HA created, fast switching disabled, ICMP unreachable enabled
 5 packets input, 600 bytes, 0 drops
 5 packets output, 600 bytes
```

The following is sample output when the mobile router is configured for multipath support:

```
Router# show ip mobile tunnel

Mobile Tunnels:

Total mobile ip tunnels 1
Tunnel0:
    src 10.1.1.11, dest 10.1.1.10 Key 6
```

```
encap IP/IP, mode reverse-allowed, tunnel-users 1
IP MTU 1480 bytes
Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
outbound interface Ethernet1/0
MR created, fast switching enabled, ICMP unreachable enabled
4 packets input, 306 bytes, 0 drops
6 packets output, 436 bytes
Template configuration:
    ip pim sparse-dense-mode
```

Table 17 describes the significant fields shown in the display.

Table 17 show ip mobile tunnel Field Descriptions

Field	Description
src	Tunnel source IP address.
dest	Tunnel destination IP address.
Key	Identifies the tunnel when there are multiple tunnels between the same end points (source address and destination address) for multipath support. This situation can occur if a mobile router registers through foreign agents on different interfaces. All of the HA-MR tunnels would have the same end points.
encap	Tunnel encapsulation type.
mode	Either reverse-allowed or reverse-off for reverse tunnel mode.
tunnel-users	Number of users on the tunnel.
HA created	Entity that created the tunnel. This field can be one of three values: HA created, FA created, or MR created.
fast switching	Enabled or disabled.
ICMP unreachable	Enabled or disabled.
packets input	Number of packets in.
bytes	Number of bytes in.
drops	Number of packets dropped. Packets are dropped when there are no visitors to send to after the foreign agent deencapsulates incoming packets. This prevents loops because the foreign agent will otherwise route the de-encapsulated packets back to the home agent.
packets output	Number of packets output.
bytes	Number of bytes output.
Route Map is	Name of the route map.
Running template configuration	If tunnel templates for multicast are enabled or disabled, this information is displayed or absent, respectively.

Related Commands

Command	Description
show ip mobile binding	Displays the mobility binding table.
show ip mobile host	Displays mobile node information.
show ip mobile visitor	Displays the table that contains a visitor list of foreign agents.

show ip mobile violation

To display information about security violations, use the **show ip mobile violation** command in privileged EXEC mode.

show ip mobile violation [*address* | **nai** *string*]

Syntax Description

address	(Optional) Displays violations from a specific IP address.
nai *string*	(Optional) Network access identifier.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The **nai** keyword and associated parameters were added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

The most recent violation is saved for all the mobile nodes. A circular log holds up to 50 unknown requesters, which are the violators without security associations. The oldest violations will be purged to make room for new unknown requesters when the log limit is reached.

Security violation messages are logged at the informational level (see the **logging** global configuration command). When logging is enabled to include this severity level, violation history can be displayed using the **show logging** command.

Examples

The following is sample output from the **show ip mobile violation** command:

```
Router# show ip mobile violation
Security Violation Log:

Mobile Hosts:
20.0.0.1:
    Violations: 1, Last time: 06/18/97 01:16:47
    SPI: 300, Identification: B751B581.77FD0E40
    Error Code: MN failed authentication (131), Reason: Bad authenticator (2)
```

Table 18 describes significant fields shown in the display.

Table 18 show ip mobile violation Field Descriptions

Field	Description
IP address	IP address of the violator. The network access identifier (NAI) is displayed if configured.
Violations	Total number of security violations for this peer.
Last time	Time of the most recent security violation for this peer.

Table 18 show ip mobile violation Field Descriptions (continued)

Field	Description
SPI	SPI of the most recent security violation for this peer. If the security violation is due to an identification mismatch, then this is the SPI from the mobile-home authentication extension. If the security violation is due to an invalid authenticator, then this is the SPI from the offending authentication extension. In all other cases, it should be set to zero.
Identification	Identification used in request or reply of the most recent security violation for this peer.
Error Code	Error code in request or reply.
Reason Codes	Reason for the most recent security violation for this peer. Possible reasons are: • (1) No mobility security association • (2) Bad authenticator • (3) Bad identifier • (4) Bad SPI • (5) Missing security extension • (6) Other

show ip route vrf

To display the IP routing table associated with a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **show ip route vrf** command in user EXEC or privileged EXEC mode.

show ip route vrf *vrf-name* [**connected**] [*protocol* [*as-number*] [*tag*] [*output-modifiers*]] [*ip-prefix*] [**list** *number* [*output-modifiers*]] [**profile**] [**static** [*output-modifiers*]] [**summary** [*output-modifiers*]] [**supernets-only** [*output-modifiers*]]

Syntax Description

vrf-name	Name assigned to the VRF.
connected	(Optional) Displays all connected routes in a VRF.
protocol	(Optional) To specify a routing protocol, use one of the following keywords: **bgp**, **egp**, **eigrp**, **hello**, **igrp**, **isis**, **ospf**, or **rip**.
as-number	(Optional) Autonomous system number.
tag	(Optional) Cisco IOS routing area label.
output-modifiers	(Optional) For a list of associated keywords and arguments, use context-sensitive help.
ip-prefix	(Optional) Specifies a network to display.
list *number*	(Optional) Specifies the IP access list to display.
profile	(Optional) Displays the IP routing table profile.
static	(Optional) Displays static routes.
summary	(Optional) Displays a summary of routes.
supernets-only	(Optional) Displays supernet entries only.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(2)T	The *ip-prefix* argument was added. The output from the **show ip route vrf** *vrf-name ip-prefix* command was enhanced to display information on the multipaths to the specified network.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(22)S	Enhanced Interior Gateway Routing Protocol (EIGRP) VRF support was added.
12.2(15)T	EIGRP VRF support was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	EIGRP VRF support was integrated into Cisco IOS Release 12.2(18)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	The output was enhanced to display remote label information and corresponding MPLS flags for prefixes that have remote labels stored in the Routing Information Base (RIB).

Usage Guidelines

This command displays specified information from the IP routing table of a VRF.

Examples

This example shows the IP routing table associated with the VRF named vrf1:

```
Router# show ip route vrf vrf1

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
       T - traffic engineered route

Gateway of last resort is not set

B    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:19
C    10.0.0.0/8 is directly connected, Ethernet1/3
B    10.0.0.0/8 [20/0] via 10.0.0.1, 02:10:22
B    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:20
```

This example shows BGP entries in the IP routing table associated with the VRF named vrf1:

```
Router# show ip route vrf vrf1 bgp

B  10.0.0.0/8 [200/0] via 10.13.13.13, 03:44:14
B  10.0.0.0/8 [20/0] via 10.0.0.1, 03:44:12
B  10.0.0.0/8 [200/0] via 10.13.13.13, 03:43:14
```

This example shows the IP routing table associated with a VRF named PATH and network 10.22.22.0:

```
Router# show ip route vrf PATH 10.22.22.0

Routing entry for 10.22.22.0/24
  Known via "bgp 1", distance 200, metric 0
  Tag 22, type internal
  Last update from 10.22.5.10 00:01:07 ago
  Routing Descriptor Blocks:
  * 10.22.7.8 (Default-IP-Routing-Table), from 10.11.3.4, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.1.9 (Default-IP-Routing-Table), from 10.11.1.2, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.6.10 (Default-IP-Routing-Table), from 10.11.6.7, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.4.10 (Default-IP-Routing-Table), from 10.11.4.5, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.5.10 (Default-IP-Routing-Table), from 10.11.5.6, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
```

Table 19 describes the significant fields shown when the **show ip route vrf** *vrf-name ip-prefix* command is used.

Table 19 show ip route vrf Field Descriptions

Field	Description
Routing entry for 10.22.22.0/24	Network number.
Known via ...	Indicates how the route was derived.
distance	Administrative distance of the information source.
metric	The metric to reach the destination network.
Tag	Integer that is used to implement the route.
type	Indicates that the route is an L1 type or L2 type route.
Last update from 10.22.5.10	Indicates the IP address of a router that is the next hop to the remote network and the router interface on which the last update arrived.
00:01:07 ago	Specifies the last time the route was updated (in hours:minutes:seconds).
Routing Descriptor Blocks:	Displays the next hop IP address followed by the information source.
10.22.6.10, from 10.11.6.7, 00:01:07 ago	Indicates the next hop address, the address of the gateway that sent the update, and the time that has elapsed since this update was received (in hours:minutes:seconds).
Route metric	This value is the best metric for this routing descriptor block.
traffic share count	Number of uses for this routing descriptor block.
AS Hops	Number of hops to the destination or to the router where the route first enters internal BGP (iBGP).

Example of Output Using the Cisco IOS Software Modularity for Layer 3 VPNs Feature

The following is sample output from the **show ip route vrf** command on routers using the Cisco IOS Software Modularity for Layer 3 VPNs feature. The output includes remote label information and corresponding MPLS flags for prefixes that have remote labels stored in the RIB, if BGP is the label distribution protocol:

```
Router# show ip route vrf v2 10.2.2.2

Routing entry for 10.2.2.2/32
  Known via "bgp 1", distance 200, metric 0, type internal
  Redistributing via ospf 2
  Advertised by ospf 2 subnets
  Last update from 10.0.0.4 00:22:59 ago
  Routing Descriptor Blocks:
  * 10.0.0.4 (Default-IP-Routing-Table), from 10.0.0.31, 00:22:59 ago
      Route metric is 0, traffic share count is 1
      AS Hops 0
      MPLS label: 1300
      MPLS Flags: MPLS Required
```

Table 20 describes the significant fields shown in the display.

Table 20 show ip route vrf Field Descriptions

Field	Description
MPLS label	Displays the BGP prefix from the BGP peer. The output shows one of the following values: • A label value (16 - 1048575) • A reserved label value, such as explicit-null or implicit-null • The word “none” if no label is received from the peer The MPLS label field does not display if any of the following conditions is true: • BGP is not the LDP. However, OSPF prefixes learned via sham link display an MPLS label. • MPLS is not supported. • The prefix was imported from another VRF, where the prefix was an IGP prefix and LDP provided the remote label for it.
MPLS Flags	The name of one of the following MPLS flags is displayed if any is set: • MPLS Required—Packets are forwarded to this prefix because the MPLS label stack is present. If MPLS is disabled in the outgoing interface, the packets are dropped. • No Global—MPLS packets for this prefix are forwarded from the VRF interface, not from the interface in global table. Using the VRF interface prevents loops in scenarios that use ieBGP multipath. • NSF—The prefix is from an NSF-aware neighbor. If the routing information temporarily disappears due to a disruption in the control plane, packets for this prefix are preserved.

Related Commands

Command	Description
show ip cache	Displays the Cisco Express Forwarding table associated with a VRF.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

snmp-server enable traps ipmobile

To enable Simple Network Management Protocol (SNMP) security notifications for Mobile IP, use the **snmp-server enable traps ipmobile** command in global configuration mode. To disable SNMP notifications for Mobile IP, use the **no** form of this command.

snmp-server enable traps ipmobile

no snmp-server enable traps ipmobile

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

SNMP Mobile IP notifications can be sent as traps or inform requests. This command enables both traps and inform requests. This command enables Mobile IP Authentication Failure notifications. This notification is defined in RFC2006-MIB.my as the mipAuthFailure notification type {mipMIBNotifications 1}. This notification, when enabled, is triggered when there is an authentication failure for the Mobile IP entity during validation of the mobile registration request or reply.

For a complete description of this notification and additional MIB functions, see the RFC2006-MIB.my file, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

The **snmp-server enable traps ipmobile** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** global configuration command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example enables the router to send Mobile IP informs to the host at the address myhost.cisco.com using the community string defined as public:

```
snmp-server enable traps ipmobile
snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

standby track decrement priority

To lower the priority of an particular HA in a redundancy scenario, use the **standby track** *tracking object id* **decrement** *priority* command in global configuration mode. To disable this function, use the **no** form of the command.

standby track *tracking object id* **decrement** *priority*

no standby track *tracking object id* **decrement** *priority*

Syntax Description

tracking object id	The name of the specific tracking object.
priority	Specifies the priority level.

Defaults

There are no default values.

Command Modes

Global Configuration

Command History

Release	Modification
12.3(14)YX	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

track id application home-agent

To create a tracking object to track the home-agent state, use the **track** *tracking object id* **application home-agent** command in global configuration. To disable this feature, use the **no** form of the command.

track *tracking object id* **application home-agent**

no track *tracking object id* **application home-agent**

Syntax Description

tracking object id	The name of the specific tracking object.

Defaults

There are no default values.

Command Modes

Global Configuration

Command History

Release	Modification
12.3(14)YX	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Examples

The following example illustrates the **track application home-agent** command:

```
router# track tracking object id application home-agent
```

virtual

To configure virtual server attributes, use the **virtual** command in SLB virtual server configuration mode. To remove the attributes, use the **no** form of this command.

Encapsulation Security Payload (ESP) and Generic Routing Encapsulation (GRE) Protocols

virtual *ip-address* [*netmask* [**group**]] {**esp** | **gre** | *protocol*}

no virtual *ip-address* [*netmask* [**group**]] {**esp** | **gre** | *protocol*}

TCP and User Datagram Protocol (UDP)

virtual *ip-address* [*netmask* [**group**]] {**tcp** | **udp**} [*port* | **any**] [**service** *service*]

no virtual *ip-address* [*netmask* [**group**]] {**tcp** | **udp**} [*port* | **any**] [**service** *service*]

Syntax Description

ip-address	IP address for this virtual server instance, used by clients to connect to the server farm.
netmask	(Optional) IP network mask for transparent web cache load balancing. The default is 0.0.0.0 (all subnets).
group	(Optional) Allows the virtual subnet to be advertised. If you do not specify the **group** keyword, the virtual subnet cannot be advertised.
esp	Performs load balancing for only Encapsulation Security Payload (ESP) connections.
gre	Performs load balancing for only Generic Routing Encapsulation (GRE) connections.
protocol	Protocol for which load balancing is performed. The valid range is 2 to 127.
tcp	Performs load balancing for only TCP connections.
udp	Performs load balancing for only User Datagram Protocol (UDP) connections.

port	(Optional) IOS Server Load Balancing (IOS SLB) virtual port (the TCP or UDP port number or port name). If specified, only the connections for the specified port on the server are load-balanced. The ports and the valid name or number for the *port* argument are as follows: • All ports: **any 0** • Connectionless secure Wireless Session Protocol (WSP): **wsp-wtls 9202** • Connectionless WSP: **wsp 9200** • Connection-oriented secure WSP: **wsp-wtp-wtls 9203** • Connection-oriented WSP: **wsp-wtp 9201** • Domain Name System: **dns 53** • File Transfer Protocol: **ftp 21** • General packet radio service (GPRS) tunneling protocol (GTP): **gtp 3386** • HTTP over Secure Socket Layer: **https 443** • Internet Key Exchange (IKE): **isakmp 500** • Mapping of airline traffic over IP, Type A: **matip-a 350** • Network News Transport Protocol: **nntp 119** • Post Office Protocol v2: **pop2 109** • Post Office Protocol v3: **pop3 110** • Simple Mail Transport Protocol: **smtp 25** • Telnet: **telnet 23** • X.25 over TCP (XOT): **xot 1998** • World Wide Web (HTTP): **www 80** Specify a port number of 0 to configure an all-port virtual server (that is, a virtual server that accepts flows destined for all ports except GTP ports).
any	(Optional) Performs load balancing on all ports.
service *service*	(Optional) Couples connections associated with a given service, such as HTTP or Telnet, so all related connections from the same client use the same real server. The following are the valid types of connection coupling: • **ftp**—Couples FTP data connections with the control session that created them. • **gtp**—Enables GPRS load balancing without general packet radio service (GPRS) tunneling protocol (GTP) cause code inspection enabled, which allows load-balancing decisions to be made using Layer 5 information. You can balance UDP flows without awareness of GTP by omitting the **service gtp** keywords. • **gtp-inspect**—Enables GPRS load balancing with GTP cause code inspection enabled. • **ipmobile**—Enables the Home Agent Director. • **per-packet**—Does not maintain connection objects for packets destined for this virtual server. • **radius**—Enables IOS SLB to build RADIUS session objects for RADIUS load balancing.

Defaults No default behavior or values.

Command Modes SLB virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.1(5a)E	The **wsp**, **wsp-wtp**, **wsp-wtls**, and **wsp-wtp-wtls** keywords were added.
12.1(9)E	The **gtp** option was added as a new value on the *service* argument.
12.1(11b)E	The following keywords, arguments, and options were added: • The **esp**, **gre**, and **all** keywords • The *protocol* argument • The **isakmp** option on the *port* argument • The **per-packet** and **radius** options on the *service* argument The **wsp**, **wsp-wtp**, **wsp-wtls**, and **wsp-wtp-wtls** keywords were changed to options for the *port* argument.
12.1(12c)E	The **group** keyword was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.1(13)E3	The **gtp-inspect** option was added as a new value on the *service* argument.
12.2(14)ZA2	The **ipmobile** option was added as a new value on the *service* argument.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines The **no virtual** command is allowed only if the virtual server was removed from service by the **no inservice** command.

For some applications, it is not feasible to configure all the virtual server TCP or UDP port numbers for IOS SLB. To support such applications, you can configure IOS SLB virtual servers to accept flows destined for all ports. To configure an all-port virtual server, specify a port number of 0 or any.

Note In general, you should use port-bound virtual servers instead of all-port virtual servers. When you use all-port virtual servers, flows can be passed to servers for which no application port exists. When servers reject these flows, IOS SLB might fail the server and remove it from load balancing.

Specifying port 9201 for connection-oriented WSP mode also activates the Wireless Application Protocol (WAP) finite state machine (FSM), which monitors WSP and drives the session FSM accordingly.

In RADIUS load balancing, IOS SLB maintains session objects in a database to ensure that re-sent RADIUS requests are load-balanced to the same real server.

Examples

The following example specifies that the virtual server with the IP address 10.0.0.1 performs load balancing for TCP connections for the port named www. The virtual server processes HTTP requests.

```
Router(config)# ip slb vserver PUBLIC_HTTP
Router(config-slb-vserver)# virtual 10.0.0.1 tcp www
```

The following example specifies that the virtual server with the IP address 10.0.0.13 performs load balancing for UDP connections for all ports. The virtual server processes HTTP requests.

```
Router(config)# ip slb vserver PUBLIC_HTTP
Router(config-slb-vserver)# virtual 10.0.0.13 udp 0
```

Related Commands

Command	Description
ip slb vserver	Identifies a virtual server.
show ip slb vservers	Displays information about the virtual servers defined to IOS Server Load Balancing (IOS SLB).