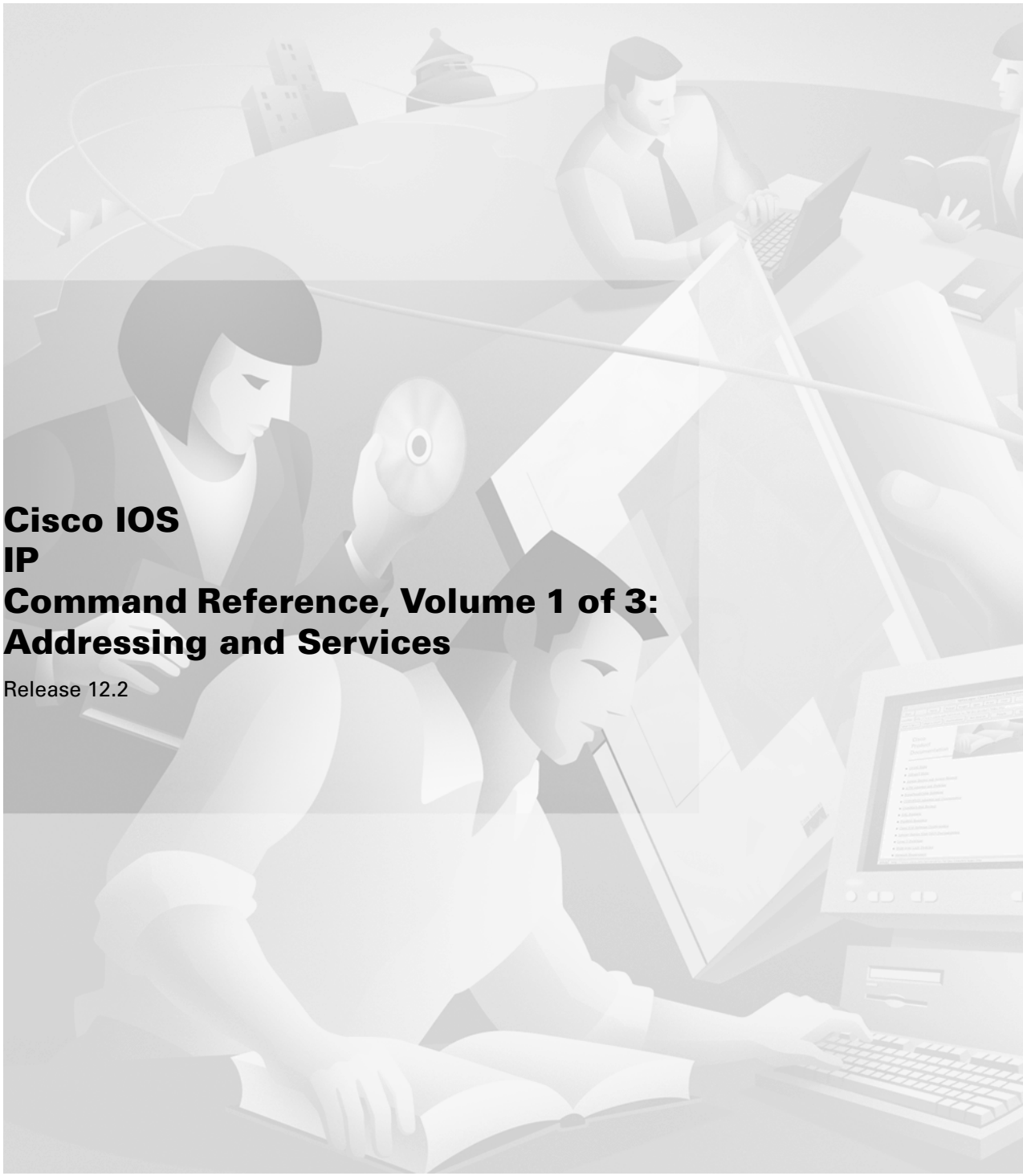


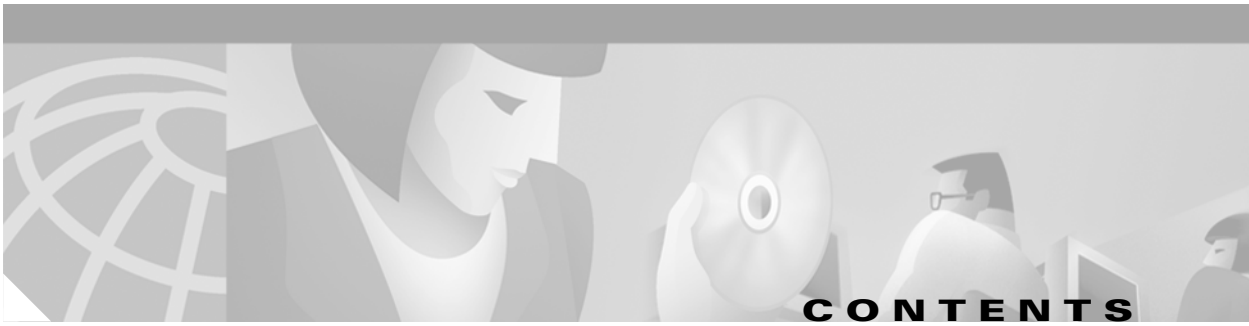
Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services

Release 12.2

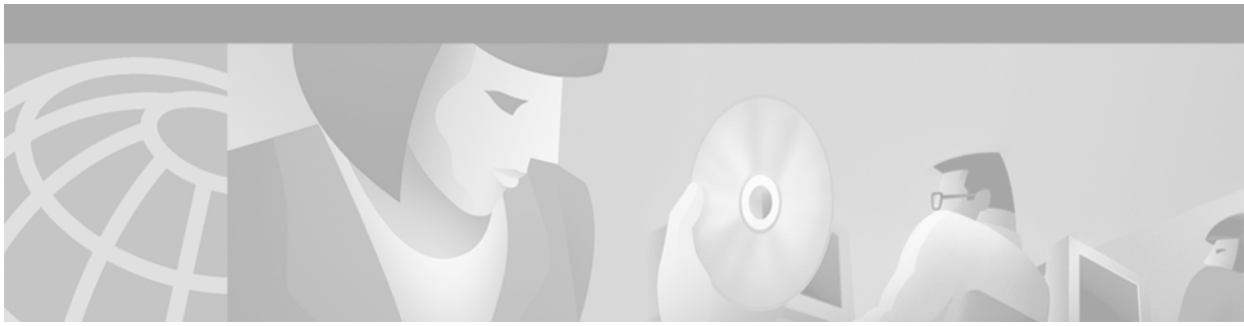
Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-7811742=
Text Part Number: 78-11742-02

Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services



CONTENTS



About Cisco IOS Software Documentation

This chapter discusses the objectives, audience, organization, and conventions of Cisco IOS software documentation. It also provides sources for obtaining documentation from Cisco Systems.

Documentation Objectives

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

Audience

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

Documentation Organization

The Cisco IOS software documentation set consists of documentation modules and master indexes. In addition to the main documentation set, there are supporting documents and resources.

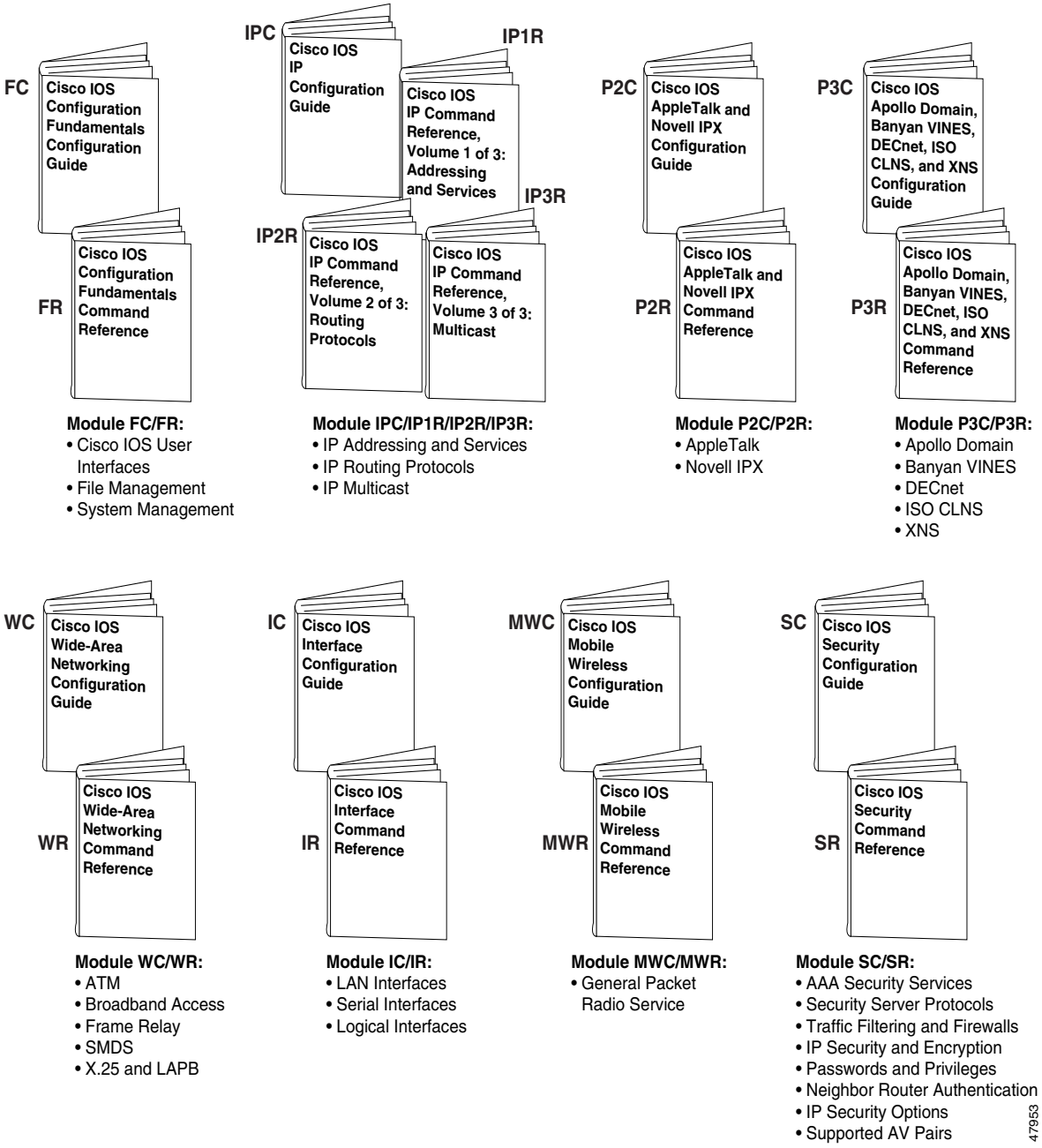
Documentation Modules

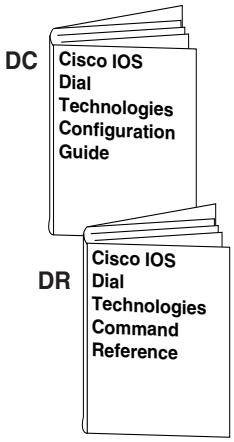
The Cisco IOS documentation modules consist of configuration guides and corresponding command reference publications. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality and contain comprehensive configuration examples. Chapters in a command reference publication provide complete Cisco IOS command syntax information. Use each configuration guide in conjunction with its corresponding command reference publication.

Figure 1 shows the Cisco IOS software documentation modules.

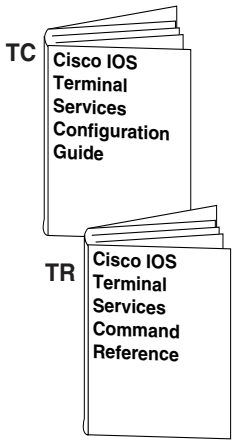
Note The abbreviations (for example, FC and FR) next to the book icons are page designators, which are defined in a key in the index of each document to help you with navigation. The bullets under each module list the major technology areas discussed in the corresponding books.

Figure 1 Cisco IOS Software Documentation Modules

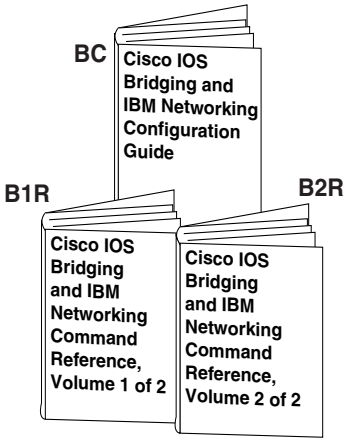




Module DC/DR:
- Preparing for Dial Access
- Modem and Dial Shelf Configuration and Management
- ISDN Configuration
- Signalling Configuration
- Dial-on-Demand Routing Configuration
- Dial-Backup Configuration
- Dial-Related Addressing Services
- Virtual Templates, Profiles, and Networks
- PPP Configuration
- Callback and Bandwidth Allocation Configuration
- Dial Access Specialized Features
- Dial Access Scenarios

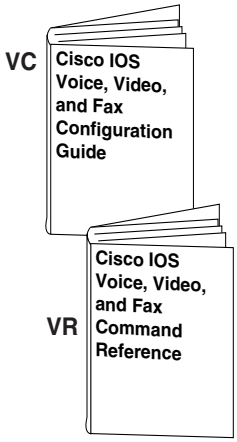


Module TC/TR:
- ARA
- LAT
- NASI
- Telnet
- TN3270
- XRemote
- X.28 PAD
- Protocol Translation

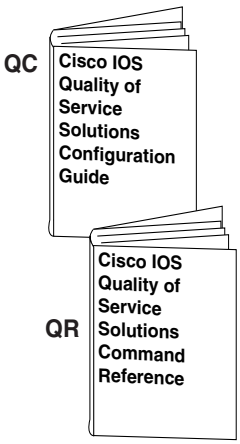


Module BC/B1R:
- Transparent Bridging
- SRB
- Token Ring Inter-Switch Link
- Token Ring Route Switch Module
- RSRB
- DLSw+
- Serial Tunnel and Block Serial Tunnel
- LLC2 and SDLC
- IBM Network Media Translation
- SNA Frame Relay Access
- NCIA Client/Server
- Airline Product Set

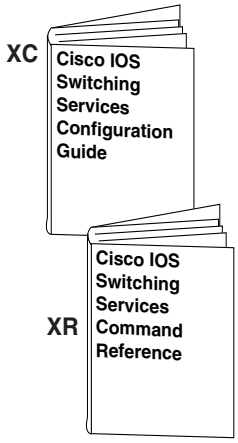
Module BC/B2R:
- DSPU and SNA Service Point
- SNA Switching Services
- Cisco Transaction Connection
- Cisco Mainframe Channel Connection
- CLAW and TCP/IP Offload
- CSNA, CMPC, and CMPC+
- TN3270 Server



Module VC/VR:
- Voice over IP
- Call Control Signalling
- Voice over Frame Relay
- Voice over ATM
- Telephony Applications
- Trunk Management
- Fax, Video, and Modem Support



Module QC/QR:
- Packet Classification
- Congestion Management
- Congestion Avoidance
- Policing and Shaping
- Signalling
- Link Efficiency Mechanisms



Module XC/XR:
- Cisco IOS Switching Paths
- NetFlow Switching
- Multiprotocol Label Switching
- Multilayer Switching
- Multicast Distributed Switching
- Virtual LANs
- LAN Emulation

47954

Master Indexes

Two master indexes provide indexing information for the Cisco IOS software documentation set: an index for the configuration guides and an index for the command references. Individual books also contain a book-specific index.

The master indexes provide a quick way for you to find a command when you know the command name but not which module contains the command. When you use the online master indexes, you can click the page number for an index entry and go to that page in the online document.

Supporting Documents and Resources

The following documents and resources support the Cisco IOS software documentation set:

- *Cisco IOS Command Summary* (two volumes)—This publication explains the function and syntax of the Cisco IOS software commands. For more information about defaults and usage guidelines, refer to the Cisco IOS command reference publications.
- *Cisco IOS System Error Messages*—This publication lists and describes Cisco IOS system error messages. Not all system error messages indicate problems with your system. Some are purely informational, and others may help diagnose problems with communications lines, internal hardware, or the system software.
- *Cisco IOS Debug Command Reference*—This publication contains an alphabetical listing of the **debug** commands and their descriptions. Documentation for each command includes a brief description of its use, command syntax, usage guidelines, and sample output.
- *Dictionary of Internetworking Terms and Acronyms*—This Cisco publication compiles and defines the terms and acronyms used in the internetworking industry.
- New feature documentation—The Cisco IOS software documentation set documents the mainline release of Cisco IOS software (for example, Cisco IOS Release 12.2). New software features are introduced in early deployment releases (for example, the Cisco IOS "T" release train for 12.2, 12.2(x)T). Documentation for these new features can be found in standalone documents called "feature modules." Feature module documentation describes new Cisco IOS software and hardware networking functionality and is available on Cisco.com and the Documentation CD-ROM.
- Release notes—This documentation describes system requirements, provides information about new and changed features, and includes other useful information about specific software releases. See the section "Using Software Release Notes" in the chapter "Using Cisco IOS Software" for more information.
- Caveats documentation—This documentation provides information about Cisco IOS software defects in specific software releases.
- RFCs—RFCs are standards documents maintained by the Internet Engineering Task Force (IETF). Cisco IOS software documentation references supported RFCs when applicable. The full text of referenced RFCs may be obtained on the World Wide Web at http://www.rfc-editor.org/.
- MIBs—MIBs are used for network monitoring. For lists of supported MIBs by platform and release, and to download MIB files, see the Cisco MIB website on Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

New and Changed Information

The following is new or changed information since the last release of the Cisco IOS IP and IP routing publications:

- The title of the *Cisco IOS IP and IP Routing Configuration Guide* has been changed to *Cisco IOS IP Configuration Guide*.
- The *Cisco IOS IP and IP Routing Command Reference* has been divided into three separate publications with the following titles:
  - *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*
  - *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*
  - *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*
- The following new chapters were added to the *Cisco IOS IP Configuration Guide*:
  - "Configuring Server Load Balancing"
  - "Configuring Source Specific Multicast"
  - "Configuring Bidirectional PIM"
  - "Configuring Router-Port Group Management Protocol"
- The following new chapter was added to the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*:
  - "Server Load Balancing Commands"

Document Conventions

Within Cisco IOS software documentation, the term *router* is generally used to refer to a variety of Cisco products (for example, routers, access servers, and switches). Routers, access servers, and other networking devices that support Cisco IOS software are shown interchangeably within examples. These products are used only for illustrative purposes; that is, an example that shows one product does not necessarily indicate that other products are not supported.

The Cisco IOS documentation set uses the following conventions:

Convention	Description
^ or Ctrl	The ^ and Ctrl symbols represent the Control key. For example, the key combination ^D or Ctrl-D means 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 an SNMP community string to public, do not use quotation marks around the string or the string will include the quotation marks.

Command syntax descriptions use the following conventions:

Convention	Description
boldface	Boldface text indicates commands and keywords that you enter literally as shown.
italics	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional element (keyword or argument).
|	A vertical line indicates a choice within an optional or required set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example:

Convention	Description
[x {y | z}]	Braces and a vertical line within square brackets indicate a required choice within an optional element.

Examples use the following conventions:

Convention	Description
`screen`	Examples of information displayed on the screen are set in Courier font.
`boldface screen`	Examples of text that you must enter are set in Courier bold font.
< >	Angle brackets enclose text that is not printed to the screen, such as passwords.
!	An exclamation point at the beginning of a line indicates a comment line. (Exclamation points are also displayed by the Cisco IOS software for certain processes.)
[ ]	Square brackets enclose default responses to system prompts.

The following conventions are used to attract the attention of the reader:

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 materials not contained in this manual.

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

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

The most current Cisco documentation is available on the World Wide Web at the following website:

http://www.cisco.com

Translated documentation is available at the following website:

http://www.cisco.com/public/countries_languages.html

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation can be ordered in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

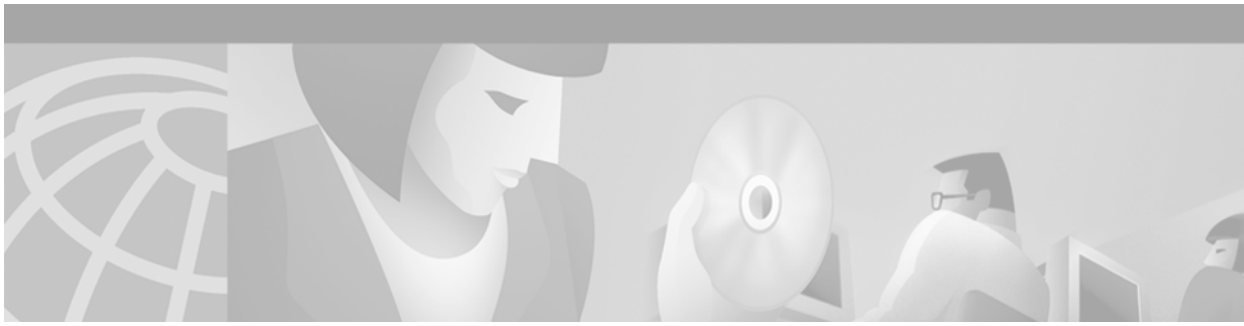
Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.



Using Cisco IOS Software

This chapter provides helpful tips for understanding and configuring Cisco IOS software using the command-line interface (CLI). It contains the following sections:

- Understanding Command Modes
- Getting Help
- Using the no and default Forms of Commands
- Saving Configuration Changes
- Filtering Output from the show and more Commands
- Identifying Supported Platforms

For an overview of Cisco IOS software configuration, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information on the conventions used in the Cisco IOS software documentation set, see the chapter "About Cisco IOS Software Documentation" located at the beginning of this book.

Understanding Command Modes

You use the CLI to access Cisco IOS software. Because the CLI is divided into many different modes, the commands available to you at any given time depend on the mode you are currently in. Entering a question mark (**?**) at the CLI prompt allows you to obtain a list of commands available for each command mode.

When you log in to the CLI, you are in user EXEC mode. User EXEC mode contains only a limited subset of commands. To have access to all commands, you must enter privileged EXEC mode, normally by using a password. From privileged EXEC mode you can issue any EXEC command—user or privileged mode—or you can enter global configuration mode. Most EXEC commands are one-time commands. For example, **show** commands show important status information, and **clear** commands clear counters or interfaces. The EXEC commands are not saved when the software reboots.

Configuration modes allow you to make changes to the running configuration. If you later save the running configuration to the startup configuration, these changed commands are stored when the software is rebooted. To enter specific configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and a variety of other modes, such as protocol-specific modes.

ROM monitor mode is a separate mode used when the Cisco IOS 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.

Table 1 describes how to access and exit various common command modes of the Cisco IOS software. It also shows examples of the prompts displayed for each mode.

Table 1 Accessing and Exiting Command Modes

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	`Router>`	Use the **logout** command.
Privileged EXEC	From user EXEC mode, use the **enable** EXEC command.	`Router#`	To return to user EXEC mode, use the **disable** command.
Global configuration	From privileged EXEC mode, use the **configure terminal** privileged EXEC command.	`Router(config)#`	To return to privileged EXEC mode from global configuration mode, use the **exit** or **end** command, or press **Ctrl-Z**.
Interface configuration	From global configuration mode, specify an interface using an **interface** command.	`Router(config-if)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command, or press **Ctrl-Z**.
ROM monitor	From privileged EXEC mode, use the **reload** EXEC command. Press the **Break** key during the first 60 seconds while the system is booting.	`>`	To exit ROM monitor mode, use the **continue** command.

For more information on command modes, refer to the "Using the Command-Line Interface" chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Getting Help

Entering a question mark (**?**) at the CLI prompt displays a list of commands available for each command mode. You can also get a list of keywords and arguments associated with any command by using the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, use one of the following commands:

Command	Purpose
help	Provides a brief description of the help system in any command mode.
*abbreviated-command-entry***?**	Provides a list of commands that begin with a particular character string. (No space between command and question mark.)
abbreviated-command-entry<**Tab**>	Completes a partial command name.
?	Lists all commands available for a particular command mode.
command **?**	Lists the keywords or arguments that you must enter next on the command line. (Space between command and question mark.)

Example: How to Find Command Options

This section provides an example of how to display syntax for a command. The syntax can consist of optional or required keywords and arguments. To display keywords and arguments for a command, enter a question mark (**?**) at the configuration prompt or after entering part of a command followed by a space. The Cisco IOS software displays a list and brief description of available keywords and arguments. For example, if you were in global configuration mode and wanted to see all the keywords or arguments for the **arap** command, you would type **arap ?**.

The <cr> symbol in command help output stands for "carriage return." On older keyboards, the carriage return key is the Return key. On most modern keyboards, the carriage return key is the Enter key. The <cr> symbol at the end of command help output indicates that you have the option to press **Enter** to complete the command and that the arguments and keywords in the list preceding the <cr> symbol are optional. The <cr> symbol by itself indicates that no more arguments or keywords are available and that you must press **Enter** to complete the command.

Table 2 shows examples of how you can use the question mark (**?**) to assist you in entering commands. The table steps you through configuring an IP address on a serial interface on a Cisco 7206 router that is running Cisco IOS Release 12.0(3).

Table 2 How to Find Command Options

Command	Comment

`Router> enable`
`Password: <password>`
`Router#`
	Enter the **enable** command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to `Router#`.

`Router# configure terminal`
`Enter configuration commands, one per line. End with CNTL/Z.`
`Router(config)#`
	Enter the **configure terminal** privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to `Router(config)#`.

`Router(config)# interface serial ?`
`  <0-6>  Serial interface number`
`Router(config)# interface serial 4 ?`
`  /`
`Router(config)# interface serial 4/ ?`
`  <0-3>  Serial interface number`
`Router(config)# interface serial 4/0`
`Router(config-if)#`
	Enter interface configuration mode by specifying the serial interface that you want to configure using the **interface serial** global configuration command.
	Enter **?** to display what you must enter next on the command line. In this example, you must enter the serial interface slot number and port number, separated by a forward slash.
	You are in interface configuration mode when the prompt changes to `Router(config-if)#`.

Table 2 How to Find Command Options (continued)

Command	Comment

`Router(config-if)# ?`
`Interface configuration commands:`
`  .`
`  .`
`  .`
`  ip  Interface Internet Protocol config commands`
`  keepalive  Enable keepalive`
`  lan-name  LAN Name command`
`  llc2  LLC2 Interface Subcommands`
`  load-interval  Specify interval for load calculation for an interface`
`  locaddr-priority  Assign a priority group`
`  logging  Configure logging for interface`
`  loopback  Configure internal loopback on an interface`
`  mac-address  Manually set interface MAC address`
`  mls  mls router sub/interface commands`
`  mpoa  MPOA interface configuration commands`
`  mtu  Set the interface Maximum Transmission Unit (MTU)`
`  netbios  Use a defined NETBIOS access list or enable name-caching`
`  no  Negate a command or set its defaults`
`  nrzi-encoding  Enable use of NRZI encoding`
`  ntp  Configure NTP`
`  .`
`  .`
`  .`
`Router(config-if)#`
	Enter **?** to display a list of all the interface configuration commands available for the serial interface. This example shows only some of the available interface configuration commands.

`Router(config-if)# ip ?`
`Interface IP configuration subcommands:`
`  access-group  Specify access control for packets`
`  accounting  Enable IP accounting on this interface`
`  address  Set the IP address of an interface`
`  authentication  authentication subcommands`
`  bandwidth-percent  Set EIGRP bandwidth limit`
`  broadcast-address  Set the broadcast address of an interface`
`  cgmp  Enable/disable CGMP`
`  directed-broadcast  Enable forwarding of directed broadcasts`
`  dvmrp  DVMRP interface commands`
`  hello-interval  Configures IP-EIGRP hello interval`
`  helper-address  Specify a destination address for UDP broadcasts`
`  hold-time  Configures IP-EIGRP hold time`
`  .`
`  .`
`  .`
`Router(config-if)# ip`
	Enter the command that you want to configure for the interface. This example uses the **ip** command.
	Enter **?** to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.

Table 2 How to Find Command Options (continued)

Command	Comment

`Router(config-if)# ip address ?`
`  A.B.C.D  IP address`
`  negotiated  IP Address negotiated over PPP`
`Router(config-if)# ip address`
	Enter the command that you want to configure for the interface. This example uses the **ip address** command.
	Enter **?** to display what you must enter next on the command line. In this example, you must enter an IP address or the **negotiated** keyword.
	A carriage return (<cr>) is not displayed; therefore, you must enter additional keywords or arguments to complete the command.

`Router(config-if)# ip address 172.16.0.1 ?`
`  A.B.C.D  IP subnet mask`
`Router(config-if)# ip address 172.16.0.1`
	Enter the keyword or argument you want to use. This example uses the 172.16.0.1 IP address.
	Enter **?** to display what you must enter next on the command line. In this example, you must enter an IP subnet mask.
	A <cr> is not displayed; therefore, you must enter additional keywords or arguments to complete the command.

`Router(config-if)# ip address 172.16.0.1 255.255.255.0 ?`
`  secondary  Make this IP address a secondary address`
`  <cr>`
`Router(config-if)# ip address 172.16.0.1 255.255.255.0`
	Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask.
	Enter **?** to display what you must enter next on the command line. In this example, you can enter the **secondary** keyword, or you can press **Enter**.
	A <cr> is displayed; you can press **Enter** to complete the command, or you can enter another keyword.

`Router(config-if)# ip address 172.16.0.1 255.255.255.0` `Router(config-if)#`	In this example, Enter is pressed to complete the command.

Using the no and default Forms of Commands

Almost every configuration command has a **no** form. In general, use the **no** form to disable a function. Use the command without the **no** keyword to reenable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, use the **no ip routing** command; to reenable IP routing, use the **ip routing** command. The Cisco IOS software command reference publications provide the complete syntax for the configuration commands and describe what the **no** form of a command does.

Configuration commands also can have a **default** form, which returns the command settings to the default values. Most commands are disabled by default, so in such cases using the **default** form has the same result as using the **no** form of the command. However, some commands are enabled by default and

have variables set to certain default values. In these cases, the **default** form of the command enables the command and sets the variables to their default values. The Cisco IOS software command reference publications describe the effect of the **default** form of a command if the command functions differently than the **no** form.

Saving Configuration Changes

Use the **copy system:running-config nvram:startup-config** command to save your configuration changes to the startup configuration so that the changes will not be lost if the software reloads or a power outage occurs. For example:

```
Router# copy system:running-config nvram:startup-config
Building configuration...
```

It might take a minute or two to save the configuration. After the configuration has been saved, the following output appears:

```
[OK]
Router#
```

On most platforms, this task saves the configuration to NVRAM. On the Class A Flash file system platforms, this task saves the configuration to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

Filtering Output from the show and more Commands

In Cisco IOS Release 12.0(1)T and later releases, you can search and filter the output of **show** and **more** commands. This functionality is useful if you need to sort through large amounts of output or if you want to exclude output that you need not see.

To use this functionality, enter a **show** or **more** command followed by the "pipe" character (|); one of the keywords **begin**, **include**, or **exclude**; and a regular expression on which you want to search or filter (the expression is case-sensitive):

command **|** {**begin | include | exclude**} *regular-expression*

The output matches certain lines of information in the configuration file. The following example illustrates how to use output modifiers with the **show interface** command when you want the output to include only lines in which the expression "protocol" appears:

```
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
```

For more information on the search and filter functionality, refer to the "Using the Command-Line Interface" chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Identifying Supported Platforms

Cisco IOS software is packaged in feature sets consisting of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a release. To identify the set of software images available in a specific release or to find out if a feature is available in a given Cisco IOS software image, see the following sections:

- Using Feature Navigator
- Using Software Release Notes

Using Feature Navigator

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image.

Feature Navigator is available 24 hours a day, 7 days a week. To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at cdbadmin@cisco.com. If you do not have an account on Cisco.com, go to http://www.cisco.com/register and follow the directions to establish an account.

To use Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. You can access Feature Navigator at the following URL:

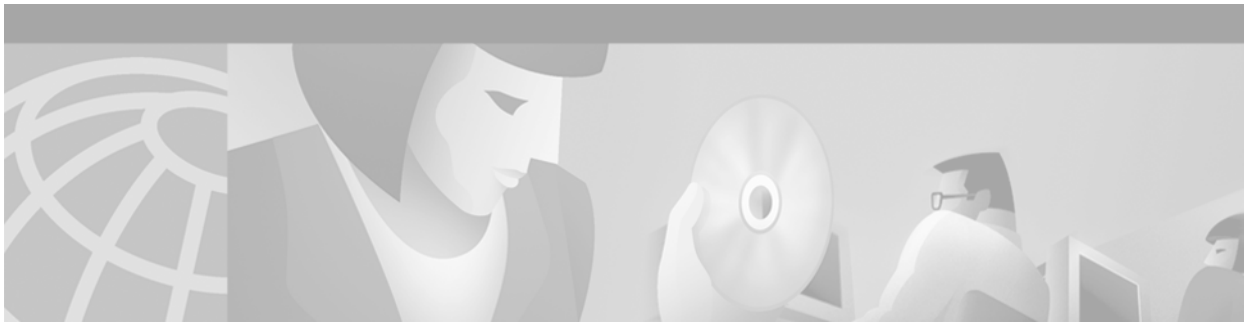
http://www.cisco.com/go/fn

Using Software Release Notes

Cisco IOS software releases include release notes that provide the following information:

- Platform support information
- Memory recommendations
- Microcode support information
- Feature set tables
- Feature descriptions
- Open and resolved severity 1 and 2 caveats for all platforms

Release notes are intended to be release-specific for the most current release, and the information provided in these documents may not be cumulative in providing information about features that first appeared in previous releases.



IP Addressing Commands

The Internet Protocol (IP) is a packet-based protocol used to exchange data over computer networks. IP handles addressing, fragmentation, reassembly, and protocol demultiplexing. It is the foundation on which all other Internet protocols, collectively referred to as the *Internet Protocol suite*, are built. IP is a network-layer protocol that contains addressing information and some control information that allows data packets to be routed.

The Transmission Control Protocol (TCP) is built upon the IP layer. TCP is a connection-oriented protocol that specifies the format of data and acknowledgments used in the transfer of data. TCP also specifies the procedures that the computers use to ensure that the data arrives correctly. TCP allows multiple applications on a system to communicate concurrently because it handles all demultiplexing of the incoming traffic among the application programs.

Use the commands in this chapter to configure and monitor the addressing of IP networks. For IP addressing configuration information and examples, refer to the "Configuring IP Addressing" chapter of the *Cisco IOS IP Configuration Guide*.

arp (global)

To add a permanent entry in the Address Resolution Protocol (ARP) cache, use the **arp** global configuration command. To remove an entry from the ARP cache, use the **no** form of this command.

arp *ip-address hardware-address type* [**alias**]

no arp *ip-address hardware-address type* [**alias**]

Syntax Description

ip-address	IP address in four-part dotted decimal format corresponding to the local data-link address.
hardware-address	Local data-link address (a 48-bit address).
type	Encapsulation description. For Ethernet interfaces, this is typically the **arpa** keyword. For FDDI and Token Ring interfaces, this is always the **snap** keyword.
alias	(Optional) Indicates that the Cisco IOS software should respond to ARP requests as if it were the owner of the specified address.

Defaults

No entries are permanently installed in the ARP cache.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The Cisco IOS software uses ARP cache entries to translate 32-bit IP addresses into 48-bit hardware addresses.

Because most hosts support dynamic resolution, you generally need not specify static ARP cache entries.

To remove all nonstatic entries from the ARP cache, use the **clear arp-cache** privileged EXEC command.

Examples

The following is an example of a static ARP entry for a typical Ethernet host:

```
arp 192.31.7.19 0800.0900.1834 arpa
```

Related Commands

Command	Description
clear arp-cache	Deletes all dynamic entries from the ARP cache.

arp (interface)

To control the interface-specific handling of IP address resolution into 48-bit Ethernet, FDDI, Frame Relay, and Token Ring hardware addresses, use the **arp** interface configuration command. To disable an encapsulation type, use the **no** form of this command.

arp {**arpa** | **frame-relay** | **probe** | **snap**}

no arp {**arpa** | **frame-relay** | **probe** | **snap**}

Syntax Description

arpa	Standard Ethernet-style Address Resolution Protocol (ARP) (RFC 826).
frame-relay	Enables ARP over a Frame Relay encapsulated interface.
probe	HP Probe protocol for IEEE-802.3 networks.
snap	ARP packets conforming to RFC 1042.

Defaults

Standard Ethernet-style ARP

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Unlike most commands that have multiple arguments, the **arp** command has arguments that are not mutually exclusive. Each command enables or disables a specific type of ARP. For example, if you enter the **arp arpa** command followed by the **arp probe** command, the Cisco IOS software would send three packets (two for **probe** and one for **arpa**) each time it needed to discover a MAC address.

The **arp probe** command allows the software to use the Probe protocol (in addition to ARP) whenever it attempts to resolve an IEEE-802.3 or Ethernet local data-link address. The subset of Probe that performs address resolution is called Virtual Address Request and Reply. Using Probe, the Cisco IOS software can communicate transparently with Hewlett Packard IEEE-802.3 hosts that use this type of data encapsulation.

Note Cisco support for HP Probe proxy support changed as of Release 8.3(2) and subsequent software releases. The **no arp probe** command is now the default. All interfaces that will use Probe must now be explicitly configured for the **arp probe** command.

Given a network protocol address (IP address), the **arp frame-relay** command determines the corresponding hardware address, which would be a data-link connection identifier (DLCI) for Frame Relay.

The **show interfaces** EXEC command displays the type of ARP being used on a particular interface. To remove all nonstatic entries from the ARP cache, use the **clear arp-cache** privileged EXEC command.

Examples

The following example enables probe services:

```
interface ethernet 0
 arp probe
```

Related Commands

Command	Description
clear arp-cache	Deletes all dynamic entries from the ARP cache.
show interfaces	Displays statistics for all interfaces configured on the router or access server.

arp timeout

To configure how long an entry remains in the Address Resolution Protocol (ARP) cache, use the **arp timeout** interface configuration command. To restore the default value, use the **no** form of this command.

arp timeout *seconds*

no arp timeout *seconds*

Syntax Description

seconds	Time (in seconds) that an entry remains in the ARP cache. A value of zero means that entries are never cleared from the cache.

Defaults

14400 seconds (4 hours)

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command is ignored when issued on interfaces that do not use ARP. The **show interfaces** EXEC command displays the ARP timeout value. The value follows the "Entry Timeout:" heading, as seen in the following example from the **show interfaces** command:

```
ARP type: ARPA, PROBE, Entry Timeout: 14400 sec
```

Examples

The following example sets the ARP timeout to 12000 seconds to allow entries to time out more quickly than the default:

```
interface ethernet 0
 arp timeout 12000
```

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router or access server.

clear arp-cache

To delete all dynamic entries from the Address Resolution Protocol ARP cache, to clear the fast-switching cache, and to clear the IP route cache, use the **clear arp-cache** EXEC command.

clear arp-cache

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example removes all dynamic entries from the ARP cache and clears the fast-switching cache:

```
clear arp-cache
```

Related Commands

Command	Description
arp (global)	Adds a permanent entry in the ARP cache.
arp (interface)	Controls the interface-specific handling of IP address resolution into 48-bit Ethernet, FDDI, and Token Ring hardware addresses.

clear host

To delete entries from the host name-to-address cache, use the **clear host** EXEC command.

clear host {*name* | *****}

Syntax Description

name	Particular host entry to remove.
*	Removes all entries.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The host name entries will not be removed from NVRAM, but will be cleared in running memory.

Examples

The following example clears all entries from the host name-to-address cache:

```
clear host *
```

Related Commands

Command	Description
ip host	Defines a static host name-to-address mapping in the host cache.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses.

clear ip nat translation

To clear dynamic Network Address Translation (NAT) translations from the translation table, use the **clear ip nat translation** EXEC command.

clear ip nat translation {***** | [**forced**] | [**inside** *global-ip local-ip*] [**outside** *local-ip global-ip*]}

clear ip nat translation *protocol* **inside** *global-ip global-port local-ip local-port* [**outside** *local-ip global-ip*]

Syntax Description

*****	Clears all dynamic translations.
forced	(Optional) Clears all dynamic translations and processes that are causing the router to hang.
inside	(Optional) Clears the inside translations containing the specified *global-ip* and *local-ip* addresses.
global-ip	(Optional) When used without the arguments *protocol*, *global-port*, and *local-port arguments*, clears a simple translation that also contains the specified *local-ip* address. When used with the *protocol*, *global-port*, and *local-port arguments*, clears an extended translation.
local-ip	(Optional) Clears an entry that contains this local IP address and the specified *global-ip* address.
outside	(Optional) Clears the outside translations containing the specified *global-ip* and *local-ip* addresses.
protocol	Clears an entry that contains this protocol and the specified *global-ip* address, *local-ip* address, *global-port value*, and *local-port value*.
global-port	Clears an entry that contains this *global-port value* and the specified *protocol value*, *global-ip* address, *local-ip* address, and *local-port value*.
local-port	Clears an entry that contains this *local-port* value and the specified *protocol value*, *global-ip* address, *local-ip* address, and *global-port value*.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to clear entries from the translation table before they time out.

Examples

The following example shows the NAT entries before and after the User Datagram Protocol (UDP) entry is cleared:

```
Router# show ip nat translation

Pro Inside global      Inside local       Outside local      Outside global
udp 171.69.233.209:1220 192.168.1.95:1220 171.69.2.132:53    171.69.2.132:53
```

```
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23  171.69.1.220:23
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23    171.69.1.161:23

Router# clear ip nat translation udp inside 171.69.233.209 1220 192.168.1.95 1220
171.69.2.132 53 171.69.2.132 53

Router# show ip nat translation

Pro Inside global      Inside local       Outside local      Outside global
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23  171.69.1.220:23
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23    171.69.1.161:23
```

Related Commands

Command	Description
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Changes the amount of time after which NAT translations time out.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

clear ip nhrp

To clear all dynamic entries from the Next Hop Resolution Protocol (NHRP) cache, use the **clear ip nhrp** EXEC command.

clear ip nhrp

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

This command does not clear any static (configured) IP-to-nonbroadcast multiaccess (NBMA) address mappings from the NHRP cache.

Examples

The following example clears all dynamic entries from the NHRP cache for the interface:

```
clear ip nhrp
```

Related Commands

Command	Description
show ip nhrp	Displays the NHRP cache.

clear ip route

To delete routes from the IP routing table, use the **clear ip route** EXEC command.

clear ip route {*network* [*mask*] | *****}

Syntax Description

network	Network or subnet address to remove.
mask	(Optional) Subnet address to remove.
*	Removes all routing table entries.

Defaults

All entries are removed.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example removes a route to network 132.5.0.0 from the IP routing table:

```
clear ip route 132.5.0.0
```

ip address

To set a primary or secondary IP address for an interface, use the **ip address** interface configuration command. To remove an IP address or disable IP processing, use the **no** form of this command.

ip address *ip-address mask* [**secondary**]

no ip address *ip-address mask* [**secondary**]

Syntax Description

ip-address	IP address.
mask	Mask for the associated IP subnet.
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.

Defaults

No IP address is defined for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the Cisco IOS software always use the primary IP address. Therefore, all routers and access servers on a segment should share the same primary network number.

Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) mask request message. Routers respond to this request with an ICMP mask reply message.

You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command. If the software detects another host using one of its IP addresses, it will print an error message on the console.

The optional **secondary** keyword allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.

Secondary IP addresses can be used in a variety of situations. The following are the most common applications:

- There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need 300 host addresses. Using secondary IP addresses on the routers or access servers allows you to have two logical subnets using one physical subnet.

- Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnetted, router-based network. Routers on an older, bridged segment can be easily made aware that many subnets are on that segment.
- Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is *extended*, or layered on top of the second network using secondary addresses.

Note If any router on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.

Note When you are routing using the Open Shortest Path First (OSPF) algorithm, ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.

To transparently bridge IP on an interface, you must perform the following two tasks:

- Disable IP routing (specify the **no ip routing** command).
- Add the interface to a bridge group, see the **bridge-group** command.

To concurrently route and transparently bridge IP on an interface, see the **bridge crb** command.

Examples

In the following example, 131.108.1.27 is the primary address and 192.31.7.17 and 192.31.8.17 are secondary addresses for Ethernet interface 0:

```
interface ethernet 0
 ip address 131.108.1.27 255.255.255.0
 ip address 192.31.7.17 255.255.255.0 secondary
 ip address 192.31.8.17 255.255.255.0 secondary
```

Related Commands

Command	Description
bridge crb	Enables the Cisco IOS software to both route and bridge a given protocol on separate interfaces within a single router.
bridge-group	Assigns each network interface to a bridge group.

ip broadcast-address

To define a broadcast address for an interface, use the **ip broadcast-address** interface configuration command. To restore the default IP broadcast address, use the **no** form of this command.

ip broadcast-address [*ip-address*]

no ip broadcast-address [*ip-address*]

Syntax Description

ip-address	(Optional) IP broadcast address for a network.

Defaults

Default address: 255.255.255.255 (all ones)

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example specifies an IP broadcast address of 0.0.0.0:

```
ip broadcast-address 0.0.0.0
```

ip cef traffic-statistics

To change the time interval that controls when Next Hop Resolution Protocol (NHRP) will set up or tear down a switched virtual circuit (SVC), use the **ip cef traffic-statistics** global configuration command. To restore the default values, use the **no** form of this command.

ip cef traffic-statistics [**load-interval** *seconds*] [**update-rate** *seconds*]

no ip cef traffic-statistics

Syntax Description

load-interval *seconds*	(Optional) Length of time (in 30-second increments) during which the average *trigger-threshold* and *teardown-threshold* intervals are calculated before an SVC setup or teardown action is taken. (These thresholds are configured in the **ip nhrp trigger-svc** command.) The **load-interval** range is from 30 seconds to 300 seconds, in 30-second increments. The default value is 30 seconds.
update-rate *seconds*	(Optional) Frequency that the port adapter sends the accounting statistics to the Route Processor (RP). When using NHRP in distributed CEF switching mode, this value must be set to 5 seconds. The default value is 10 seconds.

Defaults

load-interval: 30 seconds

update-rate: 10 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The thresholds in the **ip nhrp trigger-svc** command are measured during a sampling interval of 30 seconds, by default. To change that interval, use the **load-interval** *seconds* option of the **ip cef traffic-statistics** command.

When NHRP is configured on a CEF switching node with a Versatile Interface Processor (VIP2) adapter, you must make sure the **update-rate** keyword is set to 5 seconds.

Other Cisco IOS features could also use the **ip cef traffic-statistics** command; this NHRP feature relies on it.

Examples

In the following example, the triggering and teardown thresholds are calculated based on an average over 120 seconds:

```
ip cef traffic-statistics load-interval 120
```

Related Commands

Command	Description
ip nhrp trigger-svc	Configures when NHRP will set up and tear down an SVC based on aggregate traffic rates.

ip classless

At times the router might receive packets destined for a subnet of a network that has no network default route. To have the Cisco IOS software forward such packets to the best supernet route possible, use the **ip classless** global configuration command. To disable this feature, use the **no** form of this command.

ip classless

no ip classless

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3	The default behavior changed from disabled to enabled.

Usage Guidelines

This command allows the software to forward packets that are destined for unrecognized subnets of directly connected networks. The packets are forwarded to the best supernet route.

When this feature is disabled, the Cisco IOS software discards the packets when a router receives packets for a subnet that numerically falls within its subnetwork addressing scheme, no such subnet number is in the routing table and there is no network default route.

Note If the supernet, or default route, is learned via IS-IS or OSPF, the **no ip classless** configuration command is ignored.

Examples

The following example prevents the software from forwarding packets destined for an unrecognized subnet to the best supernet possible:

```
no ip classless
```

ip default-gateway

To define a default gateway (router) when IP routing is disabled, use the **ip default-gateway** global configuration command. To disable this function, use the **no** form of this command.

ip default-gateway *ip-address*

no ip default-gateway *ip-address*

Syntax Description

ip-address	IP address of the router.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The Cisco IOS software sends any packets that need the assistance of a gateway to the address you specify. If another gateway has a better route to the requested host, the default gateway sends an Internet Control Message Protocol (ICMP) redirect message back. The ICMP redirect message indicates which local router the Cisco IOS software should use.

Examples

The following example defines the router on IP address 192.31.7.18 as the default router:

```
ip default-gateway 192.31.7.18
```

Related Commands

Command	Description
ip redirects	Enables the sending of ICMP redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received.
show ip redirects	Displays the address of a default gateway (router) and the address of hosts for which an ICMP redirect message has been received.

ip directed-broadcast

To enable the translation of a directed broadcast to physical broadcasts, use the **ip directed-broadcast** interface configuration command. To disable this function, use the **no** form of this command.

ip directed-broadcast [*access-list-number*] | [*extended access-list-number*]

no ip directed-broadcast [*access-list-number*] | [*extended access-list-number*]

Syntax Description

access-list-number	(Optional) Standard access list number in the range from 1 to 199. If specified, a broadcast must pass the access list to be forwarded.
extended access-list-number	(Optional) Extended access list number in the range from 1300 to 2699.

Defaults

Disabled; all IP directed broadcasts are dropped.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0	The default behavior changed to directed broadcasts being dropped.

Usage Guidelines

An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet, but which originates from a node that is not itself part of that destination subnet.

A router that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a router that is directly connected to its destination subnet, that packet is "exploded" as a broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast.

The **ip directed-broadcast** interface command controls the explosion of directed broadcasts when they reach their target subnets. The command affects only the final transmission of the directed broadcast on its ultimate destination subnet. It does not affect the transit unicast routing of IP directed broadcasts.

If directed broadcast is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached will be exploded as broadcasts on that subnet. If an access list has been configured with the **ip directed-broadcast** command, only directed broadcasts that are permitted by the access list in question will be forwarded; all other directed broadcasts destined for the interface subnet will be dropped.

If the **no ip directed-broadcast** command has been configured for an interface, directed broadcasts destined for the subnet to which that interface is attached will be dropped, rather than being broadcast.

Note Because directed broadcasts, and particularly Internet Control Message Protocol (ICMP) directed broadcasts, have been abused by malicious persons, we recommend that security-conscious users disable the **ip directed-broadcast** command on any intereface where directed broadcasts are not needed and that they use access lists to limit the number of exploded packets.

Examples

The following example enables forwarding of IP directed broadcasts on Ethernet interface 0:

```
interface ethernet 0
 ip directed-broadcast
```

Related Commands

Command	Description
ip forward-protocol	Specifies which protocols and ports the router forwards when forwarding broadcast packets.

ip dns primary

To configure the router as authoritative for its zone, use the **ip dns primary** command in global configuration mode. To disable, use the **no** form of this command.

ip dns primary *name* **soa** *server-name mailbox-name* [*refresh-time* [*retry-time*]]

no ip dns primary *name* **soa** *server-name mailbox-name* [*refresh-time* [*retry-time*]]

Syntax Description

name	DNS domain name.
soa	Start of authority record parameters.
server-name	Authoritative name server.
mailbox-name	DNS mailbox of responsible person.
refresh-time	(Optional) Time in seconds...Range is from 0 to 424967295.
retry-time	(Optional) Time in seconds...Range is from 0 to 424967295.

Command Default

<<Statement of the command-level default (see SAWG for definition).>>

Command Modes

<<Text.>>

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

<<Text.>>

Examples

The following example <<text>>:

```
ip dns primary bar soa hello.cisco.com postmaster.cisco.com
```

Related Commands

Command	Description
<<command>>	<<FID.>>

ip domain list

To define a list of default domain names to complete unqualified host names, use the **ip domain list** command in global configuration mode. To delete a name from a list, use the **no** form of this command.

ip domain list *name*

no ip domain list *name*

Syntax Description

name	Domain name. Do not include the initial period that separates an unqualified name from the domain name.

Defaults

No domain names are defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2	The syntax of the command changed from **ip domain-list** to **ip domain list**.

Usage Guidelines

If there is no domain list, the domain name that you specified with the **ip domain name** global configuration command is used. If there is a domain list, the default domain name is not used. The **ip domain list** command is similar to the **ip domain name** command, except that with the **ip domain list** command you can define a list of domains, each to be tried in turn.

The Cisco IOS software will still accept the previous version of the command **ip domain-list**.

Examples

The following example adds several domain names to a list:

```
ip domain list company.com
ip domain list school.edu
```

The following example adds a name to and then deletes a name from the list:

```
ip domain list school.edu
no ip domain list school.edu
```

Related Commands

Command	Description
ip domain name	Defines a default domain name to complete unqualified host names (names without a dotted-decimal domain name).

ip domain lookup

To enable the IP Domain Naming System (DNS)-based host name-to-address translation, use the **ip domain lookup** command in global configuration mode. To disable the DNS, use the **no** form of this command.

ip domain lookup

no ip domain lookup

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2	The syntax of the command changed from **ip domain-lookup** to **ip domain lookup**.

Usage Guidelines

The Cisco IOS software will still accept the previous version of the command **ip domain-lookup**.

Examples

The following example enables the IP DNS-based host name-to-address translation:

```
ip domain lookup
```

Related Commands

Command	Description
ip domain name	Defines a default domain name to complete unqualified host names (names without a dotted decimal domain name).
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip domain name

To define a default domain name that the Cisco IOS software uses to complete unqualified host names (names without a dotted-decimal domain name), use the **ip domain-name** command in global configuration mode. To disable use of the Domain Name System (DNS), use the **no** form of this command.

ip domain name *name*

no ip domain name *name*

Syntax Description

name	Default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2	The syntax of the command changed from **ip domain-name** to **ip domain name**.

Usage Guidelines

Any IP host name that does not contain a domain name (that is, any name without a dot) will have the dot and cisco.com appended to it before being added to the host table.

The Cisco IOS software will still accept the previous version of the command **ip domain-name**.

Examples

The following example defines cisco.com as the default domain name:

```
ip domain name cisco.com
```

Related Commands

Command	Description
ip domain list	Defines a list of default domain names to complete unqualified host names.
ip domain lookup	Enables the IP DNS-based host name-to-address translation.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip domain round-robin

To enable round-robin functionality on DNS servers, use the **ip domain round-robin** command in global configuration mode. To disable round-robin functionality, use the no form of the command.

ip domain round-robin

no ip domain round-robin

Syntax Description

This command has no arguments or keywords.

Defaults

Round robin is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

In a multiple server configuration *without* the DNS round-robin functionality, the first host server/IP address is used for the whole time to live (TTL) of the cache, and uses the second and third only in the event of host failure. This behavior presents a problem when a high volume of users all arrive at the first host during the TTL time. The network access server (NAS) then sends out a DNS query; the DNS servers reply with a list of the configured IP addresses to the NAS. The NAS then caches these IP addresses for a given time (for example, five minutes). All users that dial in during the five minute TTL time will land on one host, the first IP address in the list.

In a multiple server configuration *with* the DNS round-robin functionality, the DNS server returns the IP address of all hosts to rotate between the cache of host names. During the TTL of the cache, users are distributed among the hosts. This functionality distributes calls across the configured hosts and reduces the amount of DNS queries.

Examples

The following example allows a Telnet to www.company.com to connect to each of the three IP addresses specified in the following order: the first time the Telnet command is given, it would connect to 10.0.0.1; the second time the command is given, it would connect to 20.0.0.1; and the third time the command is given, it would connect to 30.0.0.1. In each case, the other two addresses would also be tried if the first one failed; this is the normal operation of the Telnet command.

```
Router(config)# ip host www.company.com 10.0.0.1 20.0.0.1 30.0.0.1
Router(config)# ip domain round-robin
```

ip forward-protocol

To specify which protocols and ports the router forwards when forwarding broadcast packets, use the **ip forward-protocol** global configuration command. To remove a protocol or port, use the **no** form of this command.

ip forward-protocol {**udp** [*port*] | **nd** | **sdns**}

no ip forward-protocol {**udp** [*port* | **nd** | **sdns**}

Syntax Description

udp	Forwards User Datagram Protocol (UDP) datagrams. See the "Defaults" section for a list of port numbers forwarded by default.
port	(Optional) Destination port that controls which UDP services are forwarded.
nd	Forwards Network Disk (ND) datagrams. This protocol is used by older diskless Sun workstations.
sdns	Secure Data Network Service.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Enabling a helper address or UDP flooding on an interface causes the Cisco IOS software to forward particular broadcast packets. You can use the **ip forward-protocol** command to specify exactly which types of broadcast packets you would like to have forwarded. A number of commonly forwarded applications are enabled by default. Enabling forwarding for some ports (for example, Routing Information Protocol (RIP) may be hazardous to your network.

If you use the **ip forward-protocol** command, specifying only UDP without the port enables forwarding and flooding on the default ports.

One common application that requires helper addresses is Dynamic Host Configuration Protocol (DHCP). DHCP is defined in RFC 1531. DHCP protocol information is carried inside of BOOTP packets. To enable BOOTP broadcast forwarding for a set of clients, configure a helper address on the router interface closest to the client. The helper address should specify the address of the DHCP server. If you have multiple servers, you can configure one helper address for each server. Because BOOTP packets are forwarded by default, DHCP information can now be forwarded by the software. The DHCP server now receives broadcasts from the DHCP clients.

If an IP helper address is defined, UDP forwarding is enabled on default ports. If UDP flooding is configured, UDP flooding is enabled on the default ports.

If a helper address is specified and UDP forwarding is enabled, broadcast packets destined to the following port numbers are forwarded by default:

- Trivial File Transfer Protocol (TFTP) (port 69)
- Domain Naming System (port 53)
- Time service (port 37)
- NetBIOS Name Server (port 137)
- NetBIOS Datagram Server (port 138)
- Boot Protocol (BOOTP) client and server datagrams (ports 67 and 68)
- TACACS service (port 49)
- IEN-116 Name Service (port 42)

ip forward-protocol spanning-tree

To permit IP broadcasts to be flooded throughout the internetwork in a controlled fashion, use the **ip forward-protocol spanning-tree** global configuration command. To disable the flooding of IP broadcasts, use the **no** form of this command.

ip forward-protocol spanning-tree [**any-local-broadcast**]

no ip forward-protocol spanning-tree [**any-local-broadcast**]

Syntax Description

any-local-broadcast	(Optional) Accept any local broadcast when flooding.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

A packet must meet the following criteria to be considered for flooding:

- The MAC address of the received frame must be all-ones broadcast address (ffff.ffff.ffff).
- The IP destination address must be one of the following: all-ones broadcast (255.255.255.255), subnet broadcast for the receiving interface; major-net broadcast for the receiving interface if the **no ip classless** command is also configured; or any local IP broadcast address if the **ip forward-protocol spanning-tree any-local-broadcast** command is configured.
- The IP time-to-live (TTL) value must be at least 2.
- The IP protocol must be UDP (17).
- The UDP destination port must be for TFTP, Domain Name System (DNS), Time, NetBIOS, ND, or BOOTP packet, or a UDP port specified by the **ip forward-protocol udp** global configuration command.

A flooded UDP datagram is given the destination address specified by the **ip broadcast-address** interface configuration command on the output interface. The destination address can be set to any desired address. Thus, the destination address may change as the datagram propagates through the network. The source address is never changed. The TTL value is decremented.

After a decision has been made to send the datagram out on an interface (and the destination address possibly changed), the datagram is handed to the normal IP output routines and is therefore subject to access lists, if they are present on the output interface.

The **ip forward-protocol spanning-tree** command uses the database created by the bridging Spanning-Tree Protocol. Therefore, the transparent bridging option must be in the routing software, and bridging must be configured on each interface that is to participate in the flooding in order to support this capability.

If an interface does not have bridging configured, it still will be able to receive broadcasts, but it will never forward broadcasts received on that interface. Also, it will never use that interface to send broadcasts received on a different interface.

If no actual bridging is desired, you can configure a type-code bridging filter that will deny all packet types from being bridged. Refer to the "Configuring Transparent Bridging" chapter in the *Cisco IOS Bridging and IBM Networking Configuration Guide* for more information about using access lists to filter bridged traffic. The spanning-tree database is still available to the IP forwarding code to use for the flooding.

The spanning-tree-based flooding mechanism forwards packets whose contents are all ones (255.255.255.255), all zeros (0.0.0.0), and, if subnetting is enabled, all networks (131.108.255.255 as an example in the network number 131.108.0.0). This mechanism also forward packets whose contents are the zeros version of the all-networks broadcast when subnetting is enabled (for example, 131.108.0.0).

This command is an extension of the **ip helper-address** interface configuration command, in that the same packets that may be subject to the helper address and forwarded to a single network can now be flooded. Only one copy of the packet will be put on each network segment. In some cases, where DHCP broadcasts are being forwarded to spanning-tree enabled interfaces, a duplicate copy of the packet will be put on a network segment. See the **ip directed-broadcast** global configuration command for information on how to ensure that duplicate packets are not copied onto a network segment.

Examples

The following example permits IP broadcasts to be flooded through the internetwork in a controlled fashion:

```
ip forward-protocol spanning-tree
```

Related Commands

Command	Description
ip broadcast-address	Defines a broadcast address for an interface.
ip directed-broadcast	Sets the gateway address (giaddr) field in the DHCP packet before forwarding to spanning-tree interfaces
ip forward-protocol	Specifies which protocols and ports the router forwards when forwarding broadcast packets.
ip forward-protocol turbo-flood	Speeds up flooding of UDP datagrams using the spanning-tree algorithm.
ip helper-address	Forwards UDP broadcasts, including BOOTP, received on an interface.

ip forward-protocol turbo-flood

To speed up flooding of User Datagram Protocol (UDP) datagrams using the spanning-tree algorithm, use the **ip forward-protocol turbo-flood** global configuration command. To disable this feature, use the **no** form of this command.

ip forward-protocol turbo-flood

no ip forward-protocol turbo-flood

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Used in conjunction with the **ip forward-protocol spanning-tree** global configuration command, this feature is supported over Advanced Research Projects Agency (ARPA)-encapsulated Ethernets, FDDI, and High-Level Data Link Control (HDLC) encapsulated serials, but is not supported on Token Rings. As long as the Token Rings and the non-HDLC serials are not part of the bridge group being used for UDP flooding, turbo flooding will behave normally.

Examples

The following is an example of a two-port router using this command:

```
ip forward-protocol turbo-flood
ip forward-protocol spanning-tree
!
interface ethernet 0
 ip address 128.9.1.1
 bridge-group 1
!
interface ethernet 1
 ip address 128.9.1.2
 bridge-group 1
!
 bridge 1 protocol dec
```

Related Commands

Command	Description
ip forward-protocol	Specifies which protocols and ports the router forwards when forwarding broadcast packets.
ip forward-protocol spanning-tree	Permits IP broadcasts to be flooded throughout the internetwork in a controlled fashion.

ip helper-address

To have the Cisco IOS software forward User Datagram Protocol (UDP) broadcasts, including BOOTP, received on an interface, use the **ip helper-address** interface configuration command. To disable the forwarding of broadcast packets to specific addresses, use the **no** form of this command.

ip helper-address *address*

no ip helper-address *address*

Syntax Description

address	Destination broadcast or host address to be used when forwarding UDP broadcasts. There can be more than one helper address per interface.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Combined with the **ip forward-protocol** global configuration command, the **ip helper-address** command allows you to control which broadcast packets and which protocols are forwarded.

One common application that requires helper addresses is Dynamic Host Configuration Protocol (DHCP), which is defined in RFC 1531. DHCP protocol information is carried inside of BOOTP packets. To enable BOOTP broadcast forwarding for a set of clients, configure a helper address on the router interface closest to the client. The helper address should specify the address of the DHCP server. If you have multiple servers, you can configure one helper address for each server. Because BOOTP packets are forwarded by default, DHCP information can now be forwarded by the router. The DHCP server now receives broadcasts from the DHCP clients.

All of the following conditions must be met in order for a UDP or IP packet to be helpered by the **ip helper-address** command:

- The MAC address of the received frame must be all-ones broadcast address (ffff.ffff.ffff).
- The IP destination address must be one of the following: all-ones broadcast (255.255.255.255), subnet broadcast for the receiving interface; or major-net broadcast for the receiving interface if the **no ip classless** command is also configured.
- The IP time-to-live (TTL) value must be at least 2.
- The IP protocol must be UDP (17).
- The UDP destination port must be for TFTP, Domain Name System (DNS), Time, NetBIOS, ND, BOOTP or DHCP packet, or a UDP port specified by the **ip forward-protocol udp** global configuration command.

Note The **ip helper-address** command does not work on an X.25 interfaceon a destination router because the router cannot determine if the packet was intended as a physical broadcast.

Examples

The following example defines an address that acts as a helper address:

```
interface ethernet 1
 ip helper-address 121.24.43.2
```

Related Commands

Command	Description
ip forward-protocol	Specifies which protocols and ports the router forwards when forwarding broadcast packets.

Related Commands

Command	Description
ip forward-protocol	Specifies which protocols and ports the router forwards when forwarding broadcast packets.

ip host

To define a static host name-to-address mapping in the host cache, use the **ip host** global configuration command. To remove the name-to-address mapping, use the **no** form of this command.

ip host *name* [*tcp-port-number*] {*address1* [*address2...address8*]}

no ip host *name* [*tcp-port-number*] {*address1* [*address2...address8*]}

Syntax Description

name	Name of the host. The first character can be either a letter or a number. If you use a number, the operations you can perform are limited.
tcp-port-number	(Optional) TCP port number to connect to when using the defined host name in conjunction with an EXEC connect or Telnet command. The default is Telnet (port 23).
address1	Associated IP address.
address2...address8	(Optional) Additional associated IP addresses. You can bind up to eight addresses to a host name.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The first character can be either a letter or a number. If you use a number, the types of operations you can perform (such as **ping**) are limited.

Examples

The following example defines two static mappings:

```
ip host croff 192.31.7.18
ip host bisso-gw 10.2.0.2 192.31.7.33
```

ip hp-host

To enter into the host table the host name of a Hewlett-Packard (HP) host to be used for HP Probe Proxy service, use the **ip hp-host** global configuration command. To remove a host name, use the **no** form of this command.

ip hp-host *host-name ip-address*

no ip hp-host *host-name ip-address*

Syntax Description

host-name	Name of the host.
ip-address	IP address of the host.

Defaults

No host names are defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

To use the HP Probe Proxy service, you must first enter the host name of the HP host into the host table using this command.

Examples

The following example specifies the name and address of an HP host, and then enables HP Probe Proxy:

```
ip hp-host BCWjo 131.108.1.27
interface ethernet 0
ip probe proxy
```

Related Commands

Command	Description
ip probe proxy	Enables the HP Probe Proxy support, which allows the Cisco IOS software to respond to HP Probe Proxy name requests.

ip irdp

To enable ICMP Router Discovery Protocol (IRDP) processing on an interface, use the **ip irdp** interface configuration command. To disable IRDP routing, use the **no** form of this command.

ip irdp [**multicast** | **holdtime** *seconds* | **maxadvertinterval** *seconds* | **minadvertinterval** *seconds* | **preference** *number* | **address** *address* [*number*]]

no ip irdp

Syntax Description

multicast	(Optional) Use the multicast address (224.0.0.1) instead of IP broadcasts.
holdtime *seconds*	(Optional) Length of time in seconds that advertisements are held valid. Default is three times the **maxadvertinterval** value. Must be greater than **maxadvertinterval** and cannot be greater than 9000 seconds.
maxadvertinterval *seconds*	(Optional) Maximum interval in seconds between advertisements. The range is from 1 to 1800. A value of 0 means only advertise when solicited. The default is 600 seconds.
minadvertinterval *seconds*	(Optional) Minimum interval in seconds between advertisements. The range is from 1 to 1800. The default is 450 seconds.
preference *number*	(Optional) Preference value. The allowed range is -2^{31} to 2^{31}. The default is 0. A higher value increases the preference level of the router. You can modify a particular router so that it will be the preferred router to which other routers will home.
address *address* [*number*]	(Optional) IP address (*address*) to proxy advertise, and optionally, its preference value (*number*).

Defaults

Disabled

When enabled, IRDP uses these defaults:

- Broadcast IRDP advertisements
- Maximum interval between advertisements: 600 seconds
- Minimum interval between advertisements: 450 seconds
- Preference: 0

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

If you change the **maxadvertinterval** value, the other two values also change, so it is important to change the **maxadvertinterval** value before changing either the **holdtime** or **minadvertinterval** values.

The **ip irdp multicast** command allows for compatibility with Sun Microsystems Solaris, which requires IRDP packets to be sent out as multicasts. Many implementations cannot receive these multicasts; ensure end-host ability before using this command.

Examples

The following example sets the various IRDP processes:

```
! enable irdp on interface Ethernet 0
interface ethernet 0
 ip irdp
! send IRDP advertisements to the multicast address
 ip irdp multicast
! increase router preference from 100 to 50
 ip irdp preference 50
! set maximum time between advertisements to 400 secs
 ip irdp maxadvertinterval 400
! set minimum time between advertisements to 100 secs
 ip irdp minadvertinterval 100
! advertisements are good for 6000 seconds
 ip irdp holdtime 6000
! proxy-advertise 131.108.14.5 with default router preference
 ip irdp address 131.108.14.5
! proxy-advertise 131.108.14.6 with preference of 50
 ip irdp address 131.108.14.6 50
```

Related Commands

Command	Description
The following is sample output from the show ip interface brief command:	Displays IRDP values.

ip mobile arp

To enable local-area mobility, use the **ip mobile arp** interface configuration command. To disable local-area mobility, use the **no** form of this command.

ip mobile arp [**timers** *keepalive hold-time*] [**access-group** *access-list-number* | *name*]

no ip mobile arp [**timers** *keepalive hold-time*] [**access-group** *access-list-number* | *name*]

Syntax Description

timers	(Optional) Indicates that you are setting local-area mobility timers.
keepalive	(Optional) Frequency, in minutes, at which the Cisco IOS software sends unicast Address Resolution Protocol (ARP) messages to a relocated host to verify that the host is present and has not moved. The default keepalive time is 5 minutes (300 seconds).
hold-time	(Optional) Hold time, in minutes. This is the length of time the software considers that a relocated host is present without receiving some type of ARP broadcast or unicast from the host. Normally, the hold time should be at least three times greater than the keepalive time. The default hold time is 15 minutes (900 seconds).
access-group	(Optional) Indicates that you are applying an access list. This access list applies only to local-area mobility.
access-list-number	(Optional) Number of a standard IP access list. It is a decimal number from 1 to 99. Only hosts with addresses permitted by this access list are accepted for local-area mobility.
name	(Optional) Name of an IP access list. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.

Defaults

Local-area mobility is disabled.

If you enable local-area mobility:
keepalive: 5 minutes (300 seconds)
hold-time: 15 minutes (900 seconds)

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Local-area mobility is supported on Ethernet, Token Ring, and FDDI interfaces only.

To create larger mobility areas, you must first redistribute the mobile routes into your Interior Gateway Protocol (IGP). The IGP must support host routes. You can use Enhanced IGRP, Open Shortest Path First (OSPF), or Intermediate System-to-Intermediate System (IS-IS); you can also use Routing Information Protocol (RIP), but RIP is not recommended. The mobile area must consist of a contiguous set of subnets.

Using an access list to control the list of possible mobile nodes is strongly encouraged. Without an access list, misconfigured hosts can be taken for mobile nodes and disrupt normal operations.

Examples

The following example configures local-area mobility on Ethernet interface 0:

```
access-list 10 permit 198.92.37.114
 interface ethernet 0
 ip mobile arp access-group 10
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
default-metric (BGP)	Sets default metric values for the BGP, OSPF, and RIP routing protocols.
default-metric (OSPF)	Sets default metric values for OSPF.
default-metric (RIP)	Sets default metric values for RIP.
network (BGP)	Specifies the list of networks for the BGP routing process.
network (IGRP)	Specifies a list of networks for the IGRP or Enhanced IGRP routing process.
network (RIP)	Specifies a list of networks for the RIP routing process.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
router eigrp	Configures the IP Enhanced IGRP routing process.
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process for IP.
router ospf	Configures an OSPF routing process.

ip name-server

To specify the address of one or more name servers to use for name and address resolution, use the **ip name-server** global configuration command. To remove the addresses specified, use the **no** form of this command.

ip name-server *server-address1* [*server-address2...server-address6*]

no ip name-server *server-address1* [*server-address2...server-address6*]

Syntax Description

server-address1	IP addresses of name server.
server-address2...server-address6	(Optional) IP addresses of additional name servers (a maximum of six name servers).

Defaults

No name server addresses are specified.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example specifies host 131.108.1.111 as the primary name server and host 131.108.1.2 as the secondary server:

```
ip name-server 131.108.1.111 131.108.1.2
```

This command will be reflected in the configuration file as follows:

```
ip name-server 131.108.1.111
ip name-server 131.108.1.2
```

Related Commands

Command	Description
ip domain lookup	Enables the IP DNS-based host name-to-address translation.
ip domain name	Defines a default domain name to complete unqualified host names (names without a dotted decimal domain name).

ip nat

To designate that traffic originating from or destined for the interface is subject to Network Address Translation (NAT), use the **ip nat** interface configuration command. To prevent the interface from being able to translate, use the **no** form of this command.

ip nat {**inside** | **outside**} | **log** {**translations syslog**}

no ip nat {**inside** | **outside**} | **log** {**translations syslog**}

Syntax Description

inside	Indicates that the interface is connected to the inside network (the network subject to NAT translation).
outside	Indicates that the interface is connected to the outside network.
log	Enables NAT logging.
translations	Enables NAT logging translations.
syslog	Enables syslog for NAT logging translations.

Defaults

Traffic leaving or arriving at this interface is not subject to NAT.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Only packets moving between inside and outside interfaces can be translated. You must specify at least one inside interface and outside interface for each border router where you intend to use NAT.

NAT translations logging can be enabled or disabled with the **ip nat log translations syslog** command.

Examples

The following example translates between inside hosts addressed from either the 192.168.1.0 or 192.168.2.0 network to the globally unique 171.69.233.208/28 network:

```
ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat inside destination

To enable Network Address Translation (NAT) of the inside destination address, use the **ip nat inside destination** global configuration command. To remove the dynamic association to a pool, use the **no** form of this command.

ip nat inside destination list {*access-list-number* | *name*} **pool** *name*

no ip nat inside destination list {*access-list-number* | *name*}

Syntax Description

list *access-list-number*	Standard IP access list number. Packets with destination addresses that pass the access list are translated using global addresses from the named pool.
list *name*	Name of a standard IP access list. Packets with destination addresses that pass the access list are translated using global addresses from the named pool.
pool *name*	Name of the pool from which global IP addresses are allocated during dynamic translation.

Defaults

No inside destination addresses are translated.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command has two forms: dynamic and static address translation. The form with an access list establishes dynamic translation. Packets from addresses that match the standard access list are translated using global addresses allocated from the pool named with the **ip nat pool** command.

Examples

The following example translates between inside hosts addressed to either the 192.168.1.0 or 192.168.2.0 network to the globally unique 171.69.233.208/28 network:

```
ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat inside destination list 1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat inside source

To enable Network Address Translation (NAT) of the inside source address, use the **ip nat inside source** global configuration command. To remove the static translation or remove the dynamic association to a pool, use the **no** form of this command.

ip nat inside source {**list** {*access-list-number* | *access-list-name*} | **route-map** *name*} {**interface** *type number* | **pool** *pool-name*} [**overload**]

no ip nat inside source {**list** {*access-list-number* | *access-list-name*} | **route-map** *name*} {**interface** *type number* | **pool** *pool-name*} [**overload**]

Static NAT

ip nat inside source {**static** {*local-ip global-ip*} [**extendable**] [**no-alias**]

no ip nat inside source {**static** {*local-ip global-ip*} [**extendable**] [**no-alias**]

Port Static NAT

ip nat inside source {**static** {**tcp** | **udp** *local-ip local-port global-ip global-port*} [**extendable**] [**no-alias**]

no ip nat inside source {**static** {**tcp** | **udp** *local-ip local-port global-ip global-port*} [**extendable**] [**no-alias**]

Network Static NAT

ip nat inside source {**static** {**network** *local-network global-network mask*} [**extendable**] [**no-alias**]

no ip nat inside source {**static** {**network** *local-network global-network mask*} [**extendable**] [**no-alias**]

Syntax Description

list *access-list-number*	Standard IP access list number. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
list *name*	Name of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
pool *name*	Name of the pool from which global IP addresses are allocated dynamically.
overload	(Optional) Enables the router to use one global address for many local addresses. When overloading is configured, the TCP or UDP port number of each inside host distinguishes between the multiple conversations using the same local IP address.
static *local-ip*	Sets up a single static translation. This argument establishes the local IP address assigned to a host on the inside network. The address could be randomly chosen, allocated from RFC 1918, or obsolete.
local-port	Sets the local TCP/UDP port in a range from 1-65535.

static *global-ip*	Sets up a single static translation. This argument establishes the globally unique IP address of an inside host as it appears to the outside world.
global-port	Sets the global TCP?UDP port in a range from 1-65535.
extendable	(Optional) Extends the translation.
no-alias	(Optional) Prohibits an alias from being created for the global address.
tcp	Establishes the Transmission Control Protocol.
udp	Establishes the User Datagram Protocol.
network *local-network*	Specifies the local subnet translation.
global-network	Specifies the global subnet translation.
mask	Establishes the IP Network mask the subnet translations.

Defaults

No NAT translation of inside source addresses occurs.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command has two forms: dynamic and static address translation. The form with an access list establishes dynamic translation. Packets from addresses that match the standard access list are translated using global addresses allocated from the pool named with the **ip nat pool** command.

Packets that enter the router through the inside interface and packets sourced from the router are checked against the access list for possible NAT candidates. The access list is used to specify which traffic is to be translated.

Alternatively, the syntax form with the keyword **static** establishes a single static translation.

Examples

The following example translates between inside hosts addressed from either the 192.168.1.0 or 192.168.2.0 network to the globally unique 171.69.233.208/28 network:

```
ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat outside source

To enable Network Address Translation (NAT) of the outside source address, use the **ip nat outside source** global configuration command. To remove the static entry or the dynamic association, use the **no** form of this command.

ip nat outside source {**list** {*access-list-number* | *access-list-name*} | **route-map** *name*} **pool** *pool-name* [**add-route**]

no ip nat outside source {**list** {*access-list-number* | *access-list-name*} | **route-map** *name*} **pool** *pool-name* [**add-route**]

Static NAT

ip nat outside source static {*global-ip local-ip*}[**add-route**] [**extendable**] [**no-alias**]

no ip nat outside source static {*global-ip local-ip*} **add-route**] [**extendable**] [**no-alias**]

Port Static NAT

ip nat outside source {**static** {**tcp** | **udp** *global-ip global-port local-ip local-port*} [**add-route**] [**extendable**] [**no-alias**]

no ip nat outside source {**static** {**tcp** | **udp** *global-ip global-port local-ip local-port*} [**add-route**] [**extendable**] [**no-alias**]

Networkt Static NAT

ip nat outside source {**static network** *global-network local-network mask*} [**add-route**] [**extendable**] [**no-alias**]

no ip nat outside source {**static network** *global-network local-network mask*} [**add-route**] [**extendable**] [**no-alias**]

Syntax Description

list *access-list-number*	Standard IP access list number. Packets with source addresses that pass the access list are translated using global addresses from the named pool.
list *name*	Name of a standard IP access list. Packets with source addresses that pass the access list are translated using global addresses from the named pool.
pool *name*	Name of the pool from which global IP addresses are allocated.
add-route	(Optional) Adds a static route for the outside local address.
static *global-ip*	Sets up a single static translation. This argument establishes the globally unique IP address assigned to a host on the outside network by its owner. It was allocated from globally routable network space.
global-port	Sets the global TCP/UDP port in a range from 1-65535.
static *local-ip*	Sets up a single static translation. This argument establishes the local IP address of an outside host as it appears to the inside world. The address was allocated from address space routable on the inside (RFC 1918, *Address Allocation for Private Internets*).
local-port	Sets the local TCP/UDP orto in a range from 1-65535.
extendable	(Optional) Extends the translation.

no-alias	(Optional) Prohibits an alias from being created for the local address.
tcp	Establishes the Transmission Control Protocol.
udp	Establishes the User Datagram Protocol.
network *global-network*	Specifies the global subnet translation.
local-network	Specifies the local subnet translation.
mask	Establishes the IP network mask for the subnet translations.

Defaults

No translation of source addresses coming from the outside to the inside network occurs.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

You might have IP addresses that are not legal, officially assigned IP addresses. Perhaps you chose IP addresses that officially belong to another network. The case of an address used illegally and legally is called *overlapping*. You can use NAT to translate inside addresses that overlap with outside addresses. Use this feature if your IP addresses in the stub network happen to be legitimate IP addresses belonging to another network, and you need to communicate with those hosts or routers.

This command has two forms: dynamic and static address translation. The form with an access list establishes dynamic translation. Packets from addresses that match the standard access list are translated using global addresses allocated from the pool named with the **ip nat pool** command.

Alternatively, the syntax form with the **static** keyword establishes a single static translation.

Examples

The following example translates between inside hosts addressed from the 9.114.11.0 network to the globally unique 171.69.233.208/28 network. Further packets from outside hosts addressed from the 9.114.11.0 network (the true 9.114.11.0 network) are translated to appear to be from the 10.0.1.0/24 network.

```
ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat pool net-10 10.0.1.0 10.0.1.255 prefix-length 24
ip nat inside source list 1 pool net-208
ip nat outside source list 1 pool net-10
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 9.114.11.39 255.255.255.0
 ip nat inside
!
access-list 1 permit 9.114.11.0 0.0.0.255
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat pool

To define a pool of IP addresses for Network Address Translation (NAT), use the **ip nat pool** global configuration command. To remove one or more addresses from the pool, use the **no** form of this command.

ip nat pool *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}[**type rotary**]

no ip nat pool *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} [**type rotary**]

Syntax Description

name	Name of the pool.
start-ip	Starting IP address that defines the range of addresses in the address pool.
end-ip	Ending IP address that defines the range of addresses in the address pool.
netmask *netmask*	Network mask that indicates which address bits belong to the network and subnetwork fields and which bits belong to the host field. Specify the netmask of the network to which the pool addresses belong.
prefix-length *prefix-length*	Number that indicates how many bits of the netmask are ones (how many bits of the address indicate network). Specify the netmask of the network to which the pool addresses belong.
type rotary	(Optional) Indicates that the range of address in the address pool identify real, inside hosts among which TCP load distribution will occur.

Defaults

No pool of addresses is defined.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command defines a pool of addresses using start address, end address, and either netmask or prefix length. The pool could define either an inside global pool, an outside local pool, or a rotary pool.

Examples

The following example translates between inside hosts addressed from either the 192.168.1.0 or 192.168.2.0 network to the globally unique 171.69.233.208/28 network:

```
ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
```

```
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat service	Enables a port other than the default port.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat service

To specify a port other than the default port, use the **ip nat service** command in global configuration mode. To disable the port, use the **no** form of this command.

ip nat service {**H225** | **list** {*access-list-number* | *access-list-name*} **ftp tcp port** *port-number* | **skinny tcp port** *port-number*}

no ip nat service {**H225** | **list** {*access-list-number* | *access-list-name*} **ftp tcp port** *port-number* | **skinny tcp port** *port-number*}

Syntax Description

H225	H323-H225 protocol.
list *access-list-number*	Standard access list number in the range from 1 to 199.
access-list-name	Name of a standard IP access list.
ftp	FTP protocol.
tcp	TCP protocol.
port *port-number*	Port other than the default port in the range from 1 to 65533.
skinny	Skinny protocol.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.1(5)T	The **skinny** keyword was added.

Usage Guidelines

A host with an FTP server using a port other than the default port can have an FTP client using the default FTP control port. When a port other than the default port is configured for an FTP server, Network Address Translation (NAT) prevents FTP control sessions that are using port 21 for that particular server. If an FTP server uses the default port and a port other than the default port, both ports need to be configured using the **ip nat service** command.

NAT listens on the default port of the Cisco CallManager to translate the skinny messages. If the CallManager uses a port other than the default port, that port needs to be configured using the **ip nat service** command.

Use the **no ip nat service H225** command to disable support of H.225 packets by NAT.

Examples

The following example configures the nonstandard port 2021:

```
ip nat service list 10 ftp tcp port 2021
access-list 10 permit 10.1.1.1
```

The following example configures the standard FTP port 21 and the nonstandard port 2021:

```
ip nat service list 10 ftp tcp port 21
ip nat service list 10 ftp tcp port 2021
access-list 10 permit 10.1.1.1
```

The following example configures the 20002 port of the CallManager:

```
ip nat service skinny tcp port 20002
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat translation

To change the amount of time after which Network Address Translation (NAT) translations time out, use the **ip nat translation** global configuration command. To disable the timeout, use the **no** form of this command.

ip nat translation [**max-entries** *number*] {**timeout** | **udp-timeout** | **dns-timeout** | **tcp-timeout** | **finrst-timeout** | **icmp-timeout** | **pptp-timeout** | **syn-timeout** | **port-timeout**} *seconds* | *never*

no ip nat translation [**max-entries** *number*] {**timeout** | **udp-timeout** | **dns-timeout** | **tcp-timeout** | **finrst-timeout** | **icmp-timeout** | **pptp-timeout** | **syn-timeout** | **port-timeout**}

Syntax Description

max-entries *number*	(Optional) Specifies the maximum number (1-2147483647) of NAT entries. Default is unlimited.
timeout	Specifies that the timeout value applies to dynamic translations except for overload translations. Default is 86400 seconds (24 hours).
udp-timeout	Specifies that the timeout value applies to the User Datagram Protocol (UDP) port. Default is 300 seconds (5 minutes).
dns-timeout	Specifies that the timeout value applies to connections to the Domain Naming System (DNS). Default is 60 seconds.
tcp-timeout	Specifies that the timeout value applies to the TCP port. Default is 86400 seconds (24 hours).
finrst-timeout	Specifies that the timeout value applies to Finish and Reset TCP packets, which terminate a connection. Default is 60 seconds.
icmp-timeout	Specifies the timeout value for Internet Control Message Protocol (ICMP) flows. Default is 60 seconds.
pptp-timeout	Specifies the timeout value for NAT Point-to-Point Tunneling Protocol (PPTP) flows. Default is 86400 seconds (24 hours).
syn-timeout	Specifies the timeout value for TCP flows immediately after a synchronous transmission (SYN) message. The default is 60 seconds.
port-timeout	Specifies that the timeout value applies to the TCP/UDP port.
seconds	Number of seconds after which the specified port translation times out. The default is 0.
never	Specifies no port translation time out.

Defaults

timeout: 86400 seconds (24 hours)

udp-timeout: 300 seconds (5 minutes)

dns-timeout: 60 seconds (1 minute)

tcp-timeout: 86400 seconds (24 hours)

finrst-timeout: 60 seconds (1 minute)

icmp-timeout: 60 seconds (1 minute)

pptp-timeout: 86400 seconds (24 hours)

syn-timeout: 60 seconds (1 minute)

port-timeout: 0 (never)

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

When port translation is configured, there is finer control over translation entry timeouts because each entry contains more context about the traffic that is using it. Non-DNS UDP translations time out after 5 minutes, while DNS times out in 1 minute. TCP translations timeout in 24 hours, unless an RST or FIN is seen on the stream, in which case they will time out in 1 minute.

Examples

The following example causes UDP port translation entries to time out after 10 minutes:

```
ip nat translation udp-timeout 600
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip netmask-format

To specify the format in which netmasks are displayed in **show** command output, use the **ip netmask-format** line configuration command. To restore the default display format, use the **no** form of this command.

ip netmask-format {**bit-count** | **decimal** | **hexadecimal**}

no ip netmask-format {**bit-count** | **decimal** | **hexadecimal**}

Syntax Description

bit-count	Addresses are followed by a slash and the total number of bits in the netmask. For example, 131.108.11.0/24 indicates that the netmask is 24 bits.
decimal	Network masks are displayed in dotted-decimal notation (for example, 255.255.255.0).
hexadecimal	Network masks are displayed in hexadecimal format, as indicated by the leading 0X (for example, 0XFFFFFF00).

Defaults

Netmasks are displayed in dotted-decimal format.

Command Modes

Line configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

IP uses a 32-bit mask that indicates which address bits belong to the network and subnetwork fields, and which bits belong to the host field. This is called a *netmask*. By default, **show** commands display an IP address and then its netmask in dotted decimal notation. For example, a subnet would be displayed as 131.108.11.0 255.255.255.0.

However, you can specify that the display of the network mask appear in hexadecimal format or bit count format instead. The hexadecimal format is commonly used on UNIX systems. The previous example would be displayed as 131.108.11.0 0XFFFFFF00.

The bitcount format for displaying network masks is to append a slash (/) and the total number of bits in the netmask to the address itself. The previous example would be displayed as 131.108.11.0/24.

Examples

The following example configures network masks for the specified line to be displayed in bitcount notation in the output of **show** commands:

```
line vty 0 4
 ip netmask-format bitcount
```

ip nhrp authentication

To configure the authentication string for an interface using the Next Hop Resolution Protocol (NHRP), use the **ip nhrp authentication** interface configuration command. To remove the authentication string, use the **no** form of this command.

ip nhrp authentication *string*

no ip nhrp authentication [*string*]

Syntax Description

string	Authentication string configured for the source and destination stations that controls whether NHRP stations allow intercommunication. The string can be up to eight characters long.

Defaults

No authentication string is configured; the Cisco IOS software adds no authentication option to NHRP packets it generates.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

All routers configured with NHRP within one logical NBMA network must share the same authentication string.

Examples

In the following example, the authentication string named specialxx must be configured in all devices using NHRP on the interface before NHRP communication occurs:

```
ip nhrp authentication specialxx
```

ip nhrp holdtime

To change the number of seconds that Next Hop Resolution Protocol (NHRP) nonbroadcast multiaccess (NBMA) addresses are advertised as valid in authoritative NHRP responses, use the **ip nhrp holdtime** interface configuration command. To restore the default value, use the **no** form of this command.

ip nhrp holdtime *seconds*

no ip nhrp holdtime [*seconds*]

Syntax Description

seconds	Time in seconds that NBMA addresses are advertised as valid in positive authoritative NHRP responses.

Defaults

7200 seconds (2 hours)

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The **ip nhrp holdtime** command affects authoritative responses only. The advertised holding time is the length of time the Cisco IOS software tells other routers to keep information that it is providing in authoritative NHRP responses. The cached IP-to-NBMA address mapping entries are discarded after the holding time expires.

The NHRP cache can contain static and dynamic entries. The static entries never expire. Dynamic entries expire regardless of whether they are authoritative or nonauthoritative.

Examples

In the following example, NHRP NBMA addresses are advertised as valid in positive authoritative NHRP responses for 1 hour:

```
ip nhrp holdtime 3600
```

ip nhrp interest

To control which IP packets can trigger sending a Next Hop Resolution Protocol (NHRP) request packet, use the **ip nhrp interest** interface configuration command. To restore the default value, use the **no** form of this command.

ip nhrp interest *access-list-number*

no ip nhrp interest [*access-list-number*]

Syntax Description

access-list-number	Standard or extended IP access list number in the range from 1 to 199.

Defaults

All non-NHRP packets can trigger NHRP requests.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Use this command with the **access-list** command to control which IP packets trigger NHRP requests.

The **ip nhrp interest** command controls *which* packets cause NHRP address resolution to take place; the **ip nhrp use** command controls *how readily* the system attempts such address resolution.

Examples

In the following example, any TCP traffic can cause NHRP requests to be sent, but no other IP packets will cause NHRP requests:

```
ip nhrp interest 101
access-list 101 permit tcp any any
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
ip nhrp use	Configures the software so that NHRP is deferred until the system has attempted to send data traffic to a particular destination multiple times.

ip nhrp map

To statically configure the IP-to-NonBroadcast MutiAccess (NBMA) address mapping of IP destinations connected to an MBMA network, use the **ip nhrp map** interface configuration command. To remove the static entry from Next Hop Resolution Protocol (NHRP) cache, use the **no** form of this command.

ip nhrp map *ip-address nbma-address*

no ip nhrp map *ip-address nbma-address*

Syntax Description

ip-address	IP address of the destinations reachable through the NBMA network. This address is mapped to the NBMA address.
nbma-address	NBMA address that is directly reachable through the NBMA network. The address format varies depending on the medium you are using. For example, ATM has a Network Service Access Point (NSAP) address, Ethernet has a MAC address, and Switched Multimegabit Data Service (SMDS) has an E.164 address. This address is mapped to the IP address.

Defaults

No static IP-to-NBMA cache entries exist.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

You will probably need to configure at least one static mapping in order to reach the Next Hop Server. Repeat this command to statically configure multiple IP-to-NBMA address mappings.

Examples

In the following example, this station in a multipoint tunnel network is statically configured to be served by two Next Hop Servers 100.0.0.1 and 100.0.1.3. The NBMA address for 100.0.0.1 is statically configured to be 11.0.0.1 and the NBMA address for 100.0.1.3 is 12.2.7.8.

```
interface tunnel 0
 ip nhrp nhs 100.0.0.1
 ip nhrp nhs 100.0.1.3
 ip nhrp map 100.0.0.1 11.0.0.1
 ip nhrp map 100.0.1.3 12.2.7.8
```

Related Commands

Command	Description
clear ip nhrp	Clears all dynamic entries from the NHRP cache.

ip nhrp map multicast

To configure NonBroadcast MultiAccess (NBMA) addresses used as destinations for broadcast or multicast packets to be sent over a tunnel network, use the **ip nhrp map multicast** interface configuration command. To remove the destinations, use the **no** form of this command.

ip nhrp map multicast *nbma-address*

no ip nhrp map multicast *nbma-address*

Syntax Description

nbma-address	NBMA address that is directly reachable through the NBMA network. The address format varies depending on the medium you are using.

Defaults

No NBMA addresses are configured as destinations for broadcast or multicast packets.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This command applies only to tunnel interfaces.

The command is useful for supporting broadcasts over a tunnel network when the underlying network does not support IP multicast. If the underlying network does support IP multicast, you should use the **tunnel destination** command to configure a multicast destination for transmission of tunnel broadcasts or multicasts.

When multiple NBMA addresses are configured, the system replicates the broadcast packet for each address.

Examples

In the following example, if a packet is sent to 10.255.255.255, it is replicated to destinations 11.0.0.1 and 11.0.0.2. Addresses 11.0.0.1 and 11.0.0.2 are the IP addresses of two other routers that are part of the tunnel network, but those addresses are their addresses in the underlying network, not the tunnel network. They would have tunnel addresses that are in network 10.0.0.0.

```
interface tunnel 0
 ip address 10.0.0.3 255.0.0.0
 ip nhrp map multicast 11.0.0.1
 ip nhrp map multicast 11.0.0.2
```

ip nhrp max-send

To change the maximum frequency at which Next Hop Resolution Protocol (NHRP) packets can be sent, use the **ip nhrp max-send** interface configuration command. To restore this frequency to the default value, use the **no** form of this command.

ip nhrp max-send *pkt-count* **every** *interval*

no ip nhrp max-send

Syntax Description

pkt-count	Number of packets that can be sent in the range from 1 to 65535. Default is 5 packets.
every *interval*	Time (in seconds) in the range from 10 to 65535. Default is 10 seconds.

Defaults

pkt-count: 5 packets

interval: 10 seconds

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

The software maintains a per-interface quota of NHRP packets that can be sent. NHRP traffic, whether locally generated or forwarded, cannot be sent at a rate that exceeds this quota. The quota is replenished at the rate specified by the *interval value*.

Examples

In the following example, only one NHRP packet can be sent from serial interface 0 each minute:

```
interface serial 0
 ip nhrp max-send 1 every 60
```

Related Commands

Command	Description
ip nhrp interest	Controls which IP packets can trigger sending an NHRP request.
ip nhrp use	Configures the software so that NHRP is deferred until the system has attempted to send data traffic to a particular destination multiple times.

ip nhrp network-id

To enable the Next Hop Resolution Protocol (NHRP) on an interface, use the **ip nhrp network-id** interface configuration command. To disable NHRP on the interface, use the **no** form of this command.

ip nhrp network-id *number*

no ip nhrp network-id [*number*]

Syntax Description

number	Globally unique, 32-bit network identifier from a nonbroadcast multiaccess (NBMA) network. The range is from 1 to 4294967295.

Defaults

NHRP is disabled on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

In general, all NHRP stations within one logical NBMA network must be configured with the same network identifier.

Examples

The following example enables NHRP on the interface:

```
ip nhrp network-id 1
```

ip nhrp nhs

To specify the address of one or more Next Hop Resolution Protocol (NHRP) servers, use the **ip nhrp nhs** interface configuration command. To remove the address, use the **no** form of this command.

ip nhrp nhs *nhs-address* [*net-address* [*netmask*]]

no ip nhrp nhs *nhs-address* [*net-address* [*netmask*]]

Syntax Description

nhs-address	Address of the Next Hop Server being specified.
net-address	(Optional) IP address of a network served by the Next Hop Server.
netmask	(Optional) IP network mask to be associated with the *net* IP address. The *net* IP address is logically ANDed with the mask.

Defaults

No Next Hop Servers are explicitly configured, so normal network layer routing decisions are used to forward NHRP traffic.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Use this command to specify the address of a Next Hop Server and the networks it serves. Normally, NHRP consults the network layer forwarding table to determine how to forward NHRP packets. When Next Hop Servers are configured, these next hop addresses override the forwarding path that would otherwise be used for NHRP traffic.

For any Next Hop Server that is configured, you can specify multiple networks that it serves by repeating this command with the same *nhs-address* argument, but with different *net-address* IP network addresses.

Examples

In the following example, the Next Hop Server with address 131.108.10.11 serves IP network 10.0.0.0. The mask is 255.0.0.0.

```
ip nhrp nhs 131.108.10.11 10.0.0.0 255.0.0.0
```

ip nhrp record

To reenable the use of forward record and reverse record options in Next Hop Resolution Protocol (NHRP) request and reply packets, use the **ip nhrp record** interface configuration command. To suppress the use of such options, use the **no** form of this command.

ip nhrp record

no ip nhrp record

Syntax Description

This command has no arguments or keywords.

Defaults

Forward record and reverse record options are used in NHRP request and reply packets.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Forward record and reverse record options provide loop detection and are enabled by default. Using the **no** form of this command disables this method of loop detection. For another method of loop detection, see the **ip nhrp responder** command.

Examples

The following example suppresses forward record and reverse record options:

```
no ip nhrp record
```

Related Commands

Command	Description
ip nhrp responder	Designates the primary IP address of which interface the Next Hop Server will use in NHRP reply packets when the NHRP requester uses the Responder Address option.

ip nhrp responder

To designate the primary IP address the Next Hop Server that an interface will use in Next Hop Resolution Protocol (NHRP) reply packets when the NHRP requestor uses the Responder Address option, use the **ip nhrp responder** interface configuration command. To remove the designation, use the **no** form of this command.

ip nhrp responder *type number*

no ip nhrp responder [*type*] [*number*]

Syntax Description

type	Interface type whose primary IP address is used when a Next Hop Server complies with a Responder Address option (for example, **serial** or **tunnel**).
number	Interface number whose primary IP address is used when a Next Hop Server complies with a Responder Address option.

Defaults

The Next Hop Server uses the IP address of the interface where the NHRP request was received.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

If an NHRP requestor wants to know which Next Hop Server generates an NHRP reply packet, it can request that information through the Responder Address option. The Next Hop Server that generates the NHRP reply packet then complies by inserting its own IP address in the Responder Address option of the NHRP reply. The Next Hop Server uses the primary IP address of the specified interface.

If an NHRP reply packet being forwarded by a Next Hop Server contains the IP address of that Next Hop Server, the Next Hop Server generates an Error Indication of type “NHRP Loop Detected” and discards the reply packet.

Examples

In the following example, any NHRP requests for the Responder Address will cause this router acting as a Next Hop Server to supply the primary IP address of serial interface 0 in the NHRP reply packet:

```
ip nhrp responder serial 0
```

ip nhrp server-only

To configure the interface to operate in Next Hop Resolution Protocol (NHRP) server-only mode, use the **ip nhrp server-only** interface configuration command. To disable this feature, use the **no** form of this command.

ip nhrp server-only [**non-caching**]

no ip nhrp server-only

Syntax Description

non-caching	(Optional) The router will not cache NHRP information received on this interface.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0	The **non-caching** keyword was added.

Usage Guidelines

When the interface is operating in NHRP server-only mode, the interface does not originate NHRP requests or set up an NHRP shortcut Switched Virtual Circuit (SVC).

Examples

The following example configures the interface to operate in server-only mode:

```
ip nhrp server-only
```

ip nhrp trigger-svc

To configure when the Next Hop Resolution Protocol (NHRP) will set up and tear down a switched virtual circuit (SVC) based on aggregate traffic rates, use the **ip nhrp trigger-svc** interface configuration command. To restore the default thresholds, use the **no** form of this command.

ip nhrp trigger-svc *trigger-threshold teardown-threshold*

no ip nhrp trigger-svc

Syntax Description

trigger-threshold	Average traffic rate calculated during the load interval, at or above which NHRP will set up an SVC for a destination. The default value is 1 kbps.
teardown-threshold	Average traffic rate calculated during the load interval, at or below which NHRP will tear down the SVC to the destination. The default value is 0 kbps.

Defaults

trigger-threshold: 1 kbps

teardown-threshold: 0 kbps

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The two thresholds are measured during a sampling interval of 30 seconds, by default. To change that interval, use the **load-interval** *seconds* argument of the **ip cef traffic-statistics** command.

Examples

In the following example, the triggering and teardown thresholds are set to 100 kbps and 5 kbps, respectively:

```
ip nhrp trigger-svc 100 5
```

Related Commands

Command	Description
ip cef	Enables CEF on the route processor card.
ip cef accounting	Enables network accounting of CEF information.
ip cef traffic-statistics	Changes the time interval that controls when NHRP will set up or tear down an SVC.
ip nhrp interest	Controls which IP packets can trigger sending an NHRP request.

ip nhrp use

To configure the software so that Next Hop Resolution Protocol (NHRP) is deferred until the system has attempted to send data traffic to a particular destination multiple times, use the **ip nhrp use** interface configuration command. To restore the default value, use the **no** form of this command.

ip nhrp use *usage-count*

no ip nhrp use *usage-count*

Syntax Description

usage-count	Packet count in the range from 1 to 65535. Default is 1.

Defaults

usage-count: 1. The first time a data packet is sent to a destination for which the system determines NHRP can be used, an NHRP request is sent.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

When the software attempts to send a data packet to a destination for which it has determined that NHRP address resolution can be used, an NHRP request for that destination is normally sent immediately. Configuring the *usage-count* argument causes the system to wait until that many data packets have been sent to a particular destination before it attempts NHRP. The *usage-count* argument for a particular destination is measured over 1-minute intervals (the NHRP cache expiration interval).

The usage count applies *per destination*. So if the *usage-count* argument is configured to be 3, and four data packets are sent toward 10.0.0.1 and one packet toward 10.0.0.2, then an NHRP request is generated for 10.0.0.1 only.

If the system continues to need to forward data packets to a particular destination, but no NHRP response has been received, retransmission of NHRP requests is performed. This retransmission occurs only if data traffic continues to be sent to a destination.

The **ip nhrp interest** command controls *which* packets cause NHRP address resolution to take place; the **ip nhrp use** command controls *how readily* the system attempts such address resolution.

Examples

In the following example, if in the first minute five packets are sent to the first destination and five packets are sent to a second destination, then a single NHRP request is generated for the second destination.

If in the second minute the same traffic is generated and no NHRP responses have been received, then the system resends its request for the second destination.

```
ip nhrp use 5
```

Related Commands

Command	Description
ip nhrp interest	Controls which IP packets can trigger sending an NHRP request.
ip nhrp max-send	Changes the maximum frequency at which NHRP packets can be sent.

ip probe proxy

To enable the HP Probe Proxy support, which allows the Cisco IOS software to respond to HP Probe Proxy name requests, use the **ip probe proxy** interface configuration command. To disable HP Probe Proxy, use the **no** form of this command.

ip probe proxy

no ip probe proxy

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

HP Probe Proxy Name requests are typically used at sites that have Hewlett-Packard (HP) equipment and are already using HP Probe.

To use the HP Probe Proxy service, you must first enter the host name of the HP host into the host table using the **ip hp-host** global configuration command.

Examples

The following example specifies an HP host name and address, and then enables Probe Proxy:

```
ip hp-host BCWjo 131.108.1.27
interface ethernet 0
ip probe proxy
```

Related Commands

Command	Description
ip hp-host	Enters into the host table the host name of an HP host to be used for HP Probe Proxy service.

ip proxy-arp

To enable proxy Address Resolution Protocol (ARP) on an interface, use the **ip proxy-arp** interface configuration command. To disable proxy ARP on the interface, use the **no** form of this command.

ip proxy-arp

no ip proxy-arp

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example enables proxy ARP on Ethernet interface 0:

```
interface ethernet 0
ip proxy-arp
```

ip routing

To enable IP routing, use the **ip routing** global configuration command. To disable IP routing, use the **no** form of this command.

ip routing

no ip routing

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

To bridge IP, the **no ip routing** command must be configured to disable IP routing. However, you need not specify **no ip routing** in conjunction with concurrent routing and bridging to bridge IP.

The ip routing command is disabled on the Cisco VG200 voice over IP gateway.

Examples

The following example enables IP routing:

```
ip routing
```

ip subnet-zero

To enable the use of subnet 0 for interface addresses and routing updates, use the **ip subnet-zero** global configuration command. To restore the default, use the **no** form of this command.

ip subnet-zero

no ip subnet-zero

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **ip subnet-zero** command provides the ability to configure and route to subnet 0 subnets.

Subnetting with a subnet address of 0 is discouraged because of the confusion inherent in having a network and a subnet with indistinguishable addresses.

Examples

The following example enables subnet zero:

```
ip subnet-zero
```

ip unnumbered

To enable IP processing on a serial interface without assigning an explicit IP address to the interface, use the **ip unnumbered** interface configuration command. To disable the IP processing on the interface, use the **no** form of this command.

ip unnumbered *type number*

no ip unnumbered *type number*

Syntax Description

type number	Type and number of another interface on which the router has an assigned IP address. It cannot be another unnumbered interface.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Whenever the unnumbered interface generates a packet (for example, for a routing update), it uses the address of the specified interface as the source address of the IP packet. It also uses the address of the specified interface in determining which routing processes are sending updates over the unnumbered interface. Restrictions include the following:

- Serial interfaces using High Level Data Link Control (HDLC), PPP, Link Access Procedure, Balanced (LAPB), Frame Relay encapsulations, and Serial Line Internet Protocol (SLIP) and tunnel interfaces can be unnumbered. It is not possible to use this interface configuration command with X.25 or Switched Multimegabit Data Service (SMDS) interfaces.
- You cannot use the **ping** EXEC command to determine whether the interface is up, because the interface has no address. Simple Network Management Protocol (SNMP) can be used to remotely monitor interface status.
- You cannot netboot a runnable image over an unnumbered serial interface.
- You cannot support IP security options on an unnumbered interface.

The interface you specify by the *type* and *number* arguments must be enabled (listed as "up" in the **show interfaces** command display).

If you are configuring Intermediate System-to-Intermediate System (IS-IS) across a serial line, you should configure the serial interfaces as unnumbered, which allows you to conform with RFC 1195, which states that IP addresses are not required on each interface.

Note Using an unnumbered serial line between different major networks (or *majornets*) requires special care. If at each end of the link there are different majornets assigned to the interfaces you specified as unnumbered, then any routing protocol running across the serial line must not advertise subnet information.

Examples

In the following example, the first serial interface is given the address of Ethernet 0:

```
interface ethernet 0
 ip address 131.108.6.6 255.255.255.0
!
interface serial 0
 ip unnumbered ethernet 0
```

no ip gratuitous-arps

To disable the transmission of gratuitous Address Resolution Protocol (ARP) messages for an address in a local pool, use the **no ip gratuitous-arps** command in global configuration mode.

no ip gratuitous-arps

Syntax Description

This command has no keywords or arguments.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

A Cisco router will send out a gratuitous ARP message when a client connects and negotiates an address over a PPP connection. This transmission occurs even when the client receives the address from a local address pool.

Examples

The following example disables gratuitous arp messages from being sent:

```
no ip gratuitous-arps
```

show arp

To display the entries in the Address Resolution Protocol (ARP) table, use the **show arp** privileged EXEC command.

show arp

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

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

```
Router# show arp

Protocol   Address          Age (min)   Hardware Addr    Type    Interface

Internet   131.108.42.112   120         0000.a710.4baf   ARPA    Ethernet3
AppleTalk  4028.5           29          0000.0c01.0e56   SNAP    Ethernet2
Internet   131.108.42.114   105         0000.a710.859b   ARPA    Ethernet3
AppleTalk  4028.9           -           0000.0c02.a03c   SNAP    Ethernet2
Internet   131.108.42.121   42          0000.a710.68cd   ARPA    Ethernet3
Internet   131.108.36.9     -           0000.3080.6fd4   SNAP    TokenRing0
AppleTalk  4036.9           -           0000.3080.6fd4   SNAP    TokenRing0
Internet   131.108.33.9     -           0000.0c01.7bbd   SNAP    Fddi0
```

Table 3 describes the significant fields shown in the display.

Table 3 show arp Field Descriptions

Field	Description
Protocol	Protocol for network address in the Address field.
Address	The network address that corresponds to the Hardware Address.
Age (min)	Age in munutes of the cache entryh. A hyphen (-) means the address is local.
Hardware Addr	LAN hardware address of a MAC address that corresponds to the network address.

Table 3 show arp Field Descriptions (continued)

Field	Description
Type	Indicates the encapsulation type the Cisco IOS software is using for the network address in this entry. Possible values include: • ARPA • SNAP • ETLK (EtherTalk) • SMDS
Interface	Indicates the interface associated with this network address.

show hosts

To display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses, use the **show hosts** EXEC command.

show hosts

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

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

```
Router# show hosts

Default domain is CISCO.COM
Name/address lookup uses domain service
Name servers are 255.255.255.255
Host              Flag        Age   Type       Address(es)
SLAG.CISCO.COM    (temp, OK)  1     IP         131.108.4.10
CHAR.CISCO.COM    (temp, OK)  8     IP         192.31.7.50
CHAOS.CISCO.COM   (temp, OK)  8     IP         131.108.1.115
DIRT.CISCO.COM    (temp, EX)  8     IP         131.108.1.111
DUSTBIN.CISCO.COM (temp, EX)  0     IP         131.108.1.27
DREGS.CISCO.COM   (temp, EX)  24    IP         131.108.1.30
```

Table 4 describes the significant fields shown in the display.

Table 4 show hosts Field Descriptions

Field	Description
Flag	A temporary entry is entered by a name server; the Cisco IOS software removes the entry after 72 hours of inactivity. A permanent entry is entered by a configuration command and is not timed out. Entries marked OK are believed to be valid. Entries marked?? are considered suspect and subject to revalidation. Entries marked EX are expired.
Age	Indicates the number of hours since the software last referred to the cache entry.
Type	Identifies the type of address, for example, IP, Connectionless Network Service (CLNS), or X.121. If you have used the **ip hp-host** global configuration command, the **show hosts** command will display these host names as type HP-IP.
Address(es)	Displays the address of the host. One host may have up to eight addresses.

Related Commands

Command	Description
clear host	Deletes entries from the host name-to-address cache.

show ip aliases

To display the IP addresses mapped to TCP ports (aliases) and Serial Line Internet Protocol (SLIP) addresses, which are treated similarly to aliases, use the **show ip aliases** EXEC command.

show ip aliases

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

To distinguish a SLIP address from a normal alias address, the command output uses the form SLIP TTY1 for the "port" number, where 1 is the auxiliary port.

Examples

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

```
Router# show ip aliases

 IP Address    Port
131.108.29.245 SLIP TTY1
```

The display lists the IP address and corresponding port number.

Related Commands

Command	Description
show line	Displays the parameters of a terminal line.

show ip arp

To display the Address Resolution Protocol (ARP) cache, where Serial Line Internet Protocol (SLIP) addresses appear as permanent ARP table entries, use the **show ip arp** EXEC command.

show ip arp [*ip-address*] [*host-name*] [*mac-address*] [*interface type number*]

Syntax Description

ip-address	(Optional) ARP entries matching this IP address are displayed.
host-name	(Optional) Host name.
mac-address	(Optional) 48-bit MAC address.
interface type number	(Optional) ARP entries learned via this interface type and number are displayed.

Command Modes

EXEC

Command History

Release	Modification
9.0	This command was introduced.

Usage Guidelines

ARP establishes correspondences between network addresses (an IP address, for example) and LAN hardware addresses (Ethernet addresses). A record of each correspondence is kept in a cache for a predetermined amount of time and then discarded.

Examples

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

```
Router# show ip arp

Protocol  AddressAge(min)  Hardware Addr  Type   Interface
Internet  171.69.233.2290000.0c59.f892 ARPA   Ethernet0/0
Internet  171.69.233.2180000.0c07.ac00 ARPA   Ethernet0/0
Internet  171.69.233.19-0000.0c63.1300 ARPA   Ethernet0/0
Internet  171.69.233.3090000.0c36.6965 ARPA   Ethernet0/0
Internet  172.19.168.11-0000.0c63.1300 ARPA   Ethernet0/0
Internet  172.19.168.25490000.0c36.6965 ARPA   Ethernet0/0
```

Table 5 describes the significant fields shown in the display.

Table 5 show ip arp Field Descriptions

Field	Description
Protocol	Protocol for network address in the Address field.
Address	The network address that corresponds to the Hardware Address.
Age (min)	Age in minutes of the cache entry. A hyphen (-) means the address is local.
Hardware Addr	LAN hardware address of a MAC address that corresponds to the network address.

Table 5 show ip arp Field Descriptions (continued)

Field	Description
Type	Indicates the encapsulation type the Cisco IOS software is using the network address in this entry. Possible value include: • ARPA • SNAP • SAP
Interface	Indicates the interface associated with this network address.

show ip interface

To display the usability status of interfaces configured for IP, use the **show ip interface** EXEC command.

show ip interface [*type number*] [**brief**]

Syntax Description

type	(Optional) Interface type.
number	(Optional) Interface number.
brief	(Optional) Displays a summary of the usability status information for each interface.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	This command was expanded to include the status of **ip wccp redirect out** and **ip wccp redirect exclude add in** commands.

Usage Guidelines

The Cisco IOS software automatically enters a directly connected route in the routing table if the interface is usable. A usable interface is one through which the software can send and receive packets. If the software determines that an interface is not usable, it removes the directly connected routing entry from the routing table. Removing the entry allows the software to use dynamic routing protocols to determine backup routes to the network, if any.

If the interface can provide two-way communication, the line protocol is marked "up." If the interface hardware is usable, the interface is marked "up."

If you specify an optional interface type, you will see only information on that specific interface.

If you specify no optional arguments, you will see information on all the interfaces.

When an asynchronous interface is encapsulated with PPP or Serial Line Internet Protocol (SLIP), IP fast switching is enabled. A **show ip interface** command on an asynchronous interface encapsulated with PPP or SLIP displays a message indicating that IP fast switching is enabled.

Examples

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

```
Router# show ip interface

Ethernet0 is up, line protocol is up
  Internet address is 192.195.78.24, subnet mask is 255.255.255.240
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Secondary address 131.192.115.2, subnet mask 255.255.255.0
  Directed broadcast forwarding is enabled
  Multicast groups joined: 224.0.0.1 224.0.0.2
```

```
Outgoing access list is not set
Inbound  access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP SSE switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
Probe proxy name replies are disabled
WCCP Redirect outbound is enabled
WCCP Redirect exclude is disabled
```

Table 6 describes the significant fields shown in the display.

Table 6 show ip interface Field Descriptions

Field	Description
Ethernet0 is up	If the interface hardware is usable, the interface is marked “up.” For an interface to be usable, both the interface hardware and line protocol must be up.
line protocol is up	If the interface can provide two-way communication, the line protocol is marked “up.” For an interface to be usable, both the interface hardware and line protocol must be up.
Internet address and subnet mask	IP Internet address and subnet mask of the interface.
Broadcast address	Displays the broadcast address.
Address determined by...	Indicates how the IP address of the interface was determined.
MTU	Displays the MTU value set on the interface.
Helper address	Displays a helper address, if one has been set.
Secondary address	Displays a secondary address, if one has been set.
Directed broadcast forwarding	Indicates whether directed broadcast forwarding is enabled.
Multicast groups joined	Indicates the multicast groups this interface is a member of.
Outgoing access list	Indicates whether the interface has an outgoing access list set.
Inbound access list	Indicates whether the interface has an incoming access list set.
Proxy ARP	Indicates whether Proxy Address Resolution Protocol (ARP) is enabled for the interface.
Security level	Specifies the IP Security Option (IPSO) security level set for this interface.
Split horizon	Indicates that split horizon is enabled.
ICMP redirects	Specifies whether redirect messages will be sent on this interface.
ICMP unreachables	Specifies whether unreachable messages will be sent on this interface.
ICMP mask replies	Specifies whether mask replies will be sent on this interface.

Table 6 show ip interface Field Descriptions (continued)

Field	Description
IP fast switching	Specifies whether fast switching has been enabled for this interface. It is generally enabled on serial interfaces, such as this one.
IP SSE switching	Specifies whether IP silicon switching engine (SSE) is enabled.
Router Discovery	Specifies whether the discovery process has been enabled for this interface. It is generally disabled on serial interfaces.
IP output packet accounting	Specifies whether IP accounting is enabled for this interface and what the threshold (maximum number of entries) is.
TCP/IP header compression	Indicates whether compression is enabled or disabled.
Probe proxy name	Indicates whether HP Probe proxy name replies are generated.
WCCP Redirect outbound is enabled	Indicates the status of whether packets received on an interface are redirected to a cache engine. Displays “enabled” or “disabled.”
WCCP Redirect exclude is disabled	Indicates the status of whether packets targeted for an interface will be excluded from being redirected to a cache engine. Displays “enabled” or “disabled.”

The following is sample output from the **show ip interface brief** command:

```
Router# show ip interface brief

Interface      IP-Address      OK?  Method  Status                  Protocol
Ethernet0      151.108.0.5     YES  NVRAM   up                      up
Ethernet1      unassigned      YES  unset   administratively down   down
Loopback0      152.108.20.5    YES  NVRAM   up                      up
Serial0        162.108.10.5    YES  NVRAM   up                      up
Serial1        162.108.4.5     YES  NVRAM   up                      up
Serial2        152.108.10.5    YES  manual  up                      up
Serial3        unassigned      YES  unset   administratively down   down
```

The **method** field has the following possible values:

- RARP or SLARP—Reverse Address Resolution Protocol (RARP) or SLARP request
- BOOTP—Bootstrap protocol
- TFTP—Configuration file obtained from Trivial File Transfer Protocol (TFTP) server
- manual—Manually changed by CLI command
- NVRAM—Configuration file in nonvolatile RAM (NVRAM)
- IPCP—**ip address negotiated** command
- DHCP—**ip address dhcp** command
- unassigned—No IP address
- unset—Unset
- other—Unknown

show ip irdp

To display ICMP Router Discovery Protocol (HRDP) values, use the **show ip irdp** EXEC command.

show ip irdp

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

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

```
Router# show ip irdp

Ethernet 0 has router discovery enabled

Advertisements will occur between every 450 and 600 seconds.
Advertisements are valid for 1800 seconds.
Default preference will be 100.
 --More--
Serial 0 has router discovery disabled
 --More--
Ethernet 1 has router discovery disabled
```

As the display shows, **show ip irdp** output indicates whether router discovery has been configured for each router interface, and it lists the values of router discovery configurables for those interfaces on which router discovery has been enabled. Explanations for the less obvious lines of output in the display are as follows:

```
Advertisements will occur between every 450 and 600 seconds.
```

This indicates the configured minimum and maximum advertising interval for the interface.

```
Advertisements are valid for 1800 seconds.
```

This indicates the configured holdtime values for the interface.

```
Default preference will be 100.
```

This indicates the configured (or in this case default) preference value for the interface.

Related Commands

Command	Description
ip irdp	Enables IRDP processing on an interface.

show ip masks

To display the masks used for network addresses and the number of subnets using each mask, use the **show ip masks** EXEC command.

show ip masks *address*

Syntax Description

address	Network address for which a mask is required.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **show ip masks** command is useful for debugging when a variable-length subnet mask (VLSM) is used. It shows the number of masks associated with the network and the number of routes for each mask.

Examples

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

```
Router# show ip masks 131.108.0.0

Mask            Reference count
255.255.255.255 2
255.255.255.0   3
255.255.0.0     1
```

show ip nat statistics

To display Network Address Translation (NAT) statistics, use the **show ip nat statistics** EXEC command.

show ip nat statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Examples

The following is sample output from the **show ip nat statistics** command:

```
Router# show ip nat statistics

Total translations: 2 (0 static, 2 dynamic; 0 extended)
Outside interfaces: Serial0
Inside interfaces: Ethernet1
Hits: 135  Misses: 5
Expired translations: 2
Dynamic mappings:
-- Inside Source
access-list 1 pool net-208 refcount 2
 pool net-208: netmask 255.255.255.240
        start 171.69.233.208 end 171.69.233.221
        type generic, total addresses 14, allocated 2 (14%), misses 0
```

Table 7 describes the significant fields shown in the display.

Table 7 show ip nat statistics Field Descriptions

Field	Description
Total translations	Number of translations active in the system. This number is incremented each time a translation is created and is decremented each time a translation is cleared or times out.
Outside interfaces	List of interfaces marked as outside with the **ip nat outside** command.
Inside interfaces	List of interfaces marked as inside with the **ip nat inside** command.
Hits	Number of times the software does a translations table lookup and finds an entry.
Misses	Number of times the software does a translations table lookup, fails to find an entry, and must try to create one.

Table 7 show ip nat statistics Field Descriptions (continued)

Field	Description
Expired translations	Cumulative count of translations that have expired since the router was booted.
Dynamic mappings	Indicates that the information that follows is about dynamic mappings.
Inside Source	The information that follows is about an inside source translation.
access-list	Access list number being used for the translation.
pool	Name of the pool (in this case, net-208).
refcount	Number of translations using this pool.
netmask	IP network mask being used in the pool.
start	Starting IP address in the pool range.
end	Ending IP address in the pool range.
type	Type of pool. Possible types are generic or rotary.
total addresses	Number of addresses in the pool available for translation.
allocated	Number of addresses being used.
misses	Number of failed allocations from the pool.

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Changes the amount of time after which NAT translations time out.
show ip nat translations	Displays active NAT translations.

show ip nat translations

To display active Network Address Translation (NAT) translations, use the **show ip nat translations** EXEC command.

show ip nat translations [**verbose**]

Syntax Description

verbose	(Optional) Displays additional information for each translation table entry, including how long ago the entry was created and used.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Examples

The following is sample output from the **show ip nat translations** command. Without overloading, two inside hosts are exchanging packets with some number of outside hosts.

```
Router# show ip nat translations

Pro Inside global      Inside local       Outside local      Outside global
--- 171.69.233.209     192.168.1.95       ---                ---
--- 171.69.233.210     192.168.1.89       ---                --
```

With overloading, a translation for a Domain Name Server (DNS) transaction is still active, and translations for two Telnet sessions (from two different hosts) are also active. Note that two different inside hosts appear on the outside with a single IP address.

```
Router# show ip nat translations

Pro Inside global        Inside local       Outside local      Outside global
udp 171.69.233.209:1220  192.168.1.95:1220  171.69.2.132:53    171.69.2.132:53
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23    171.69.1.220:23
tcp 171.69.233.209:1067  192.168.1.95:1067  171.69.1.161:23    171.69.1.161:23
```

The following is sample output that includes the **verbose** keyword:

```
Router# show ip nat translations verbose

Pro Inside global        Inside local       Outside local      Outside global
udp 171.69.233.209:1220  192.168.1.95:1220  171.69.2.132:53    171.69.2.132:53
        create 00:00:02, use 00:00:00, flags: extended
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23    171.69.1.220:23
        create 00:01:13, use 00:00:50, flags: extended
tcp 171.69.233.209:1067  192.168.1.95:1067  171.69.1.161:23    171.69.1.161:23
        create 00:00:02, use 00:00:00, flags: extended
```

Table 8 describes the significant fields shown in the display.

Table 8 show ip nat translations Field Descriptions

Field	Description
Pro	Protocol of the port identifying the address.
Inside global	The legitimate IP address that represents one or more inside local IP addresses to the outside world.
Inside local	The IP address assigned to a host on the inside network; probably not a legitimate address assigned by the NIC or service provider.
Outside local	IP address of an outside host as it appears to the inside network; probably not a legitimate address assigned by the NIC or service provider.
Outside global	The IP address assigned to a host on the outside network by its owner.
create	How long ago the entry was created (in hours:minutes:seconds).
use	How long ago the entry was last used (in hours:minutes:seconds).
flags	Indication of the type of translation. Possible flags are: • extended—Extended translation • static—Static translation • destination—Rotary translation • outside—Outside translation • timing out—Translation will no longer be used, due to a TCP finish (FIN) or reset (RST) flag.

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Changes the amount of time after which NAT translations time out.
show ip nat statistics	Displays NAT statistics.

show ip nhrp

To display the Next Hop Resolution Protocol (NHRP) cache, use the **show ip nhrp** EXEC command.

show ip nhrp [**detail** | **purge**] | [*type number* [**detail**]] | [**dynamic** | **incomplete** | **nhs** | **static** [*type number*] [**detail**]]

Syntax Description

detail	(Optional) Displays detailed information about NHRP cache.
purge	(Optional) Displays NHRP cache purge information.
type number	(Optional) Displays the interface type and number in the NHRP cache. See Table 9 for types, number ranges, and descriptions.
dynamic	(Optional) Displays only the dynamic (learned) IP-to-nonbroadcast multiaccess address (NBMA) cache entries. See Table 9 for types, number ranges, and descriptions.
incomplete	(Optional) Displays information about an incomplete cache. See Table 9 for types, number ranges, and descriptions.
nhs	(Optional) Displays information about the next-hop server (NHS). See Table 9 for types, number ranges, and descriptions.
static	(Optional) Displays only the static IP-to-NBMA address entries in the cache (configured using the **ip nhrp map** command). See Table 9 for types, number ranges, and descriptions.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Table 9 lists the valid types, number ranges, and descriptions for the *type* and *number* optional arguments.

Note The valid types can vary according to the platform and interfaces on the platform.

Table 9 Valid Types, Number Ranges, and Interface Descriptions

Valid Types	Number Ranges	Interface Descriptions
async	1	Async
atm	0 to 6	ATM
bvi	1 to 255	Bridge-Group Virtual Interface
cdma-ix	1	CDMA Ix

Table 9 Valid Types, Number Ranges, and Interface Descriptions (continued)

Valid Types	Number Ranges	Interface Descriptions
ctunnel	0 to 2147483647	C-Tunnel
dialer	0 to 20049	Dialer
fastethernet	0 to 6	FastEthernet IEEE 802.3
lex	0 to 2147483647	Lex
loopback	0 to 2147483647	Loopback
mfr	0 to 2147483647	Multilink Frame Relay bundle
multilink	0 to 2147483647	Multilink-group
null	0	Null
port-channel	1 to 64	Port channel
tunnel	0 to 2147483647	Tunnel
vif	1	PGM multicast host
virtual-ppp	0 to 2147483647	Virtual PPP
virtual-template	1 to 1000	Virtual template
virtual-tokenring	0 to 2147483647	Virtual Token Ring
xtagatm	0 to 2147483647	Extended tag ATM

Examples

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

```
Router# show ip nhrp

10.0.0.2 255.255.255.255, ATM0/0 created 0:00:43 expire 1:59:16
  Type: dynamic Flags: authoritative
  NBMA address: 11.1111.1111.1111.1111.1111.1111.1111.1111.1111.11
10.0.0.1 255.255.255.255, Tunnel0 created 0:10:03 expire 1:49:56
  Type: static Flags: authoritative
  NBMA address: 11.1.1.2
```

Table 9 describes the significant fields shown in the display.

Table 10 show ip nhrp Field Descriptions

Field	Description
10.0.0.2 255.255.255.255	IP address and its network mask in the IP-to-NBMA address cache. The mask is currently always 255.255.255.255 because we do not support aggregation of NBMA information through NHRP.
ATM0/0 created 0:00:43	Interface type and number (in this case, ATM slot and port numbers) and how long ago it was created (hours:minutes:seconds).
expire 1:59:16	Time in which the positive and negative authoritative NBMA address will expire (hours:minutes:seconds). This value is based on the **ip nhrp holdtime** command.

Table 10 show ip nhrp Field Descriptions (continued)

Field	Description
Type	• dynamic—NBMA address was obtained from NHRP Request packet. • static—NBMA address was statically configured.
Flags	• authoritative—Indicates that the NHRP information was obtained from the Next Hop Server or router that maintains the NBMA-to-IP address mapping for a particular destination. • implicit—Indicates that the information was learned not from an NHRP request generated from the local router, but from an NHRP packet being forwarded or from an NHRP request being received by the local router. • negative—For negative caching; indicates that the requested NBMA mapping could not be obtained.
NBMA address	Nonbroadcast multiaccess address. The address format is appropriate for the type of network being used (for example, ATM, Ethernet, Switched Multimegabit Data Service (SMDS), or multipoint tunnel).

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.

show ip nhrp traffic

To display Next Hop Resolution Protocol (NHRP) traffic statistics, use the **show ip nhrp traffic** EXEC command.

show ip nhrp traffic

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.

Examples

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

```
Router# show ip nhrp traffic

Tunnel0
  request packets sent: 2
  request packets received: 4
  reply packets sent: 4
  reply packets received: 2
  register packets sent: 0
  register packets received: 0
  error packets sent: 0
  error packets received: 0
```

Table 10 describes the significant fields shown in the display.

Table 11 show ip nhrp traffic Field Descriptions

Field	Description
Tunnel 0	Interface type and number.
request packets sent	Number of NHRP request packets originated from this station.
request packets received	Number of NHRP request packets received by this station.
reply packets sent	Number of NHRP reply packets originated from this station.
reply packets received	Number of NHRP reply packets received by this station.
register packets sent	Number of NHRP register packets originated from this station. Currently, our routers and access servers do not send register packets, so this value is 0.
register packets received	Number of NHRP register packets received by this station. Currently, our routers or access servers do not send register packets, so this value is 0.

Table 11 show ip nhrp traffic Field Descriptions (continued)

Field	Description
error packets sent	Number of NHRP error packets originated by this station.
error packets received	Number of NHRP error packets received by this station.

term ip netmask-format

To specify the format in which netmasks are displayed in **show** command output, use the **term ip netmask-format** EXEC command. To restore the default display format, use the **no** form of this command.

term ip netmask-format {**bitcount** | **decimal** | **hexadecimal**}

no term ip netmask-format [**bitcount** | **decimal** | **hexadecimal**]

Syntax Description

bitcount	Number of bits in the netmask.
decimal	Netmask dotted decimal notation.
hexadecimal	Netmask hexadecimal format.

Defaults

Netmasks are displayed in dotted decimal format.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

IP uses a 32-bit mask that indicates which address bits belong to the network and subnetwork fields, and which bits belong to the host field. This range of IP addresses is called a *netmask*. By default, **show** commands display an IP address and then its netmask in dotted decimal notation. For example, a subnet would be displayed as 131.108.11.55 255.255.255.0.

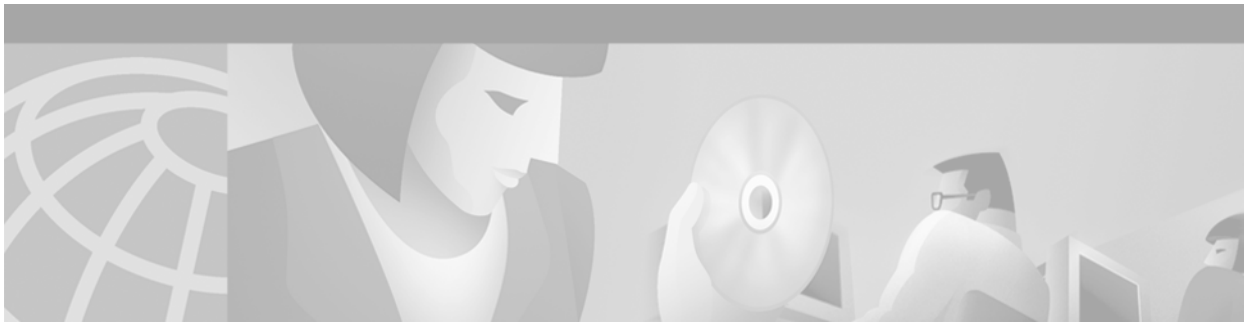
However, you can specify that the display of the network mask appear in hexadecimal format or bit count format instead. The hexadecimal format is commonly used on UNIX systems. The previous example would be displayed as 131.108.11.55 0XFFFFFF00.

The bitcount format for displaying network masks is to append a slash (/) and the total number of bits in the netmask to the address itself. The previous example would be displayed as 131.108.11.55/24.

Examples

The following example specifies that network masks for the session be displayed in bitcount notation in the output of **show** commands:

```
term ip netmask-format bitcount
```



DHCP Commands

Use the commands in this chapter to configure and monitor Dynamic Host Configuration Protocol (DHCP). For DHCP configuration information and examples, refer to the "Configuring DHCP" chapter of the *Cisco IOS IP Configuration Guide*.

bootfile

To specify the name of the default boot image for a Dynamic Host Configuration Protocol (DHCP) client, use the **bootfile** DHCP pool configuration command. To delete the boot image name, use the **no** form of this command.

bootfile *filename*

no bootfile

Syntax Description

filename	Specifies the name of the file that is used as a boot image.

Defaults

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

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

Examples

The following example specifies xllboot as the name of the boot file:

```
bootfile xllboot
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.
next-server	Configures the next server in the boot process of a DHCP client.

clear ip dhcp binding

To delete an automatic address binding from the Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server database, use the **clear ip dhcp binding** privileged EXEC command.

clear ip dhcp binding {*address* | ***** }

Syntax Description

address	The address of the binding you want to clear.
*	Clears all automatic bindings.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Typically, the address denotes the IP address of the client. If the asterisk (*) character is used as the address parameter, DHCP clears all automatic bindings.

Use the **no ip dhcp pool** global configuration command to delete a manual binding.

Examples

The following example deletes the address binding 10.12.1.99 from a DHCP server database:

```
Router# clear ip dhcp binding 10.12.1.99
```

Related Commands

Command	Description
show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP Server.

clear ip dhcp conflict

To clear an address conflict from the Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server database, use the **clear ip dhcp conflict** privileged EXEC command.

clear ip dhcp conflict {*address* | *****}

Syntax Description

address	The IP address of the host that contains the conflicting address you want to clear.
*	Clears all address conflicts.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The server detects conflicts using a ping session. The client detects conflicts using gratuitous Address Resolution Protocol (ARP). If the asterisk (*) character is used as the address parameter, DHCP clears all conflicts.

Examples

The following example shows an address conflict of 10.12.1.99 being deleted from the DHCP server database:

```
Router# clear ip dhcp conflict 10.12.1.99
```

Related Commands

Command	Description
show ip dhcp conflict	Displays address conflicts found by a Cisco IOS DHCP Server when addresses are offered to the client.

clear ip dhcp server statistics

To reset all Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server counters, use the **clear ip dhcp server statistics** privileged EXEC command.

clear ip dhcp server statistics

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.

Usage Guidelines

The **show ip dhcp server statistics** command displays DHCP counters. All counters are cumulative. The counters will be initialized, or set to zero, with the **clear ip dhcp server statistics** command.

Examples

The following example resets all DHCP counters to zero:

```
Router# clear ip dhcp server statistics
```

Related Commands

Command	Description
show ip dhcp server statistics	Displays Cisco IOS DHCP Server statistics.

clear ip route dhcp

To remove routes from the routing table added by the Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server and Relay Agent for the DHCP clients on unnumbered interfaces, use the **clear ip route dhcp** command in EXEC configuration mode.

clear ip route [**vrf** *vrf-name*] **dhcp** [*ip-address*]

Syntax Description

vrf	(Optional) VPN routing and forwarding instance.
vrf-name	(Optional) Name of the VRF.
ip-address	(Optional) Address about which routing information should be removed.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

To remove information about global routes in the routing table, use the **clear ip route dhcp** command. To remove routes in the VRF routing table, use the **clear ip route vrf** *vrf-name* **dhcp** command.

Examples

The following example removes a route to network 55.5.5.217 from the routing table:

```
Router# clear ip route dhcp 55.5.5.217
```

Related Commands

Command	Description
show ip route dhcp	Displays the routes added to the routing table by the Cisco IOS DHCP Server and Relay Agent.

client-identifier

To specify the unique identifier (in dotted hexadecimal notation) for a Microsoft Dynamic Host Configuration Protocol (DHCP) client, use the **client-identifier** DHCP pool configuration command. It is valid for manual bindings only. To delete the client identifier, use the **no** form of this command.

client-identifier *unique-identifier*

no client-identifier

Syntax Description

unique-identifier	The distinct identification of the client in dotted-hexadecimal notation, for example, 01b7.0813.8811.66.

Command Modes

DHCP pool configuration

Command History

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

Usage Guidelines

Microsoft DHCP clients require client identifiers instead of hardware addresses. The client identifier is formed by concatenating the media type and the MAC address. For example, the Microsoft client identifier for Ethernet address b708.1388.f166 is 01b7.0813.88f1.66, where 01 represents the Ethernet media type. For a list of media type codes, refer to the "Address Resolution Protocol Parameters" section of RFC 1700, *Assigned Numbers*.

Examples

The following example specifies the client identifier for MAC address b7.0813.8811.66 in dotted hexadecimal notation:

```
client-identifier 01b7.0813.8811.66
```

Related Commands

Command	Description
hardware-address	Specifies the hardware address of a DHCP client.
host	Specifies the IP address and network mask for a manual binding to a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.

client-name

To specify the name of a DHCP client, use the **client-name** DHCP pool configuration command. The client name should not include the domain name. To remove the client name, use the **no** form of this command.

client-name *name*

no client-name

Syntax Description

name	Specifies the name of the client, using any standard ASCII character. The client name should not include the domain name. For example, the name mars should not be specified as mars.cisco.com.

Command Modes

DHCP pool configuration

Command History

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

Examples

The following example specifies a string client1 that will be the name of the client:

```
client-name client1
```

Related Commands

Command	Description
host	Specifies the IP address and network mask for a manual binding to a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.

default-router

To specify the default router list for a Dynamic Host Configuration Protocol (DHCP) client, use the **default-router** DHCP pool configuration command. To remove the default router list, use the **no** form of this command.

default-router *address* [*address2...address8*]

no default-router

Syntax Description

address	Specifies the IP address of a router. One IP address is required, although you can specify up to eight addresses in one command line.
address2...address8	(Optional) Specifies up to eight addresses in the command line.

Command Modes

DHCP pool configuration

Command History

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

Usage Guidelines

The IP address of the router should be on the same subnet as the client subnet. You can specify up to eight routers in the list. Routers are listed in order of preference (address1 is the most preferred router, address2 is the next most preferred router, and so on).

Examples

The following example specifies 10.12.1.99 as the IP address of the default router:

```
default-router 10.12.1.99
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.

dns-server

To specify the Domain Name System (DNS) IP servers available to a Dynamic Host Configuration Protocol (DHCP) client, use the **dns-server** DHCP pool configuration command. To remove the DNS server list, use the **no** form of this command.

dns-server *address* [*address2...address8*]

no dns-server

Syntax Description

address	Specifies the IP address of a DNS server. One IP address is required, although you can specify up to eight addresses in one command line.
address2...address8	(Optional) Specifies up to eight addresses in the command line.

Defaults

If DNS IP servers are not configured for a DHCP client, the client cannot correlate host names to IP addresses.

Command Modes

DHCP pool configuration

Command History

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

Usage Guidelines

Servers are listed in order of preference (address1 is the most preferred server, address2 is the next most preferred server, and so on).

Examples

The following example specifies 10.12.1.99 as the IP address of the domain name server of the client:

```
dns-server 10.12.1.99
```

Related Commands

Command	Description
domain-name	Specifies the domain name for a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.

domain-name

To specify the domain name for a Dynamic Host Configuration Protocol (DHCP) client, use the **domain-name** DHCP pool configuration command. To remove the domain name, use the **no** form of this command.

domain-name *domain*

no domain-name

Syntax Description

domain	Specifies the domain name string of the client.

Command Modes

DHCP pool configuration

Command History

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

Examples

The following example specifies cisco.com as the domain name of the client:

```
domain-name cisco.com
```

Related Commands

Command	Description
dns-server	Specifies the DNS IP servers available to a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.

hardware-address

To specify the hardware address of a Dynamic Host Configuration Protocol (DHCP) client, use the **hardware-address** DHCP pool configuration command. It is valid for manual bindings only. To remove the hardware address, use the **no** form of this command.

hardware-address *hardware-address type*

no hardware-address

Syntax Description

hardware-address	Specifies the MAC address of the hardware platform of the client.
type	Indicates the protocol of the hardware platform. Strings and values are acceptable. The string options are: • ethernet • ieee802 The value options are: • 1 10Mb Ethernet • 6 IEEE 802 If no type is specified, the default protocol is Ethernet.

Defaults

Ethernet is the default type if none is specified.

Command Modes

DHCP pool configuration

Command History

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

Examples

The following example specifies b708.1388.f166 as the MAC address of the client:

```
hardware-address b708.1388.f166
```

Related Commands

Command	Description
client-identifier	Specifies the unique identifier of a Microsoft DHCP client in dotted hexadecimal notation.
host	Specifies the IP address and network mask for a manual binding to a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.

host

To specify the IP address and network mask for a manual binding to a Dynamic Host Configuration Protocol (DHCP) client, use the **host** DHCP pool configuration command. To remove the IP address of the client, use the **no** form of this command.

host *address* [*mask* | *prefix-length*]

no host

Syntax Description

address	Specifies the IP address of the client.
mask	(Optional) Specifies the network mask of the client.
prefix-length	(Optional) Specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).

Command Modes

DHCP pool configuration

Command History

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

Usage Guidelines

If the mask and prefix length are unspecified, DHCP examines its address pools. If no mask is found in the pool database, the Class A, B, or C natural mask is used. This command is valid for manual bindings only.

There is no limit on the number of manual bindings but you can only configure one manual binding per host pool.

Examples

The following example specifies 10.12.1.99 as the IP address of the client and 255.255.248.0 as the subnet mask:

```
host 10.12.1.99 255.255.248.0
```

Related Commands

Command	Description
client-identifier	Specifies the unique identifier of a Microsoft DHCP client in dotted hexadecimal notation.
hardware-address	Specifies the hardware address of a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP Server.

import all

To import Dynamic Host Configuration Protocol (DHCP) option parameters into the DHCP Server database, use the **import all** DHCP pool configuration command. To disable this feature, use the **no** form of this command.

import all

no import all

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

When the **no import all** command is used, the Cisco IOS DHCP Server deletes all "imported" option parameters that were added to the specified pool in the server database. Manually configured DHCP option parameters override imported DHCP option parameters.

Imported option parameters are not part of the router configuration and are not saved in NVRAM.

Examples

The following example allows the importing of all DHCP options for a pool named pool1:

```
ip dhcp pool pool1
 network 172.16.0.0 /16
 import all
```

Related Commands

Command	Description
ip dhcp database	Configures a Cisco IOS DHCP Server to save automatic bindings on a remote host called a database agent.
show ip dhcp import	Displays the option parameters that were imported into the DHCP Server database.

ip address dhcp

To acquire an IP address on an Ethernet interface from the Dynamic Host Configuration Protocol (DHCP), use the **ip address dhcp** interface configuration command. To deconfigure any address that was acquired, use the **no** form of this command.

ip address dhcp [**client-id** *interface-name*] [**hostname** *host-name*]

no ip address dhcp [**client-id** *interface-name*] [**hostname** *host-name*]

Syntax Description

client-id	(Optional) Specifies the client identifier. By default, the client identifier is an ASCII value. The **client-id** *interface-name* option sets the client identifier to the hexadecimal MAC address of the named interface.
interface-name	(Optional) The interface name from which the MAC address is taken.
hostname	(Optional) Specifies the host name.
host-name	(Optional) Name of the host to be placed in the DHCP option 12 field. This name need not be the same as the host name entered in global configuration mode.

Defaults

The host name is the globally configured host name of the router.

The client identifier is an ASCII value.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.1(3)T	The following keyword and argument were added: • **client-id** • *interface-name*
12.2(3)	The following keyword and argument were added: • **hostname** • *host-name* The behavior of the **client-id** *interface-name* option changed. See the "Usage Guidelines" section for details.

Usage Guidelines

The **ip address dhcp** command allows any interface to dynamically learn its IP address by using the DHCP protocol. It is especially useful on Ethernet interfaces that dynamically connect to an Internet Service Provider (ISP). Once assigned a dynamic address, the interface can be used with the Port Address Translation (PAT) of Cisco IOS Network Address Translation (NAT) to provide Internet access to a privately addressed network attached to the router.

Some ISPs require that the DHCPDISCOVER message have a specific host name and client identifier that is the MAC address of the interface. The most typical usage of the **ip address dhcp client-id** *interface-name* **hostname** *host-name* command is when *interface-name* is the Ethernet interface where the command is configured and *host-name* is the host name provided by the ISP.

A client identifier (DHCP option 61) can be a hexadecimal or an ASCII value. By default, the client identifier is an ASCII value. The **client-id** *interface* option overrides the default and forces the use of the hexadecimal MAC address of the named interface.

Note Between 12.1(3)T and 12.2(3), the **client-id** optional keyword allowed the change of the fixed ASCII value for the client identifier. After 12.2(3), the optional **client-id** keyword forced the use of the hexadecimal MAC address of the named interface as the client identifier.

If a Cisco router is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.

If you use the **ip address dhcp** command with or without any of the optional keywords, the DHCP option 12 field (host name option) is included in the DISCOVER message. By default, the host name specified in option 12 will be the globally configured host name of the router. However, you can use the **ip address dhcp hostname** *host-name* command to place a different name in the DHCP option 12 field than the globally configured host name of the router.

The **no ip address dhcp** command deconfigures any IP address that was acquired, thus sending a DHCPRELEASE message.

You might need to experiment with different configurations to determine the one required by your DHCP server. Table 12 shows the possible configuration methods and the information placed in the DISCOVER message for each method.

Table 12 Configuration Method and Resulting Contents of the DISCOVER Message

Configuration Method	Contents of DISCOVER Messages
ip address dhcp	The DISCOVER message contains "cisco-*mac-address* -Eth1" in the client ID field. The *mac-address* is the media access control (MAC) address of the Ethernet 1 interface and contains the default host name of the router in the option 12 field.
ip address dhcp hostname *host-name*	The DISCOVER message contains "cisco-*mac-address* -Eth1" in the client ID field. The *mac-address* is the MAC address of the Ethernet 1 interface, and contains *host-name* in the option 12 field.
ip address dhcp client-id ethernet 1	The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains the default host name of the router in the option 12 field.
ip address dhcp client-id ethernet 1 hostname *host-name*	The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains *host-name* in the option 12 field.

Examples

In the examples that follow, the command **ip address dhcp** is entered for the Ethernet 1 interface. The DISCOVER message sent by a router configured as shown in the following example would contain "cisco- *mac-address* -Eth1" in the client-ID field, and the value fresno in the option 12 field.

```
hostname fresno
!
interface Ethernet 1
 ip address dhcp
```

The DISCOVER message sent by a router configured as shown in the following example would contain "cisco- *mac-address* -Eth1" in the client-ID field, and the value sanfran in the option 12 field.

```
hostname fresno
!
interface Ethernet 1
 ip address dhcp hostname sanfran
```

The DISCOVER message sent by a router configured as shown in the following example would contain the MAC address of the Ethernet 1 interface in the client-id field, and the value fresno in the option 12 field.

```
hostname fresno
!
interface Ethernet 1
 ip address dhcp client-id Ethernet 1
```

The DISCOVER message sent by a router configured as shown in the following example would contain the MAC address of the Ethernet 1 interface in the client-id field, and the value sanfran in the option 12 field.

```
hostname fresno
!
interface Ethernet 1
 ip address dhcp client-id Ethernet 1 hostname sanfran
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.

ip dhcp-client broadcast-flag

To configure the Cisco IOS Dynamic Host Configuration (DHCP) client to set the broadcast flag, use the **ip dhcp-client broadcast-flag** command in global configuration mode. To disable this feature, use the **no** form of this command.

ip dhcp-client broadcast-flag

no dhcp-client broadcast-flag

Syntax Description

This command has no arguments or keywords.

Defaults

The broadcast flag is on.

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Use this command to set the broadcast flag to 1 or 0 in the DHCP header when the DHCP client sends a discover requesting an IP address. The DHCP Server listens to this broadcast flag and broadcasts the reply packet if the flag is set to 1.

If you enter **no ip dhcp-client broadcast-flag**, the broadcast flag is set to 0 and the DHCP Server unicasts the reply packets to the client with the offered IP address.

The Cisco IOS DHCP client can receive both broadcast and unicast offers from the DHCP Server.

Examples

The following example sets the broadcast flag on:

```
Router(config)# ip dhcp-client broadcast-flag
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an interface via DHCP.
service dhcp	Enables DHCP server and relay functions.

ip dhcp-client default-router distance

To configure a default DHCP administrative distance for clients, use the **ip dhcp-client default-router distance** command in global configuration mode. To return to the default of 254, use the **no** form of this command.

ip dhcp-client default-router distance *value*

no ip dhcp-client default-router distance *value*

Syntax Description

distance	DHCP administrative distance. The *value* argument sets the default distance. The range is from 1 to 255.

Defaults

254

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.

Examples

The following example shows how to configure the default admininstrative distance to be 25:

```
ip dhcp-client default-router distance 25
```

Related Commands

Command	Description
debug dhcp client	Displays debugging information about the DHCP client activities and monitors the status of DHCP packets.
show ip route dhcp	Displays the routes added to the routing table by the DHCP server and relay agent.

ip dhcp conflict logging

To enable conflict logging on a Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server, use the **ip dhcp conflict logging** global configuration command. To disable conflict logging, use the **no** form of this command.

ip dhcp conflict logging

no ip dhcp conflict logging

Syntax Description

This command has no arguments or keywords.

Defaults

Conflict logging is enabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

We recommend using a DHCP server database agent to store automatic bindings. If you decide not to use a DHCP Server database agent to store automatic bindings, use the **no ip dhcp conflict logging** command to disable the recording of address conflicts. By default, the Cisco IOS DHCP Server records DHCP address conflicts in a log file.

Examples

The following example disables the recording of DHCP address conflicts:

```
no ip dhcp conflict logging
```

Related Commands

Command	Description
clear ip dhcp conflict	Clears an address conflict from the Cisco IOS DHCP Server database.
ip dhcp database	Configures a Cisco IOS DHCP Server to save automatic bindings on a remote host called a database agent.
show ip dhcp conflict	Displays address conflicts found by a Cisco IOS DHCP Server when addresses are offered to the client.

ip dhcp database

To configure a Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server and relay agent to save automatic bindings on a remote host called a database agent, use the **ip dhcp database** global configuration command. To remove the database agent, use the **no** form of this command.

ip dhcp database *url* [**timeout** *seconds* | **write-delay** *seconds*]

no ip dhcp database *url*

Syntax Description

url	Specifies the remote file used to store the automatic bindings. Following are the acceptable URL file formats: • tftp://host/filename • ftp://user:password@host/filename • rcp://user@host/filename
timeout *seconds*	(Optional) Specifies how long (in seconds) the DHCP Server should wait before aborting a database transfer. Transfers that exceed the timeout period are aborted. By default, DHCP waits 300 seconds (5 minutes) before aborting a database transfer. Infinity is defined as 0 seconds.
write-delay *seconds*	(Optional) Specifies how soon the DHCP server should send database updates. By default, DHCP waits 300 seconds (5 minutes) before sending database changes. The minimum delay is 60 seconds.

Defaults

DHCP waits 300 seconds for both a write delay and a timeout.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The administrator may configure multiple database agents. Bindings are transferred by using FTP, Trivial File Transport Protocol (TFTP), or remote copy protocol (rcp).

The DHCP relay agent can save route information to the same database agents to ensure recovery after reloads.

Examples

The following example specifies the DHCP database transfer timeout value at 80 seconds:

```
ip dhcp database ftp://user:password@172.16.1.1/router-dhcp timeout 80
```

The following example specifies the DHCP database update delay value at 100 seconds:

```
ip dhcp database tftp://172.16.1.1/router-dhcp write-delay 100
```

Related Commands

Command	Description
show ip dhcp database	Displays Cisco IOS DHCP Server database agent information.

ip dhcp excluded-address

To specify IP addresses that a Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server should not assign to DHCP clients, use the **ip dhcp excluded-address** global configuration command. To remove the excluded IP addresses, use the **no** form of this command.

ip dhcp excluded-address *low-address* [*high-address*]

no ip dhcp excluded-address *low-address* [*high-address*]

Syntax Description

low-address	The excluded IP address, or first IP address in an excluded address range.
high-address	(Optional) The last IP address in the excluded address range.

Defaults

All IP pool addresses are assignable.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The DHCP Server assumes that all pool addresses may be assigned to clients. Use this command to exclude a single IP address or a range of IP addresses.

Examples

The following example configures an excluded IP address range from 172.16.1.100 through 172.16.1.199:

```
ip dhcp excluded-address 172.16.1.100 172.16.1.199
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP Server.

ip dhcp limited-broadcast-address

To override a configured network broadcast and have the DHCP server and relay agent send an all networks, all nodes broadcast to a DHCP client, use the **ip dhcp limited-broadcast-address** global configuration command. To disable this functionality, use the **no** form of this command.

ip dhcp limited-broadcast-address

no ip dhcp limited-broadcast-address

Syntax Description

This command has no arguments or keywords.

Defaults

Default broadcast address: 255.255.255.255 (all ones)

Command Modes

Global configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

When a DHCP client sets the broadcast bit in the DHCP packet, the DHCP server and relay agent send DHCP messages to clients using the all ones broadcast address (255.255.255.255). If the **ip broadcast-address** interface configuration command has been configured to send a network broadcast, the all ones broadcast set by DHCP is overridden. To remedy this situation, use the **ip dhcp limited-broadcast-address** command to ensure that a configured network broadcast does not override the default DHCP behavior.

Some DHCP clients can only accept an all ones broadcast and may not be able to acquire a DHCP address unless this command is configured on the router interface connected to the client.

Examples

The following example configures DHCP to override any network broadcast:

```
ip dhcp limited-broadcast-address
```

Related Commands

Command	Description
ip broadcast-address	Defines a broadcast address for an interface.

ip dhcp ping packets

To specify the number of packets a Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server sends to a pool address as part of a ping operation, use the **ip dhcp ping packets** global configuration command. To prevent the server from pinging pool addresses, use the **no** form of this command.

ip dhcp ping packets *number*

no ip dhcp ping packets

Syntax Description

number	Indicates the number of ping packets that are sent before assigning the address to a requesting client. The default value is two packets.

Defaults

Two packets

Command Modes

Global configuration

Command History

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

Usage Guidelines

The DHCP Server pings a pool address before assigning the address to a requesting client. If the ping is unanswered, the DHCP Server assumes (with a high probability) that the address is not in use and assigns the address to the requesting client.

Setting the *number* argument to a value of 0 turns off DHCP Server ping operation completely.

Examples

The following example specifies five ping attempts by the DHCP Server before ceasing any further ping attempts:

```
ip dhcp ping packets 5
```

Related Commands

Command	Description
clear ip dhcp conflict	Clears an address conflict from the Cisco IOS DHCP Server database.
ip dhcp ping timeout	Specifies how long a Cisco IOS DHCP Server waits for a ping reply from an address pool.
show ip dhcp conflict	Displays address conflicts found by a Cisco IOS DHCP Server when addresses are offered to the client.

ip dhcp ping timeout

To specify how long a Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server waits for a ping reply from an address pool, use the **ip dhcp ping timeout** global configuration command. To restore the default number of milliseconds (500) of the timeout, use the **no** form of this command.

ip dhcp ping timeout *milliseconds*

no ip dhcp ping timeout

Syntax Description

milliseconds	The amount of time (in milliseconds) that the DHCP server waits for a ping reply before it stops attempting to reach a pool address for client assignment. The maximum timeout is 10000 milliseconds (10 seconds). The default timeout is 500 milliseconds.

Defaults

500 milliseconds

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command specifies how long to wait for a ping reply (in milliseconds).

Examples

The following example specifies that the DHCP Server will wait 800 milliseconds for a ping reply before considering the ping a failure:

```
ip dhcp ping timeout 800
```

Related Commands

Command	Description
clear ip dhcp conflict	Clears an address conflict from the Cisco IOS DHCP Server database.
ip dhcp ping packets	Specifies the number of packets a Cisco IOS DHCP Server sends to a pool address as part of a ping operation.
show ip dhcp conflict	Displays address conflicts found by a Cisco IOS DHCP Server when addresses are offered to the client.

ip dhcp pool

To configure a Dynamic Host Configuration Protocol (DHCP) address pool on a Cisco IOS DHCP Server and enter DHCP pool configuration mode, use the **ip dhcp pool** global configuration command. To remove the address pool, use the **no** form of this command.

ip dhcp pool *name*

no ip dhcp pool *name*

Syntax Description

name	Can either be a symbolic string (such as engineering) or an integer (such as 0).

Defaults

DHCP address pools are not configured.

Command Modes

Global configuration

Command History

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

Usage Guidelines

During execution of this command, the configuration mode changes to DHCP pool configuration mode, which is identified by the (config-dhcp)# prompt. In this mode, the administrator can configure pool parameters, like the IP subnet number and default router list.

Examples

The following example configures pool1 as the DHCP address pool:

```
ip dhcp pool pool1
```

Related Commands

Command	Description
host	Specifies the IP address and network mask for a manual binding to a DHCP client.
ip dhcp excluded-address	Specifies IP addresses that a Cisco IOS DHCP Server should not assign to DHCP clients.
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP Server.

ip dhcp relay information check

To configure a Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server to validate the relay agent information option in forwarded BOOTREPLY messages, use the **ip dhcp relay information check** global configuration command. To disable an information check, use the **no** form of this command.

ip dhcp relay information check

no ip dhcp relay information check

Syntax Description

This command has no arguments or keywords.

Defaults

The DHCP server checks relay information. Invalid messages are dropped.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command is used by cable access router termination systems. By default, DHCP checks relay information. Invalid messages are dropped.

Examples

The following example configures the DHCP Server to check that the relay agent information option in forwarded BOOTREPLY messages is valid:

```
ip dhcp relay information check
```

Related Commands

Command	Description
ip dhcp relay information option	Configures a Cisco IOS DHCP Server to insert the DHCP relay agent information option in forwarded BOOTREQUEST messages.
ip dhcp relay information policy	Configures the information reforwarding policy of a DHCP relay agent (what a DHCP relay agent should do if a message already contains relay information).

ip dhcp relay information option

To enable the system to insert the Dynamic Host Configuration Protocol (DHCP) relay information option in forwarded BOOTREQUEST messages to a Cisco IOS DHCP Server, use the **ip dhcp relay information option** global configuration command. To disable inserting relay information into forwarded BOOTREQUEST messages, use the **no** form of this command.

ip dhcp relay information option

no ip dhcp relay information option

Syntax Description

This command has no arguments or keywords.

Defaults

The DHCP Server does not insert relay information.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command is used by cable access router termination systems. This functionality enables a DHCP server to identify the user (cable access router) sending the request and initiate appropriate action based on this information. By default, DHCP does not insert relay information.

Examples

The following example configures a DHCP Server to insert the DHCP relay agent information option in forwarded BOOTREQUEST messages:

```
ip dhcp relay information option
```

Related Commands

Command	Description
ip dhcp relay information check	Configures a Cisco IOS DHCP Server to validate the relay agent information option in forwarded BOOTREPLY messages.
ip dhcp relay information policy	Configures the information reforwarding policy of a DHCP relay agent (what a DHCP relay agent should do if a message already contains relay information).

ip dhcp relay information policy

To configure the information reforwarding policy for a Dynamic Host Configuration Protocol (DHCP) relay agent (what a relay agent should do if a message already contains relay information), use the **ip dhcp relay information policy** global configuration command. To restore the default relay information policy, use the **no** form of this command.

ip dhcp relay information policy {**drop** | **keep** | **replace**}

no ip dhcp relay information policy

Syntax Description

drop	Directs the DHCP relay agent to discard messages with existing relay information if the relay information option is already present.
keep	Indicates that existing information is left unchanged on the DHCP relay agent.
replace	Indicates that existing information is overwritten on the DHCP relay agent.

Defaults

The DHCP server replaces existing relay information.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command is used by cable access router termination systems. When a DHCP relay agent receives a message from a another DHCP relay agent, relay information might already be present in the message. By default, the relay information from the previous relay agent is replaced.

Examples

The following examples configure a DHCP relay agent to drop messages with existing relay information, keep existing information, and replace existing information:

```
ip dhcp relay information policy drop

ip dhcp relay information policy keep

ip dhcp relay information policy replace
```

Related Commands

Command	Description
ip dhcp relay information check	Configures a Cisco IOS DHCP Server to validate the relay agent information option in forwarded BOOTREPLY messages.
ip dhcp relay information option	Configures a Cisco IOS DHCP Server to insert the DHCP relay agent information option in forwarded BOOTREQUEST messages.

ip dhcp relay information trusted

To configure an interface as a trusted source of the Dynamic Host Configuration Protocol (DHCP) relay agent information option, use the **ip dhcp relay information trusted** command in interface configuration mode. To restore the interface to the default behavior, use the **no** form of the command.

ip dhcp relay information trusted

no ip dhcp relay information trusted

Syntax Description

This command has no arguments or keywords.

Defaults

All interfaces on the router are considered untrusted.

Command Modes

Interface configuration

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

By default, if the gateway address is set to all zeros in the DHCP packet and the relay information option is already present in the packet, the Cisco IOS DHCP relay agent will discard the packet. If the **ip dhcp relay information trusted** command is configured on an interface, the Cisco IOS DHCP relay agent will not discard the packet even if the gateway address is set to all zeros. Instead, the received DHCPDISCOVER or DHCPREQUEST messages will be forwarded to the addresses configured by the **ip helper-address** command as in normal DHCP relay operation.

Examples

In the following example, interface Ethernet 1 is configured as a trusted source for the relay agent information:

```
interface ethernet 1
 ip dhcp relay information trusted
```

Related Commands

Command	Description
ip helper-address	Enables the forwarding of UDP broadcasts, including BOOTP, received on an interface.
show ip dhcp relay information trusted-sources	Displays all interfaces on the router that are configured as a trusted source for the DHCP relay agent information option.

ip dhcp relay information trust-all

To configure all interfaces on a router as trusted sources of the Dynamic Host Configuration Protocol (DHCP) relay agent information option, use the **ip dhcp relay information trust-all** command in global configuration mode. To restore the interfaces to their default behavior, use the **no** form of the command.

ip dhcp relay information trust-all

no ip dhcp relay information trust-all

Syntax Description

This command has no arguments or keywords.

Defaults

All interfaces on the router are considered untrusted.

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

By default, if the gateway address is set to all zeros in the DHCP packet and the relay information option is already present in the packet, the Cisco IOS DHCP relay agent will discard the packet. If the **ip dhcp relay information trust-all** command is configured globally, the Cisco IOS DHCP relay agent will not discard the packet even if the gateway address is set to all zeros. Instead, the received DHCPDISCOVER or DHCPREQUEST messages will be forwarded to the addresses configured by the **ip helper-address** command as in normal DHCP relay operation.

Examples

In the following example, all interfaces on the router are configured as a trusted source for relay agent information:

```
ip dhcp relay information trust-all
```

Related Commands

Command	Description
ip helper-address	Enables the forwarding of UDP broadcasts, including BOOTP, received on an interface.
show ip dhcp relay information trusted-sources	Displays all interfaces on the router that are configured as a trusted source for the DHCP relay agent information option.

ip dhcp smart-relay

To allow the Cisco IOS Dynamic Host Configuration Protocol (DHCP) relay agent to switch the gateway address (giaddr field of a DHCP packet) to secondary addresses when there is no DHCPOFFER message from a DHCP server, use the **ip dhcp smart-relay** global configuration command. To disable this smart-relay functionality and restore the default behavior, use the **no** form of this command.

ip dhcp smart-relay

no ip dhcp smart-relay

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

The DHCP relay agent attempts to forward the primary address as the gateway address three times. After three attempts and no response, the relay agent automatically switches to secondary addresses.

Examples

The following example enables the DHCP relay agent to automatically switch to secondary address pools:

```
ip dhcp smart-relay
```

lease

To configure the duration of the lease for an IP address that is assigned from a Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server to a DHCP client, use the **lease** DHCP pool configuration command. To restore the default value, use the **no** form of this command.

lease {*days* [*hours*][*minutes*] | **infinite**}

no lease

Syntax Description

days	Specifies the duration of the lease in numbers of days.
hours	(Optional) Specifies the number of hours in the lease. A *days* value must be supplied before you can configure an *hours* value.
minutes	(Optional) Specifies the number of minutes in the lease. A *days* value and an *hours* value must be supplied before you can configure a *minutes* value.
infinite	Specifies that the duration of the lease is unlimited.

Defaults

One day

Command Modes

DHCP pool configuration

Command History

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

Examples

The following example shows a one-day lease:

```
lease 1
```

The following example shows a one-hour lease:

```
lease 0 1
```

The following example shows a one-minute lease:

```
lease 0 0 1
```

The following example shows an infinite (unlimited) lease:

```
lease infinite
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.

netbios-name-server

To configure NetBIOS Windows Internet Naming Service (WINS) name servers that are available to Microsoft Dynamic Host Configuration Protocol (DHCP) clients, use the **netbios-name-server** DHCP pool configuration command. To remove the NetBIOS name server list, use the **no** form of this command.

netbios-name-server *address* [*address2...address8*]

no netbios-name-server

Syntax Description

address	Specifies the IP address of the NetBIOS WINS name server. One IP address is required, although you can specify up to eight addresses in one command line.
address2...address8	(Optional) Specifies up to eight addresses in the command line.

Command Modes

DHCP pool configuration

Command History

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

Usage Guidelines

One IP address is required, although you can specify up to eight addresses in one command line. Servers are listed in order of preference (address1 is the most preferred server, address2 is the next most preferred server, and so on).

Examples

The following example specifies the IP address of a NetBIOS name server available to the client:

```
netbios-name-server 10.12.1.90
```

Related Commands

Command	Description
dns-server	Specifies the DNS IP servers available to a DHCP client.
domain-name	Specifies the domain name for a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.
netbios-node-type	Configures the NetBIOS node type for Microsoft DHCP clients.

netbios-node-type

To configure the NetBIOS node type for Microsoft Dynamic Host Configuration Protocol (DHCP) clients, use the **netbios-node-type** DHCP pool configuration command. To remove the NetBIOS node type, use the **no** form of this command.

netbios-node-type *type*

no netbios-node-type

Syntax Description

type	Specifies the NetBIOS node type. Valid types are: • **b-node—**Broadcast • **p-node—**Peer-to-peer • **m-node—**Mixed • **h-node—**Hybrid (recommended)

Command Modes

DHCP pool configuration

Command History

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

Usage Guidelines

The recommended type is h-node (hybrid).

Examples

The following example specifies the client's NetBIOS type as hybrid:

```
netbios node-type h-node
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.
netbios-name-server	Configures NetBIOS WINS name servers that are available to Microsoft DHCP clients.

network (DHCP)

To configure the subnet number and mask for a Dynamic Host Configuration Protocol (DHCP) address pool on a Cisco IOS DHCP Server, use the **network** DHCP pool configuration command. To remove the subnet number and mask, use the **no** form of this command.

network *network-number* [*mask* | *prefix-length*]

no network

Syntax Description

network-number	The IP address of the DHCP address pool.
mask	(Optional) The bit combination that renders which portion of the address of the DHCP address pool refers to the network or subnet and which part refers to the host.
prefix-length	(Optional) Specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).

Command Modes

DHCP pool configuration

Command History

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

Usage Guidelines

This command is valid for DHCP subnetwork address pools only. If the mask or prefix length is not specified, the class A, B, or C natural mask is used. The DHCP Server assumes that all host addresses are available. The system administrator can exclude subsets of the address space by using the **ip dhcp excluded-address** command.

You can not configure manual bindings within the same pool that is configured with the **network** command.

Examples

The following example configures 172.16.0.0/16 as the subnetwork number and mask of the DHCP pool:

```
network 172.16.0.0/16
```

Related Commands

Command	Description
host	Specifies the IP address and network mask for a manual binding to a DHCP client.
ip dhcp excluded-address	Specifies IP addresses that a Cisco IOS DHCP Server should not assign to DHCP clients.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.

next-server

To configure the next server in the boot process of a Dynamic Host Configuration Protocol (DHCP) client, use the **next-server** DHCP pool configuration command. To remove the boot server list, use the **no** form of this command.

next-server *address* [*address2...address8*]

no next-server *address*

Syntax Description

address	Specifies the IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server. One IP address is required, although you can specify up to eight addresses in one command line.
address2...address8	(Optional) Specifies up to eight addresses in the command line.

Defaults

If the **next-server** command is not used to configure a boot server list, the DHCP Server uses inbound interface helper addresses as boot servers.

Command Modes

DHCP pool configuration

Command History

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

Usage Guidelines

You can specify up to eight servers in the list. Servers are listed in order of preference (address1 is the most preferred server, address2 is the next most preferred server, and so on).

Examples

The following example specifies 10.12.1.99 as the IP address of the next server in the boot process:

```
next-server 10.12.1.99
```

Related Commands

Command	Description
bootfile	Specifies the name of the default boot image for a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.
ip helper-address	Forwards UDP broadcasts, including BOOTP, received on an interface.
option	Configures Cisco IOS DHCP Server options.

option

To configure Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server options, use the **option** DHCP pool configuration command. To remove the options, use the **no** form of this command.

option *code* [**instance** *number*] {**ascii** *string* | **hex** *string* | **ip** *address*}

no option *code* [**instance** *number*]

Syntax Description

code	Specifies the DHCP option code.
instance *number*	(Optional) Specifies a number from 0 to 255.
ascii *string*	Specifies an NVT ASCII character string. ASCII character strings that contain white space must be delimited by quotation marks.
hex *string*	Specifies dotted hexadecimal data. Each byte in hexadecimal character strings is two hexadecimal digits—each byte can be separated by a period, colon, or white space.
ip *address*	Specifies an IP address.

Defaults

The default instance number is 0.

Command Modes

DHCP pool configuration

Command History

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

Usage Guidelines

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. Configuration parameters and other control information are carried in tagged data items that are stored in the options field of the DHCP message. The data items themselves are also called options. The current set of DHCP options are documented in RFC 2131, *Dynamic Host Configuration Protocol*.

Examples

The following example configures DHCP option 19, which specifies whether the client should configure its IP layer for packet forwarding. A value of 0 means disable IP forwarding; a value of 1 means enable IP forwarding. IP forwarding is enabled in the following example:

```
option 19 hex 01
```

The following example configures DHCP option 72, which specifies the World Wide Web servers for DHCP clients. World Wide Web servers 172.16.3.252 and 172.16.3.253 are configured in the following example:

```
option 72 ip 172.16.3.252 172.16.3.253
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.

service dhcp

To enable the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server and relay agent features on your router, use the **service dhcp** global configuration command. To disable the Cisco IOS DHCP server and relay agent features, use the **no** form of this command.

service dhcp

no service dhcp

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

The BOOTP and DHCP servers in Cisco IOS software both use the ICMP port (port 67) by default. ICMP "port unreachable messages" will only be returned to the sender if both the BOOTP server and DHCP server are disabled. Disabling only one of the servers will not result in ICMP port unreachable messages.

Examples

The following example enables DHCP services on the DHCP Server:

```
service dhcp
```

show ip dhcp binding

To display address bindings on the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server, use the **show ip dhcp binding** EXEC command.

show ip dhcp binding [*ip-address*]

Syntax Description

ip-address	(Optional) Specifies the IP address of the DHCP client for which bindings will be displayed.

Command Modes

EXEC

Command History

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

Usage Guidelines

If the address is not specified, all address bindings are shown. Otherwise, only the binding for the specified client is displayed.

Examples

The following examples show the DHCP binding address parameters, including an IP address, an associated MAC address, a lease expiration date, and the type of address assignment that have occurred. Table 13 lists descriptions of the fields in each example.

```
Router> show ip dhcp binding 172.16.1.11

IP address    Hardware address    Lease expiration        Type
172.16.1.11   00a0.9802.32de      Feb 01 1998 12:00 AM    Automatic

Router> show ip dhcp binding 172.16.3.254

IP address    Hardware address    Lease expiration        Type
172.16.3.254  02c7.f800.0422      Infinite                Manual
```

Table 13 show ip dhcp binding Field Descriptions

Field	Description
IP address	The IP address of the host as recorded on the DHCP Server.
Hardware address	The MAC address or client identifier of the host as recorded on the DHCP Server.
Lease expiration	The lease expiration date of the IP address of the host.
Type	The manner in which the IP address was assigned to the host.

Related Commands

Command	Description
clear ip dhcp binding	Deletes an automatic address binding from the Cisco IOS DHCP Server database.

show ip dhcp conflict

To display address conflicts found by a Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server when addresses are offered to the client, use the **show ip dhcp conflict** EXEC command.

show ip dhcp conflict [*ip-address*]

Syntax Description

ip-address	(Optional) Specifies the IP address of the conflict found.

Command Modes

EXEC

Command History

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

Usage Guidelines

The server detects conflicts using ping. The client detects conflicts using gratuitous Address Resolution Protocol (ARP). If an address conflict is detected, the address is removed from the pool and the address will not be assigned until an administrator resolves the conflict.

Examples

The following example displays the detection method and detection time for all IP addresses the DHCP Server has offered that have conflicts with other devices. Table 14 lists descriptions of the fields in the example.

```
Router> show ip dhcp conflict

IP address    Detection Method     Detection time
172.16.1.32   Ping                 Feb 16 1998 12:28 PM
172.16.1.64   Gratuitous ARP       Feb 23 1998 08:12 AM
```

Table 14 show ip dhcp conflict Field Descriptions

Field	Description
IP address	The IP address of the host as recorded on the DHCP server.
Detection Method	The manner in which the IP address of the hosts were found on the DHCP Server. Can be a ping or a gratuitous ARP.
Detection time	The time when the conflict was found.

Related Commands

Command	Description
clear ip dhcp conflict	Clears an address conflict from the Cisco IOS DHCP Server database.
ip dhcp ping packets	Specifies the number of packets a Cisco IOS DHCP Server sends to a pool address as part of a ping operation.
ip dhcp ping timeout	Specifies how long a Cisco IOS DHCP Server waits for a ping reply from an address pool.

show ip dhcp database

To display Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server database agent information, use the **show ip dhcp database** privileged EXEC command.

show ip dhcp database [*url*]

Syntax Description

url	(Optional) Specifies the remote file used to store automatic DHCP bindings. Following are the acceptable URL file formats: • tftp://host/filename • ftp://user:password@host/filename • rcp://user@host/filename

Defaults

If a URL is not specified, all database agent records are shown. Otherwise, only information about the specified agent is displayed.

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows all DHCP Server database agent information. Table 15 lists descriptions for each field in the example.

```
Router# show ip dhcp database

URL       :    ftp://user:password@172.16.4.253/router-dhcp
Read      :    Dec 01 1997 12:01 AM
Written   :    Never
Status    :    Last read succeeded. Bindings have been loaded in RAM.
Delay     :    300 seconds
Timeout   :    300 seconds
Failures  :    0
Successes :    1
```

Table 15 show ip dhcp database Field Descriptions

Field	Description
URL	Specifies the remote file used to store automatic DHCP bindings. Following are the acceptable URL file formats: • tftp://host/filename • ftp://user:password@host/filename • rcp://user@host/filename
Read	The last time bindings were read from the file server.
Written	The last time bindings were written to the file server.
Status	Indication of whether the last read or write of host bindings was successful.
Delay	The amount of time to wait before updating the database.
Timeout	The amount of time before the file transfer is aborted.
Failures	The number of failed file transfers.
Successes	The number of successful file transfers.

Related Commands

Command	Description
ip dhcp database	Configures a Cisco IOS DHCP Server to save automatic bindings on a remote host called a database agent.

show ip dhcp import

To display the option parameters that were imported into the Dynamic Host Configuration Protocol (DHCP) Server database, use the **show ip dhcp import** EXEC command.

show ip dhcp import

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

Imported option parameters are not part of the router configuration and are not saved in NVRAM. Thus, the **show ip dhcp import** command is necessary to display the imported option parameters.

Examples

The following is sample output from the **show ip dhcp import** command:

```
Router# show ip dhcp import

Address Pool Name:2
Domain Name Server(s): 1.1.1.1
NetBIOS Name Server(s): 3.3.3.3
```

The following example indicates the address pool name:

```
Address Pool Name:2
```

The following example indicates the imported values, which are domain name and NetBIOS name information:

```
Domain Name Server(s): 1.1.1.1
NetBIOS Name Server(s): 3.3.3.3
```

Related Commands

Command	Description
import all	Imports option parameters into the DHCP database.
show ip dhcp database	Displays Cisco IOS server database information.

show ip dhcp relay information trusted-sources

To display all interfaces configured to be a trusted source for the Dynamic Host Configuration Protocol (DHCP) relay information option, use the **show ip dhcp relay information trusted-sources** command in EXEC mode.

show ip dhcp relay information trusted-sources

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2	This command was introduced.

Examples

The following is sample output when the **ip dhcp relay information trusted** interface configuration command is configured. Note that the display output lists the interfaces that are configured to be trusted sources.

```
Router# show ip dhcp relay information trusted-sources

List of trusted sources of relay agent information option:
Ethernet1/1       Ethernet1/2       Ethernet1/3       Serial4/1.1
Serial4/1.2       Serial4/1.3
```

The following is sample output when the **ip dhcp relay information trust-all** global configuration command is configured. Note that the display output does not list the individual interfaces.

```
Router# show ip dhcp relay information trusted-sources

All interfaces are trusted source of relay agent information option
```

Related Commands

Command	Description
ip dhcp relay information trusted	Configures an interface as a trusted source of the DHCP relay agent information option.
ip dhcp relay information trust-all	Configures all interfaces on a router as trusted sources of the DHCP relay agent information option.

show ip dhcp server statistics

To display Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server statistics, use the **show ip dhcp server statistics** EXEC command.

show ip dhcp server statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

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

Examples

The following example displays DHCP Server statistics. Table 16 lists descriptions for each field in the example.

```
Router> show ip dhcp server statistics

Memory usage          40392
Address pools         3
Database agents       1
Automatic bindings    190
Manual bindings       1
Expired bindings      3
Malformed messages    0

Message               Received
BOOTREQUEST           12
DHCPDISCOVER          200
DHCPREQUEST           178
DHCPDECLINE           0
DHCPRELEASE           0
DHCPINFORM            0

Message               Sent
BOOTREPLY             12
DHCPOFFER             190
DHCPACK               172
DHCPNAK               6
```

Table 16 show ip dhcp server statistics Field Descriptions

Field	Description
Memory usage	The number of bytes of RAM allocated by the DHCP Server.
Address pools	The number of configured address pools in the DHCP database.
Database agents	The number of database agents configured in the DHCP database.

Table 16 show ip dhcp server statistics Field Descriptions (continued)

Field	Description
Automatic bindings	The number of IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database.
Manual bindings	The number of IP addresses that have been manually mapped to the MAC addresses of hosts that are found in the DHCP database.
Expired bindings	The number of expired leases.
Malformed messages	The number of truncated or corrupted messages that were received by the DHCP Server.
Message	The DHCP message type that was received by the DHCP Server.
Received	The number of DHCP messages that were received by the DHCP Server.
Sent	The number of DHCP messages that were sent by the DHCP Server.

Related Commands

Command	Description
clear ip dhcp server statistics	Resets all Cisco IOS DHCP Server counters.

show ip route dhcp

To display the routes added to the routing table by the Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server and Relay Agent, use the **show ip route dhcp** command in EXEC configuration mode.

show ip route [**vrf** *vrf-name*] **dhcp [***ip-address*]

Syntax Description

vrf	(Optional) VPN routing and forwarding instance.
vrf-name	(Optional) Name of the VRF.
ip-address	(Optional) Address about which routing information should be displayed.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

To display information about global routes, use the **show ip route dhcp** command. To display routes in the VRF routing table, use the **show ip route vrf** *vrf-name* **dhcp** command.

Examples

The following is sample output from the **show ip route dhcp** command when entered without an address. This command gives the list of all routes added by the Cisco IOS DHCP Server and Relay Agent.

```
Router# show ip route dhcp
  55.5.5.56/32 is directly connected, ATM0.2
  55.5.5.217/32 is directly connected, ATM0.2
```

The following is sample output from the **show ip route dhcp** command when an address is specified. This command gives the details of the address with the server address (who assigned it) and the lease expiration time.

```
Router# show ip route dhcp 55.5.5.217
  55.5.5.217  is directly connected, ATM0.2
    DHCP Server: 49.9.9.10   Lease expires at Nov 08 2001 01:19 PM
```

The following is sample output from the **show ip route vrf** *vrf-name* **dhcp** command when entered without an address:

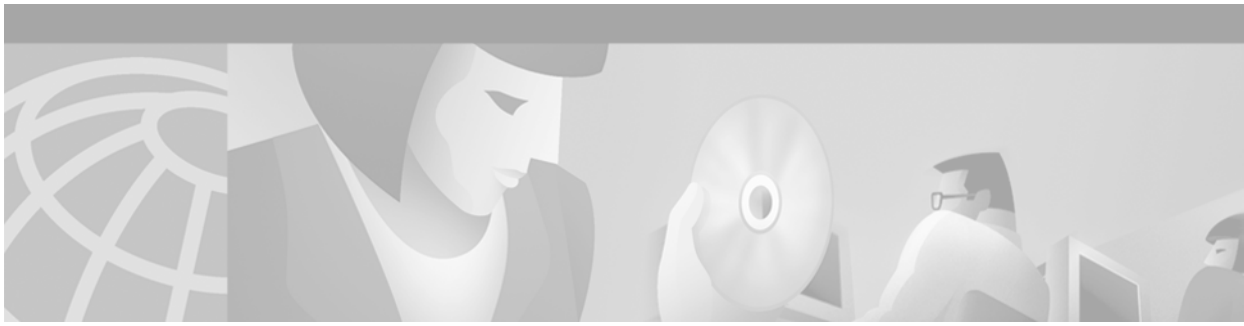
```
Router# show ip route vrf red dhcp
  55.5.5.218/32 is directly connected, ATM0.2
```

The following is sample output from the **show ip route vrf** *vrf-name* **dhcp** command when an address is specified. This command gives the details of the address with the server address (who assigned it) and the lease expiration time.

```
Router# show ip route vrf red dhcp 55.5.5.218
  55.5.5.218/32 is directly connected, ATM0.2
    DHCP Server: 49.9.9.10   Lease expires at Nov 08 2001 03:15PM
```

Related Commands

Command	Description
clear ip route dhcp	Removes routes from the routing table added by the DHCP Server and Relay Agent for the DHCP clients on unnumbered interfaces.



IP Services Commands

Use the commands in this chapter to configure various IP services. For configuration information and examples on IP services, refer to the "Configuring IP Services" chapter of the *Cisco IOS IP Configuration Guide*.

access-class

To restrict incoming and outgoing connections between a particular vty (into a Cisco device) and the addresses in an access list, use the **access-class** command in line configuration mode. To remove access restrictions, use the **no** form of this command.

access-class *access-list-number* {**in** [**vrf-also**] | **out**}

no access-class *access-list-number* {**in** | **out**}

Syntax Description

access-list-number	Number of an IP access list. This is a decimal number from 1 to 199 or from 1300 to 2699.
in	Restricts incoming connections between a particular Cisco device and the addresses in the access list.
vrf-also	Accepts incoming connections from interfaces that belong to a VRF.
out	Restricts outgoing connections between a particular Cisco device and the addresses in the access list.

Defaults

No access lists are defined.

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2	The **vrf-also** keyword was added.

Usage Guidelines

Remember to set *identical restrictions* on all the virtual terminal lines because a user can connect to any of them.

To display the access lists for a particular terminal line, use the **show line** EXEC command and specify the line number.

If you do not specify the **vrf-also** keyword, incoming Telnet connections from interfaces that are part of a VRF are rejected.

Examples

The following example defines an access list that permits only hosts on network 192.89.55.0 to connect to the virtual terminal ports on the router:

```
access-list 12 permit 192.89.55.0  0.0.0.255
 line 1 5
 access-class 12 in
```

The following example defines an access list that denies connections to networks other than network 36.0.0.0 on terminal lines 1 through 5:

```
access-list 10 permit 36.0.0.0 0.255.255.255
 line 1 5
 access-class 10 out
```

Related Commands

Command	Description
show line	Displays the parameters of a terminal line.

access-list (IP extended)

To define an extended IP access list, use the extended version of the **access-list** command in global configuration mode. To remove the access list, use the **no** form of this command.

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]

no access-list *access-list-number*

Internet Control Message Protocol (ICMP)

For ICMP, you can also use the following syntax:

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*] | *icmp-message*] [**precedence** *precedence*] [**tos** *tos*] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]

Internet Group Management Protocol (IGMP)

For IGMP, you can also use the following syntax:

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]

Transmission Control Protocol (TCP)

For TCP, you can also use the following syntax:

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} **tcp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]

User Datagram Protocol (UDP)

For UDP, you can also use the following syntax:

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} **udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]

Syntax Description

access-list-number	Number of an access list. This is a decimal number from 100 to 199 or from 2000 to 2699.
dynamic *dynamic-name*	(Optional) Identifies this access list as a dynamic access list. Refer to lock-and-key access documented in the "Configuring Lock-and-Key Security (Dynamic Access Lists)" chapter in the *Cisco IOS Security Configuration Guide*.

timeout *minutes*	(Optional) Specifies the absolute length of time, in minutes, that a temporary access list entry can remain in a dynamic access list. The default is an infinite length of time and allows an entry to remain permanently. Refer to lock-and-key access documented in the "Configuring Lock-and-Key Security (Dynamic Access Lists)" chapter in the *Cisco IOS Security Configuration Guide*.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
protocol	Name or number of an Internet protocol. It can be one of the keywords **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **pim**, **tcp**, or **udp**, or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP, and UDP) use the **ip** keyword. Some protocols allow further qualifiers described below.
source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits to be applied to source. Each wildcard bit 0 indicates the corresponding bit position in the source. Each wildcard bit set to 1 indicates that both a 0 bit and a 1 bit in the corresponding position of the IP address of the packet will be considered a match to this access list entry. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0. Wildcard bits set to 1 need not be contiguous in the source wildcard. For example, a source wildcard of 0.255.0.64 would be valid.
destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the **any** keyword as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.

destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
precedence *precedence*	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7, or by name as listed in the section "Usage Guidelines."
tos *tos*	(Optional) Packets can be filtered by type of service level, as specified by a number from 0 to 15, or by name as listed in the section "Usage Guidelines."
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. By default, the message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. Use the **ip access-list log-update** command to generate logging messages when the number of matches reaches a configurable threshold (rather than waiting for a 5-minute interval). See the **ip access-list log-update** command for more information. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list. If you enable CEF and then create an access list that uses the **log** keyword, the packets that match the access list are not CEF switched. They are fast switched. Logging disables CEF.
log-input	(Optional) Includes the input interface and source MAC address or VC in the logging output.
time-range *time-range-name*	(Optional) Name of the time range that applies to this statement. The name of the time range and its restrictions are specified by the **time-range** command.
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
icmp-code	(Optional) ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.

icmp-message	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are listed in the section "Usage Guidelines."
igmp-type	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the section "Usage Guidelines."
operator	(Optional) Compares source or destination ports. Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source* and *source-wildcard*, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard*, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number.
port	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the section "Usage Guidelines." TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST control bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
fragments	(Optional) The access list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List Processing of Fragments" and "Fragments and Policy Routing" sections in the "Usage Guidelines" section.

Defaults

An extended access list defaults to a list that denies everything. An extended access list is terminated by an implicit deny statement.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The following keywords and arguments were added: • *source* • *source-wildcard* • *destination* • *destination-wildcard* • **precedence** *precedence* • *icmp-type* • *icm-code* • *icmp-message* • *igmp-type* • *operator* • *port* • **established**
11.1	The **dynamic** *dynamic-name* keyword and argument were added.
11.1	The **timeout** *minutes* keyword and argument were added.
11.2	The **log-input** keyword was added.
12.0(1)T	The **time-range** *time-range-name* keyword and argument were added.
12.0(11) and 12.1(2)	The **fragments** keyword was added.

Usage Guidelines

You can use access lists to control the transmission of packets on an interface, control vty access, and restrict the contents of routing updates. The Cisco IOS software stops checking the extended access list after a match occurs.

Fragmented IP packets, other than the initial fragment, are immediately accepted by any extended IP access list. Extended access lists used to control vty access or restrict the contents of routing updates must not match against the TCP source port, the type of service (ToS) value, or the precedence of the packet.

Note After a numbered access list is created, any subsequent additions (possibly entered from the terminal) are placed at the end of the list. In other words, you cannot selectively add or remove access list command lines from a specific numbered access list.

The following is a list of precedence names:

- **critical**
- **flash**
- **flash-override**
- **immediate**
- **internet**
- **network**

- **priority**
- **routine**

The following is a list of ToS names:

- **max-reliability**
- **max-throughput**
- **min-delay**
- **min-monetary-cost**
- **normal**

The following is a list of ICMP message type names and ICMP message type and code names:

- **administratively-prohibited**
- **alternate-address**
- **conversion-error**
- **dod-host-prohibited**
- **dod-net-prohibited**
- **echo**
- **echo-reply**
- **general-parameter-problem**
- **host-isolated**
- **host-precedence-unreachable**
- **host-redirect**
- **host-tos-redirect**
- **host-tos-unreachable**
- **host-unknown**
- **host-unreachable**
- **information-reply**
- **information-request**
- **mask-reply**
- **mask-request**
- **mobile-redirect**
- **net-redirect**
- **net-tos-redirect**
- **net-tos-unreachable**
- **net-unreachable**
- **network-unknown**
- **no-room-for-option**
- **option-missing**
- **packet-too-big**
- **parameter-problem**

- **port-unreachable**
- **precedence-unreachable**
- **protocol-unreachable**
- **reassembly-timeout**
- **redirect**
- **router-advertisement**
- **router-solicitation**
- **source-quench**
- **source-route-failed**
- **time-exceeded**
- **timestamp-reply**
- **timestamp-request**
- **traceroute**
- **ttl-exceeded**
- **unreachable**

The following is a list of IGMP message names:

- **dvmrp**
- **host-query**
- **host-report**
- **pim**
- **trace**

The following is a list of TCP port names that can be used instead of port numbers. Refer to the current assigned numbers RFC to find a reference to these protocols. Port numbers corresponding to these protocols can also be found if you type a **?** in the place of a port number.

- **bgp**
- **chargen**
- **daytime**
- **discard**
- **domain**
- **echo**
- **finger**
- **ftp**
- **ftp-data**
- **gopher**
- **hostname**
- **irc**
- **klogin**
- **kshell**

- **lpd**
- **nntp**
- **pop2**
- **pop3**
- **smtp**
- **sunrpc**
- **syslog**
- **tacacs-ds**
- **talk**
- **telnet**
- **time**
- **uucp**
- **whois**
- **www**

The following is a list of UDP port names that can be used instead of port numbers. Refer to the current assigned numbers RFC to find a reference to these protocols. Port numbers corresponding to these protocols can also be found if you type a **?** in the place of a port number.

- **biff**
- **bootpc**
- **bootps**
- **discard**
- **dnsix**
- **domain**
- **echo**
- **mobile-ip**
- **nameserver**
- **netbios-dgm**
- **netbios-ns**
- **ntp**
- **rip**
- **snmp**
- **snmptrap**
- **sunrpc**
- **syslog**
- **tacacs-ds**
- **talk**
- **tftp**
- **time**

- **who**
- **xdmcp**

Access List Processing of Fragments

The behavior of access-list entries regarding the use or lack of the **fragments** keyword can be summarized as follows:

If the Access-List Entry has...	Then..
...no **fragments** keyword (the default behavior), and assuming all of the access-list entry information matches,	For an access-list entry containing only Layer 3 information: • The entry is applied to nonfragmented packets, initial fragments and noninitial fragments. For an access list entry containing Layer 3 and Layer 4 information: • The entry is applied to nonfragmented packets and initial fragments. – If the entry is a **permit** statement, the packet or fragment is permitted. – If the entry is a **deny** statement, the packet or fragment is denied. • The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access-list entry can be applied. If the Layer 3 portion of the access-list entry matches, and – If the entry is a **permit** statement, the noninitial fragment is permitted. – If the entry is a **deny** statement, the next access-list entry is processed. **Note** The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.
...the **fragments** keyword, and assuming all of the access-list entry information matches,	The access-list entry is applied only to noninitial fragments. **Note** The **fragments** keyword cannot be configured for an access-list entry that contains any Layer 4 information.

Be aware that you should not simply add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments** keyword, the packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair

will not include the **fragments** keyword, and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases where there are multiple **deny** access list entries for the same host but with different Layer 4 ports, a single **deny** access-list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets and each counts individually as a packet in access list accounting and access list violation counts.

Note The **fragments** keyword cannot solve all cases involving access lists and IP fragments.

Fragments and Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address** command and the access list had entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy routed, even if the first fragment was not policy routed or the reverse.

By using the **fragments** keyword in access list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made and it is more likely policy routing will occur as intended.

Examples

In the following example, serial interface 0 is part of a Class B network with the address 128.88.0.0, and the address of the mail host is 128.88.1.2. The **established** keyword is used only for the TCP protocol to indicate an established connection. A match occurs if the TCP datagram has the ACK or RST bits set, which indicates that the packet belongs to an existing connection.

```
access-list 102 permit tcp 0.0.0.0 255.255.255.255 128.88.0.0 0.0.255.255 established
access-list 102 permit tcp 0.0.0.0 255.255.255.255 128.88.1.2 0.0.0.0 eq 25
interface serial 0
 ip access-group 102 in
```

The following example permits Domain Naming System (DNS) packets and ICMP echo and echo reply packets:

```
access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
access-list 102 permit tcp any host 128.88.1.2 eq smtp
access-list 102 permit tcp any any eq domain
access-list 102 permit udp any any eq domain
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
```

The following examples show how wildcard bits are used to indicate the bits of the prefix or mask that are relevant. Wildcard bits are similar to the bitmasks that are used with normal access lists. Prefix or mask bits corresponding to wildcard bits set to 1 are ignored during comparisons and prefix or mask bits corresponding to wildcard bits set to 0 are used in comparison.

The following example permits 192.108.0.0 255.255.0.0 but denies any more specific routes of 192.108.0.0 (including 192.108.0.0 255.255.255.0):

```
access-list 101 permit ip 192.108.0.0 0.0.0.0   255.255.0.0 0.0.0.0
access-list 101 deny ip 192.108.0.0 0.0.255.255  255.255.0.0 0.0.255.255
```

The following example permits 131.108.0/24 but denies 131.108/16 and all other subnets of 131.108.0.0:

```
access-list 101 permit ip 131.108.0.0 0.0.0.0     255.255.255.0 0.0.0.0
access-list 101 deny ip 131.108.0.0 0.0.255.255 255.255.0.0   0.0.255.255
```

The following example uses a time range to deny HTTP traffic on Monday through Friday from 8:00 a.m. to 6:00 p.m.:

```
time-range no-http
 periodic weekdays 8:00 to 18:00
!
access-list 101 deny tcp any any eq http time-range no-http
!
interface ethernet 0
 ip access-group 101 in
```

Related Commands

Command	Description
access-class	Restricts incoming and outgoing connections between a particular vty (into a Cisco device) and the addresses in an access list.
access-list (IP standard)	Defines a standard IP access list.
access-list remark	Writes a helpful comment (remark) for an entry in a numbered IP access list.
clear access-template	Clears a temporary access list entry from a dynamic access list.
deny (IP)	Sets conditions under which a packet does not pass a named access list.
distribute-list in (IP)	Filters networks received in updates.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
ip access-group	Controls access to an interface.
ip access-list	Defines an IP access list by name.
ip access-list log-update	Sets the threshold number of packets that cause a logging message.
ip accounting	Enables IP accounting on an interface.
logging console	Limits messages logged to the console, based on severity.
permit (IP)	Sets conditions under which a packet passes a named access list.
remark	Writes a helpful comment (remark) for an entry in a named IP access list.
show access-lists	Displays the contents of current IP and rate-limit access lists.
show ip access-list	Displays the contents of all current IP access lists.
time-range	Specifies when an access list or other feature is in effect.

access-list (IP standard)

To define a standard IP access list, use the standard version of the **access-list** command in global configuration mode. To remove a standard access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]

no access-list *access-list-number*

Caution Enhancements to this command are backward compatible; migrating from releases prior to Cisco IOS Release 10.3 will convert your access lists automatically. However, releases prior to Release 10.3 are not upwardly compatible with these enhancements. Therefore, if you save an access list with these images and then use software prior to Release 10.3, the resulting access list will not be interpreted correctly. **This condition could cause you severe security problems.** Save your old configuration file before booting these images.

Syntax Description

access-list-number	Number of an access list. This is a decimal number from 1 to 99 or from 1300 to 1999.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
source	Number of the network or host from which the packet is being sent. There are two alternative ways to specify the source: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.

source-wildcard	(Optional) Wildcard bits to be applied to the source. There are two alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and source-wildcard of 0.0.0.0 255.255.255.255.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list number, whether the packet was permitted or denied, the source address, and the number of packets. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. Use the **ip access-list log-update** command to generate the logging messages to appear when the number of matches reaches a configurable threshold (rather than waiting for a 5-minute interval). See the **ip access-list log-update** command for more information. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list. If you enable CEF and then create an access list that uses the **log** keyword, the packets that match the access list are not CEF switched. They are fast switched. Logging disables CEF.

Defaults

The access list defaults to an implicit deny statement for everything. The access list is always terminated by an implicit deny statement for everything.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
11.3(3)T	The **log** keyword was added.

Usage Guidelines

Plan your access conditions carefully and be aware of the implicit deny statement at the end of the access list.

You can use access lists to control the transmission of packets on an interface, control vty access, and restrict the contents of routing updates.

Use the **show access-lists** EXEC command to display the contents of all access lists.

Use the **show ip access-list** EXEC command to display the contents of one access list.

Examples

The following example of a standard access list allows access for only those hosts on the three specified networks. The wildcard bits apply to the host portions of the network addresses. Any host with a source address that does not match the access list statements will be rejected.

```
access-list 1 permit 192.5.34.0  0.0.0.255
access-list 1 permit 128.88.0.0  0.0.255.255
access-list 1 permit 36.0.0.0  0.255.255.255
! (Note: all other access implicitly denied)
```

The following example of a standard access list allows access for devices with IP addresses in the range from 10.29.2.64 to 10.29.2.127. All packets with a source address not in this range will be rejected.

```
access-list 1 permit 10.29.2.64 0.0.0.63
! (Note: all other access implicitly denied)
```

To specify a large number of individual addresses more easily, you can omit the wildcard if it is all zeros. Thus, the following two configuration commands are identical in effect:

```
access-list 2 permit 36.48.0.3
access-list 2 permit 36.48.0.3  0.0.0.0
```

Related Commands

Command	Description
access-class	Restricts incoming and outgoing connections between a particular vty (into a Cisco device) and the addresses in an access list.
access-list (IP extended)	Defines an extended IP access list.
access-list remark	Writes a helpful comment (remark) for an entry in a numbered IP access list.
deny (IP)	Sets conditions under which a packet does not pass a named access list.
distribute-list in (IP)	Filters networks received in updates.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
ip access-group	Controls access to an interface.
ip access-list log-update	Sets the threshold number of packets that cause a logging message.
logging console	Limits messages logged to the console based on severity.
permit (IP)	Sets conditions under which a packet passes a named access list.
remark (IP)	Writes a helpful comment (remark) for an entry in a named IP acces s list.
show access-lists	Displays the contents of current IP and rate-limit access lists.
show ip access-list	Displays the contents of all current IP access lists.

access-list compiled

To enable the Turbo Access Control Lists (Turbo ACL) feature, use the **access-list compiled** command in global configuration mode. To disable the Turbo ACL feature, use the **no** form of this command.

access-list compiled

no access-list compiled

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.1(1)E	This command was introduced for Cisco 7200 series routers on Release 12.1 E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

By default, the Turbo ACL feature is disabled. When Turbo ACL is disabled, normal ACL processing is enabled, and no ACL acceleration occurs.

When the Turbo ACL feature is enabled using the **access-list compiled** command, the ACLs in the configuration are scanned and, if suitable, compiled for Turbo ACL acceleration. This scanning and compilation may take a few seconds when the system is processing large and complex ACLs, or when the system is processing a configuration that contains a large number of ACLs.

Any configuration change to an ACL that is being accelerated, such as the addition of new ACL entries or the deletion of the ACL, triggers a recompilation of that ACL.

When Turbo ACL tables are being built (or rebuilt) for a particular ACL, the normal sequential ACL search is used until the new tables are ready for installation.

Examples

The following example enables the Turbo ACL feature:

```
access-list compiled
```

access-list remark

To write a helpful comment (remark) for an entry in a numbered IP access list, use the **access-list remark** command in global configuration mode. To remove the remark, use the **no** form of this command.

access-list *access-list-number* **remark** *remark*

no access-list *access-list-number* **remark** *remark*

Syntax Description

access-list-number	Number of an IP access list.
remark	Comment that describes the access list entry, up to 100 characters long.

Defaults

The access list entries have no remarks.

Command Modes

Global configuration

Command History

Release	Modification
12.0(2)T	This command was introduced.

Usage Guidelines

The remark can be up to 100 characters long; anything longer is truncated.

If you want to write a comment about an entry in a named access list, use the **remark** command.

Examples

In the following example, the workstation belonging to Jones is allowed access, and the workstation belonging to Smith is not allowed access:

```
access-list 1 remark Permit only Jones workstation through
access-list 1 permit 171.69.2.88
access-list 1 remark Do not allow Smith workstation through
access-list 1 deny 171.69.3.13
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
ip access-list	Defines an IP access list by name.
remark	Writes a helpful comment (remark) for an entry in a named IP access list.

clear access-list counters

To clear the counters of an access list, use the **clear access-list counters** command in EXEC mode.

clear access-list counters {*access-list-number* | *access-list-name*}

Syntax Description

access-list-number	Access list number of the access list for which to clear the counters.
access-list-name	Name of an IP access list. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Some access lists keep counters that count the number of packets that pass each line of an access list. The **show access-lists** command displays the counters as a number of matches. Use the **clear access-list counters** command to restart the counters for a particular access list to 0.

Examples

The following example clears the counters for access list 101:

```
Router> clear access-list counters 101
```

Related Commands

Command	Description
show access-lists	Displays the contents of current IP and rate-limit access lists.

clear ip accounting

To clear the active or checkpointed database when IP accounting is enabled, use the **clear ip accounting** command in EXEC mode.

clear ip accounting [**checkpoint**]

Syntax Description

checkpoint	(Optional) Clears the checkpointed database.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can also clear the checkpointed database by issuing the **clear ip accounting** command twice in succession.

Examples

The following example clears the active database when IP accounting is enabled:

```
Router> clear ip accounting
```

Related Commands

Command	Description
ip accounting	Enables IP accounting on an interface.
ip accounting-list	Defines filters to control the hosts for which IP accounting information is kept.
ip accounting-threshold	Sets the maximum number of accounting entries to be created.
ip accounting-transits	Controls the number of transit records that are stored in the IP accounting database.
show ip accounting	Displays the active accounting or checkpointed database or displays access list violations.

clear ip drp

To clear all statistics being collected on Director Response Protocol (DRP) requests and replies, use the **clear ip drp** command in EXEC mode.

clear ip drp

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2 F	This command was introduced.

Examples

The following example clears all DRP statistics:

```
Router> clear ip drp
```

Related Commands

Command	Description
ip drp access-group	Controls the sources of DRP queries to the DRP Server Agent.
ip drp authentication key-chain	Configures authentication on the DRP Server Agent for DistributedDirector.

clear tcp statistics

To clear TCP statistics, use the **clear tcp statistics** command in privileged EXEC mode.

clear tcp statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.

Examples

The following example clears all TCP statistics:

```
Router# clear tcp statistics
```

Related Commands

Command	Description
show tcp statistics	Displays TCP statistics.

deny (IP)

To set conditions for a named IP access list, use the **deny** command in access-list configuration mode.To remove a deny condition from an access list, use the **no** form of this command.

deny *source* [*source-wildcard*]

no deny *source* [*source-wildcard*]

deny *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

no deny *protocol source source-wildcard destination destination-wildcard*

Internet Control Message Protocol (ICMP)

For ICMP, you can also use the following syntax:

deny icmp *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*] | *icmp-message*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

Internet Group Management Protocol (IGMP)

For IGMP, you can also use the following syntax:

deny igmp *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

Transmission Control Protocol (TCP)

For TCP, you can also use the following syntax:

deny tcp *source source-wildcard* [*operator port* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

User Datagram Protocol (UDP)

For UDP, you can also use the following syntax:

deny udp *source source-wildcard* [*operator port* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

Syntax Description

source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits to be applied to the source. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part, dotted decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
protocol	Name or number of an Internet protocol. It can be one of the keywords **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the **ip** keyword. Some protocols allow further qualifiers described later.
destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the **any** keyword as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part, dotted decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
precedence *precedence*	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7 or by name as listed in the section "Usage Guidelines."
tos *tos*	(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15, or by name as listed in the section "Usage Guidelines" of the **access-list** (IP extended) command.

log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. Use the **ip access-list log-update** command to generate logging messages when the number of matches reaches a configurable threshold (rather than waiting for a 5-minute interval). See the **ip access-list log-update** command for more information. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list. If you enable CEF and then create an access list that uses the **log** keyword, the packets that match the access list are not CEF switched. They are fast switched. Logging disables CEF.
time-range *time-range-name*	(Optional) Name of the time range that applies to this **deny** statement. The name of the time range and its restrictions are specified by the **time-range** and **absolute** or **periodic** commands, respectively.
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
icmp-code	(Optional) ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
icmp-message	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are listed in the section "Usage Guidelines" of the **access-list** (IP extended) command.
igmp-type	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the section "Usage Guidelines" of the **access-list** (IP extended) command.
operator	(Optional) Compares source or destination ports. Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source* and *source-wildcard*, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard*, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number.

port	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the section "Usage Guidelines" of the **access-list** (IP extended) command. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
fragments	(Optional) The access list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List Processing of Fragments" and "Fragments and Policy Routing" sections in the "Usage Guidelines" section.

Defaults

There is no specific condition under which a packet is denied passing the named access list.

Command Modes

Access-list configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0(1)T	The **time-range** *time-range-name* keyword and argument were added.
12.0(11) and 12.1(2)	The **fragments** keyword was added.

Usage Guidelines

Use this command following the **ip access-list** command to specify conditions under which a packet cannot pass the named access list.

The **time-range** option allows you to identify a time range by name. The **time-range**, **absolute**, and **periodic** commands specify when this **deny** statement is in effect.

Access List Processing of Fragments

The behavior of access-list entries regarding the use or lack of the **fragments** keyword can be summarized as follows:

If the Access-List Entry has...	Then..
...no **fragments** keyword (the default behavior), and assuming all of the access-list entry information matches,	For an access-list entry containing only Layer 3 information: • The entry is applied to nonfragmented packets, initial fragments and noninitial fragments. For an access list entry containing Layer 3 and Layer 4 information: • The entry is applied to nonfragmented packets and initial fragments. – If the entry is a **permit** statement, the packet or fragment is permitted. – If the entry is a **deny** statement, the packet or fragment is denied. • The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access-list entry can be applied. If the Layer 3 portion of the access-list entry matches, and – If the entry is a **permit** statement, the noninitial fragment is permitted. – If the entry is a **deny** statement, the next access-list entry is processed. **Note** The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.
...the **fragments** keyword, and assuming all of the access-list entry information matches,	**Note** The access-list entry is applied only to noninitial fragments.The **fragments** keyword cannot be configured for an access-list entry that contains any Layer 4 information.

Be aware that you should not simply add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments** keyword, the packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword, and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases where

there are multiple **deny** access list entries for the same host but with different Layer 4 ports, a single **deny** access-list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets and each counts individually as a packet in access list accounting and access list violation counts.

Note The **fragments** keyword cannot solve all cases involving access lists and IP fragments.

Fragments and Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address**s command and the access list had entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy routed, even if the first fragment was not policy routed or the reverse.

By using the **fragments** keyword in access list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made and it is more likely policy routing will occur as intended.

Examples

The following example sets a deny condition for a standard access list named Internetfilter:

```
ip access-list standard Internetfilter
 deny 192.5.34.0  0.0.0.255
 permit 128.88.0.0  0.0.255.255
 permit 36.0.0.0  0.255.255.255
! (Note: all other access implicitly denied)
```

The following example denies HTTP traffic on Monday through Friday from 8:00 a.m. to 6:00 p.m.:

```
time-range no-http
 periodic weekdays 8:00 to 18:00
!
ip access-list extended strict
 deny tcp any any eq http time-range no-http
!
interface ethernet 0
 ip access-group strict in
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
ip access-group	Controls access to an interface.
ip access-list	Defines an IP access list by name.
ip access-list log-update	Sets the threshold number of packets that cause a logging message.
permit (IP)	Sets conditions under which a packet passes a named IP access list.
remark	Writes a helpful comment (remark) for an entry in a named IP access list.
show ip access-list	Displays the contents of all current IP access lists.
time-range	Specifies when an access list or other feature is in effect.

dynamic

To define a named dynamic IP access list, use the **dynamic** access-list configuration command. To remove the access lists, use the **no** form of this command.

dynamic *dynamic-name* [**timeout** *minutes*] {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log**] [**fragments**]

no dynamic *dynamic-name*

Internet Control Message Protocol (ICMP)

For ICMP, you can also use the following syntax:

dynamic *dynamic-name* [**timeout** *minutes*] {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*] | *icmp-message*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**fragments**]

Internet Group Management Protocol (IGMP)

For IGMP, you can also use the following syntax:

dynamic *dynamic-name* [**timeout** *minutes*] {**deny** | **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**fragments**]

Transmission Control Protocol (TCP)

For TCP, you can also use the following syntax:

dynamic *dynamic-name* [**timeout** *minutes*] {**deny** | **permit**} **tcp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**fragments**]

User Datagram Protocol (UDP)

For UDP, you can also use the following syntax:

dynamic *dynamic-name* [**timeout** *minutes*] {**deny** | **permit**} **udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**fragments**]

Caution Named IP access lists will not be recognized by any software release prior to Cisco IOS Release 11.2.

Syntax Description

dynamic-name	Identifies this access list as a dynamic access list. Refer to lock-and-key access documented in the "Configuring Lock-and-Key Security (Dynamic Access Lists)" chapter in the *Cisco IOS Security Configuration Guide*.
timeout *minutes*	(Optional) Specifies the absolute length of time (in minutes) that a temporary access list entry can remain in a dynamic access list. The default is an infinite length of time and allows an entry to remain permanently. Refer to lock-and-key access documented in the "Configuring Lock-and-Key Security (Dynamic Access Lists)" chapter in the *Cisco IOS Security Configuration Guide*.

deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
protocol	Name or number of an Internet protocol. It can be one of the keywords **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the **ip** keyword. Some protocols allow further qualifiers described later.
source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part, dotted decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part, dotted decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part, dotted decimal format. • Use the **any** keyword as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
precedence *precedence*	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7, or by name as listed in the section "Usage Guidelines."
tos *tos*	(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15, or by name as listed in the section "Usage Guidelines."

deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
protocol	Name or number of an Internet protocol. It can be one of the keywords **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the **ip** keyword. Some protocols allow further qualifiers described later.
source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part, dotted decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part, dotted decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part, dotted decimal format. • Use the **any** keyword as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
precedence *precedence*	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7, or by name as listed in the section "Usage Guidelines."
tos *tos*	(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15, or by name as listed in the section "Usage Guidelines."

log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. Use the **ip access-list log-update** command to generate logging messages when the number of matches reaches a configurable threshold (rather than waiting for a 5-minute interval). See the **ip access-list log-update** command for more information. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
icmp-code	(Optional) ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
icmp-message	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are found in the section "Usage Guidelines."
igmp-type	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the section "Usage Guidelines."
operator	(Optional) Compares source or destination ports. Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source* and *source-wildcard*, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard*, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number.
port	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the section "Usage Guidelines" of the **access-list** (IP extended) command. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.

established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
fragments	(Optional) The access list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List Processing of Fragments" and "Fragments and Policy Routing" sections in the "Usage Guidelines" section.

Defaults

An extended access list defaults to a list that denies everything. An extended access list is terminated by an implicit deny statement.

Command Modes

Access-list configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0(11) and 12.1(2)	The **fragments** keyword was added.

Usage Guidelines

You can use named access lists to control the transmission of packets on an interface and restrict contents of routing updates. The Cisco IOS software stops checking the extended access list after a match occurs.

Fragmented IP packets, other than the initial fragment, are immediately accepted by any extended IP access list. Extended access lists used to control vty access or restrict the contents of routing updates must not match against the TCP source port, the ToS value, or the precedence of the packet.

Note After an access list is created initially, any subsequent additions (possibly entered from the terminal) are placed at the end of the list. In other words, you cannot selectively add or remove access list command lines from a specific access list.

The following is a list of precedence names:

- **critical**
- **flash**
- **flash-override**
- **immediate**
- **internet**
- **network**
- **priority**
- **routine**

The following is a list of ToS names:

- **max-reliability**
- **max-throughput**

- **min-delay**
- **min-monetary-cost**
- **normal**

The following is a list of ICMP message type names and ICMP message type and code names:

- **administratively-prohibited**
- **alternate-address**
- **conversion-error**
- **dod-host-prohibited**
- **dod-net-prohibited**
- **echo**
- **echo-reply**
- **general-parameter-problem**
- **host-isolated**
- **host-precedence-unreachable**
- **host-redirect**
- **host-tos-redirect**
- **host-tos-unreachable**
- **host-unknown**
- **host-unreachable**
- **information-reply**
- **information-request**
- **mask-reply**
- **mask-request**
- **mobile-redirect**
- **net-redirect**
- **net-tos-redirect**
- **net-tos-unreachable**
- **net-unreachable**
- **network-unknown**
- **no-room-for-option**
- **option-missing**
- **packet-too-big**
- **parameter-problem**
- **port-unreachable**
- **precedence-unreachable**
- **protocol-unreachable**
- **reassembly-timeout**
- **redirect**

- **router-advertisement**
- **router-solicitation**
- **source-quench**
- **source-route-failed**
- **time-exceeded**
- **timestamp-reply**
- **timestamp-request**
- **traceroute**
- **ttl-exceeded**
- **unreachable**

The following is a list of IGMP message names:

- **dvmrp**
- **host-query**
- **host-report**
- **pim**
- **trace**

The following is a list of TCP port names that can be used instead of port numbers. Refer to the current assigned numbers RFC to find a reference to these protocols. Port numbers corresponding to these protocols can also be found if you type a **?** in the place of a port number.

- **bgp**
- **chargen**
- **daytime**
- **discard**
- **domain**
- **echo**
- **finger**
- **ftp**
- **ftp-data**
- **gopher**
- **hostname**
- **irc**
- **klogin**
- **kshell**
- **lpd**
- **nntp**
- **pop2**
- **pop3**
- **smtp**

- **sunrpc**
- **syslog**
- **tacacs-ds**
- **talk**
- **telnet**
- **time**
- **uucp**
- **whois**
- **www**

The following is a list of UDP port names that can be used instead of port numbers. Refer to the current assigned numbers RFC to find a reference to these protocols. Port numbers corresponding to these protocols can also be found if you type a **?** in the place of a port number.

- **biff**
- **bootpc**
- **bootps**
- **discard**
- **dns**
- **dnsix**
- **echo**
- **mobile-ip**
- **nameserver**
- **netbios-dgm**
- **netbios-ns**
- **ntp**
- **rip**
- **snmp**
- **snmptrap**
- **sunrpc**
- **syslog**
- **tacacs-ds**
- **talk**
- **tftp**
- **time**
- **who**
- **xdmcp**

Access List Processing of Fragments

The behavior of access-list entries regarding the use or lack of the **fragments** keyword can be summarized as follows:

If the Access-List Entry has...	Then..
...no **fragments** keyword (the default behavior), and assuming all of the access-list entry information matches,	For an access-list entry containing only Layer 3 information: • The entry is applied to nonfragmented packets, initial fragments and noninitial fragments. For an access list entry containing Layer 3 and Layer 4 information: • The entry is applied to nonfragmented packets and initial fragments. – If the entry is a **permit** statement, the packet or fragment is permitted. – If the entry is a **deny** statement, the packet or fragment is denied. • The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access-list entry can be applied. If the Layer 3 portion of the access-list entry matches, and – If the entry is a **permit** statement, the noninitial fragment is permitted. – If the entry is a **deny** statement, the next access-list entry is processed. **Note** The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.
...the **fragments** keyword, and assuming all of the access-list entry information matches,	**Note** The access-list entry is applied only to noninitial fragments.The **fragments** keyword cannot be configured for an access-list entry that contains any Layer 4 information.

Be aware that you should not simply add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments** keyword, the packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword, and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases where

there are multiple **deny** access list entries for the same host but with different Layer 4 ports, a single **deny** access-list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets and each counts individually as a packet in access list accounting and access list violation counts.

Note The **fragments** keyword cannot solve all cases involving access lists and IP fragments.

Fragments and Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address** command and the access list had entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy routed, even if the first fragment was not policy routed or the reverse.

By using the **fragments** keyword in access list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made and it is more likely policy routing will occur as intended.

Examples

The following example defines a dynamic access list named washington:

```
ip access-group washington in
!
ip access-list extended washington
 dynamic testlist timeout 5
 permit ip any any
 permit tcp any host 185.302.21.2 eq 23
```

Related Commands

Command	Description
clear access-template	Clears a temporary access list entry from a dynamic access list manually.
distribute-list in (IP)	Filters networks received in updates.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
ip access-group	Controls access to an interface.
ip access-list	Defines an IP access list by name.
ip access-list log-update	Sets the threshold number of packets that cause a logging message.
logging console	Limits messages logged to the console based on severity.
show access-lists	Displays the contents of current IP and rate-limit access lists.
show ip access-list	Displays the contents of all current IP access lists.

forwarding-agent

To specify the port on which the Forwarding Agent will listen for wildcard and fixed affinities, use the **forwarding-agent** command in CASA-port configuration mode. To disable listening on that port, use the **no** form of the command.

forwarding-agent *port-number* [*password* [*timeout*]]

no forwarding-agent

Syntax Description

port-number	Port numbers on which the Forwarding Agent will listen for wildcards broadcast from the services manager. This must match the port number defined on the services manager.
password	(Optional) Text password used for generating the MD5 digest.
timeout	(Optional) Duration (in seconds) during which the Forwarding Agent will accept the new and old password. Valid range is from 0 to 3600 seconds. The default is 180 seconds.

Defaults

The default password timeout is 180 seconds.

The default port for the services manager is 1637.

Command Modes

CASA-port configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

The following example specifies that the Forwarding Agent will listen for wildcard and fixed affinities on port 1637:

```
forwarding-agent 1637
```

Related Commands

Command	Description
show ip casa oper	Displays operational information about the Forwarding Agent.

ip access-group

To control access to an interface, use the **ip access-group** command in interface configuration mode. To remove the specified access group, use the **no** form of this command.

ip access-group {*access-list-number* | *access-list-name*}{**in** | **out**}

no ip access-group {*access-list-number* | *access-list-name*}{**in** | **out**}

Syntax Description

access-list-number	Number of an access list. This is a decimal number from 1 to 199 or from 1300 to 2699.
access-list-name	Name of an IP access list as specified by an **ip access-list** command.
in	Filters on inbound packets.
out	Filters on outbound packets.

Defaults

No access list is applied to the interface.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-name* argument was added.

Usage Guidelines

Access lists are applied on either outbound or inbound interfaces. For standard inbound access lists, after receiving a packet, the Cisco IOS software checks the source address of the packet against the access list. For extended access lists, the router also checks the destination access list. If the access list permits the address, the software continues to process the packet. If the access list rejects the address, the software discards the packet and returns an ICMP host unreachable message.

For standard outbound access lists, after receiving and routing a packet to a controlled interface, the software checks the source address of the packet against the access list. For extended access lists, the router also checks the destination access list. If the access list permits the address, the software sends the packet. If the access list rejects the address, the software discards the packet and returns an ICMP host unreachable message.

If the specified access list does not exist, all packets are passed.

When you enable outbound access lists, you automatically disable autonomous switching for that interface. When you enable input access lists on any CBus or CxBus interface, you automatically disable autonomous switching for all interfaces (with one exception—an SSE configured with simple access lists can still switch packets, on output only).

Examples

The following example applies list 101 on packets outbound from Ethernet interface 0:

```
interface ethernet 0
 ip access-group 101 out
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
ip access-list	Defines an IP access list by name.
show access-lists	Displays the contents of current IP and rate-limit access lists.

ip access-list

To define an IP access list by name, use the **ip access-list** command in global configuration mode. To remove a named IP access list, use the **no** form of this command.

ip access-list {**standard** | **extended**} *access-list-name*

no ip access-list {**standard** | **extended**} *access-list-name*

Caution Named access lists will not be recognized by any software release prior to Cisco IOS Release 11.2.

Syntax Description

standard	Specifies a standard IP access list.
extended	Specifies an extended IP access list.
access-list-name	Name of the access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

Defaults

No named IP access list is defined.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to configure a named IP access list as opposed to a numbered IP access list. This command will take you into access-list configuration mode, where you must define the denied or permitted access conditions with the **deny** and **permit** commands.

Specifying the **standard** or **extended** keyword with the **ip access-list** command determines the prompt you get when you enter access-list configuration mode.

Use the **ip access-group** command to apply the access list to an interface.

Named access lists are not compatible with Cisco IOS releases prior to Release 11.2.

Examples

The following example defines a standard access list named Internetfilter:

```
ip access-list standard Internetfilter
 permit 192.5.34.0  0.0.0.255
 permit 128.88.0.0  0.0.255.255
 permit 36.0.0.0  0.255.255.255
! (Note: all other access implicitly denied)
```

Related Commands

Command	Description
access list (IP extended)	Defines an extended IP access list.
access list (IP standard)	Defines a standard IP access list.
access-list remark	Writes a helpful comment (remark) for an entry in a numbered access list.
deny (IP)	Sets conditions for a named IP access list.
ip access-group	Controls access to an interface.
permit (IP)	Sets conditions for a named IP access list.
remark	Writes a helpful comment (remark) for an entry in a named IP access list.
show ip access-list	Displays the contents of all current IP access lists.

ip access-list log-update

To set the threshold number of packets that generate a log message if they match an access list, use the **ip access-list log-update** command in global configuration mode. To remove the threshold, use the **no** form of this command.

ip access-list log-update threshold *number-of-matches*

no ip access-list log-update

Syntax Description

number-of-matches	Threshold number of packets necessary to match an access list before a log message is generated. The range is 0 to 2147483647. There is no default number of matches.

Defaults

Log messages are sent at the first matching packet and at 5-minute intervals after that.

Command Modes

Global configuration

Command History

Release	Modification
12.0(2)T	This command was introduced.

Usage Guidelines

Log messages are generated if you have specified the **log** keyword in the **access-list (IP standard)**, **access-list (IP extended)**, **deny (IP)**, **dynamic**, or **permit** command.

Log messages provide information about the packets that are permitted or denied by an access list. By default, log messages appear at the console. (The level of messages logged to the console is controlled by the **logging console** command.) The log message includes the access list number, whether the packet was permitted or denied, and other information.

By default, the log messages are sent at the first matching packet and after that, identical messages are accumulated for 5-minute intervals, with a single message being sent with the number of packets permitted and denied during that interval. However, you can use the **ip access-list log-update** command to set the number of packets that, when match an access list (and are permitted or denied), cause the system to generate a log message. You might want to do this to receive log messages more frequently than at 5-minute intervals.

Caution If you set the *number-of-matches* argument to 1, a log message is sent right away, rather than caching it; every packet that matches an access list causes a log message. A setting of 1 is not recommended because the volume of log messages could overwhelm the system.

Even if you use the **ip access-list log-update** command, the 5-minute timer remains in effect, so the cache is emptied at the end of 5 minutes, regardless of the count of messages in the cache. Regardless of when the log message is sent, the cache is flushed and the count reset to 0 for that message the same way it is when a threshold is not specified.

If the syslog server is not directly connected to a LAN that the router shares, any intermediate router might drop the log messages because they are UDP (unreliable) messages.

Examples

The following example enables logging whenever the 1000th packet matches an access list entry:

```
ip access-list log-update threshold 1000
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
deny (IP)	Sets conditions under which a packet is denied by a named IP access list.
dynamic	Defines a named dynamic IP access list.
logging console	Limits messages logged to the console, based on severity.
permit	Sets conditions under which a packet passes a named IP access list.

ip accounting

To enable IP accounting on an interface, use the **ip accounting** command in interface configuration mode. To disable IP accounting, use the **no** form of this command.

ip accounting [**access-violations**] [**output-packets**]

no ip accounting [**access-violations**] [**output-packets**]

Syntax Description

access-violations	(Optional) Enables IP accounting with the ability to identify IP traffic that fails IP access lists.
output-packets	(Optional) Enables IP accounting based on the IP packets output on the interface.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The **access-violations** keyword was added.

Usage Guidelines

The **ip accounting** command records the number of bytes (IP header and data) and packets switched through the system on a source and destination IP address basis. Only transit IP traffic is measured and only on an outbound basis; traffic generated by the router access server or terminating in this device is not included in the accounting statistics. Traffic coming from a remote site and transiting through a router is also recorded.

If you specify the **access-violations** keyword, the **ip accounting** command provides information identifying IP traffic that fails IP access lists. Identifying IP source addresses that violate IP access lists alerts you to possible attempts to breach security. The data might also indicate that you should verify IP access list configurations.

To receive a logging message on the console when an extended access list entry denies a packet access (to log violations), you must include the **log** keyword in the **access-list** (IP extended) or **access-list** (IP standard) command.

Statistics are accurate even if IP fast switching or IP access lists are being used on the interface.

IP accounting disables autonomous switching, SSE switching, and distributed switching (dCEF) on the interface. IP accounting will cause packets to be switched on the Route Switch Processor (RSP) instead of the Versatile Interface Processor (VIP), which can cause performance degradation.

Examples

The following example enables IP accounting on Ethernet interface 0:

```
interface ethernet 0
 ip accounting
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
clear ip accounting	Clears the active or checkpointed database when IP accounting is enabled.
ip accounting-list	Defines filters to control the hosts for which IP accounting information is kept.
ip accounting-threshold	Sets the maximum number of accounting entries to be created.
ip accounting-transits	Controls the number of transit records that are stored in the IP accounting database.
show ip accounting	Displays the active accounting or checkpointed database or displays access list violations.

ip accounting-list

To define filters to control the hosts for which IP accounting information is kept, use the **ip accounting-list** command in global configuration mode. To remove a filter definition, use the **no** form of this command.

ip accounting-list *ip-address wildcard*

no ip accounting-list *ip-address wildcard*

Syntax Description

ip-address	IP address in dotted decimal format.
wildcard	Wildcard bits to be applied to the *ip-address* argument.

Defaults

No filters are defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The *wildcard* argument is a 32-bit quantity written in dotted-decimal format. Address bits corresponding to wildcard bits set to 1 are ignored in comparisons; address bits corresponding to wildcard bits set to zero are used in comparisons.

Examples

The following example adds all hosts with IP addresses beginning with 192.31 to the list of hosts for which accounting information will be kept:

```
ip accounting-list 192.31.0.0 0.0.255.255
```

Related Commands

Command	Description
clear ip accounting	Clears the active or checkpointed database when IP accounting is enabled.
ip accounting	Enables IP accounting on an interface.
ip accounting-threshold	Sets the maximum number of accounting entries to be created.
ip accounting-transits	Controls the number of transit records that are stored in the IP accounting database.
show ip accounting	Displays the active accounting or checkpointed database or displays access list violations.

ip accounting-threshold

To set the maximum number of accounting entries to be created, use the **ip accounting-threshold** command in global configuration mode. To restore the default number of entries, use the **no** form of this command.

ip accounting-threshold *threshold*

no ip accounting-threshold *threshold*

Syntax Description

threshold	Maximum number of entries (source and destination address pairs) that the Cisco IOS software accumulates.

Defaults

The default maximum number of accounting entries is 512 entries.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The accounting threshold defines the maximum number of entries (source and destination address pairs) that the software accumulates, preventing IP accounting from possibly consuming all available free memory. This level of memory consumption could occur in a router that is switching traffic for many hosts. Overflows will be recorded; see the monitoring commands for display formats.

The default accounting threshold of 512 entries results in a maximum table size of 12,928 bytes. Active and checkpointed tables can reach this size independently.

Examples

The following example sets the IP accounting threshold to only 500 entries:

```
ip accounting-threshold 500
```

Related Commands

Command	Description
clear ip accounting	Clears the active or checkpointed database when IP accounting is enabled.
ip accounting	Enables IP accounting on an interface.
ip accounting-list	Defines filters to control the hosts for which IP accounting information is kept.
ip accounting-transits	Controls the number of transit records that are stored in the IP accounting database.
show ip accounting	Displays the active accounting or checkpointed database or displays access list violations.

ip accounting-transits

To control the number of transit records that are stored in the IP accounting database, use the **ip accounting-transits** command in global configuration mode. To return to the default number of records, use the **no** form of this command.

ip accounting-transits *count*

no ip accounting-transits

Syntax Description

count	Number of transit records to store in the IP accounting database.

Defaults

The default number of transit records that are stored in the IP accounting database is 0.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Transit entries are those that do not match any of the filters specified by **ip accounting-list** global configuration commands. If no filters are defined, no transit entries are possible.

To maintain accurate accounting totals, the Cisco IOS software maintains two accounting databases: an active and a checkpointed database.

Examples

The following example specifies that no more than 100 transit records are stored:

```
ip accounting-transits 100
```

Related Commands

Command	Description
clear ip accounting	Clears the active or checkpointed database when IP accounting is enabled.
ip accounting	Enables IP accounting on an interface.
ip accounting-list	Defines filters to control the hosts for which IP accounting information is kept.
ip accounting-threshold	Sets the maximum number of accounting entries to be created.
show ip accounting	Displays the active accounting or checkpointed database or displays access list violations.

ip accounting mac-address

To enable IP accounting on a LAN interface based on the source and destination MAC address, use the **ip accounting mac-address** command in interface configuration mode. To disable IP accounting based on the source and destination MAC address, use the **no** form of this command.

ip accounting mac-address {**input** | **output**]

no ip accounting mac-address {**input** | **output**]

Syntax Description

input	Performs accounting based on the source MAC address on received packets.
output	Performs accounting based on the destination MAC address on transmitted packets.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	This command was introduced.

Usage Guidelines

This feature is supported on Ethernet, FastEthernet, and FDDI interfaces.

To display the MAC accounting information, use the **show interface mac** EXEC command.

MAC address accounting provides accounting information for IP traffic based on the source and destination MAC address on LAN interfaces. This calculates the total packet and byte counts for a LAN interface that receives or sends IP packets to or from a unique MAC address. It also records a timestamp for the last packet received or sent. With MAC address accounting, you can determine how much traffic is being sent to and/or received from various peers at NAPS/peering points.

Examples

The following example enables IP accounting based on the source and destination MAC address for received and transmitted packets:

```
interface ethernet 4/0/0
  ip accounting mac-address input
  ip accounting mac-address output
```

Related Commands

Command	Description
show interface mac	Displays MAC accounting information for interfaces configured for MAC accounting.

ip accounting precedence

To enable IP accounting on any interface based on IP precedence, use the **ip accounting precedence** command in interface configuration mode. To disable IP accounting based on IP precedence, use the **no** form of this command.

ip accounting precedence {**input** | **output**]

no ip accounting precedence {**input** | **output**]

Syntax Description

input	Performs accounting based on IP precedence on received packets.
output	Performs accounting based on IP precedence on transmitted packets.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	This command was introduced.

Usage Guidelines

To display IP precedence accounting information, use the **show interface precedence** EXEC command.

The precedence accounting feature provides accounting information for IP traffic, summarized by IP precedence value(s). This feature calculates the total packet and byte counts for an interface that receives or sends IP packets and sorts the results based on IP precedence. This feature is supported on all interfaces and subinterfaces and supports CEF, dCEF, flow, and optimum switching.

Examples

The following example enables IP accounting based on IP precedence for received and transmitted packets:

```
interface ethernet 4/0/0
  ip accounting precedence input
  ip accounting precedence output
```

Related Commands

Command	Description
show interface precedence	Displays precedence accounting information for an interface configured for precedence accounting.

ip casa

To configure the router to function as a forwarding agent, use the **ip casa** command in global configuration mode. To disable the forwarding agent, use the **no** form of this command.

ip casa *control-address igmp-address*

no ip casa

Syntax Description

control-address	IP address of the Forwarding Agent side of the services manager/Forwarding Agent tunnel used for sending signals. This address is unique for each Forwarding Agent.
igmp-address	IGMP address on which the Forwarding Agent will listen for wildcard and fixed affinities.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

The following example specifies the Internet address (10.10.4.1) and IGMP address (224.0.1.2) for the Forwarding Agent:

```
ip-casa 10.10.4.1 224.0.1.2
```

Related Commands

Command	Description
forwarding-agent	Specifies the port on which the Forwarding Agent will listen for wildcard and fixed affinities.

ip drp access-group

To control the sources of Director Response Protocol (DRP) queries to the DRP Server Agent, use the **ip drp access-group** command in global configuration mode. To remove the access list, use the **no** form of this command.

ip drp access-group *access-list-number*

no ip drp access-group *access-list-number*

Syntax Description

access-list-number	Number of a standard IP access list in the range from 1 to 99 or from 1300 to 1999.

Defaults

The DRP Server Agent will answer all queries.

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

This command applies an access list to the interface, thereby controlling which devices can send queries to the DRP Server Agent.

If both an authentication key chain and an access group have been specified, both security measures must permit access before a request is processed.

Examples

The following example configures access list 1, which permits only queries from the host at 33.45.12.4:

```
access-list 1 permit 33.45.12.4
ip drp access-group 1
```

Related Commands

Command	Description
ip drp authentication key-chain	Configures authentication on the DRP Server Agent for DistributedDirector.
show ip drp	Displays information about the DRP Server Agent for DistributedDirector.

ip drp authentication key-chain

To configure authentication on the Director Response Protocol (DRP) Server Agent for DistributedDirector, use the **ip drp authentication key-chain** command in global configuration mode. To remove the key chain, use the **no** form of this command.

ip drp authentication key-chain *name-of-chain*

no ip drp authentication key-chain *name-of-chain*

Syntax Description

name-of-chain	Name of the key chain containing one or more authentication keys.

Defaults

No authentication is configured for the DRP Server Agent.

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

When a key chain and key are configured, the key is used to authenticate all DRP requests and responses. The active key on the DRP Server Agent must match the active key on the primary agent. Use the **key** and **key-string** commands to configure the key.

Examples

The following example configures a key chain named ddchain:

```
ip drp authentication key-chain ddchain
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ip drp access-group	Controls the sources of DRP queries to the DRP Server Agent.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show ip drp	Displays information about the DRP Server Agent for DistributedDirector.
show key chain	Displays authentication key information.

ip drp server

To enable the Director Response Protocol (DRP) Server Agent that works with DistributedDirector, use the **ip drp server** command in global configuration mode. To disable the DRP Server Agent, use the **no** form of this command.

ip drp server

no ip drp server

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Examples

The following example enables the DRP Server Agent:

```
ip drp server
```

Related Commands

Command	Description
ip drp access-group	Controls the sources of DRP queries to the DRP Server Agent.
ip drp authentication key-chain	Configures authentication on the DRP Server Agent for DistributedDirector.
show ip drp	Displays information about the DRP Server Agent for DistributedDirector.

ip icmp rate-limit unreachable

To have the Cisco IOS software limit the rate that Internet Control Message Protocol (ICMP) destination unreachable messages are generated, use the **ip icmp rate-limit unreachable** command in global configuration mode. To remove the rate limit, use the **no** form of this command.

ip icmp rate-limit unreachable [**df**] *milliseconds*

no ip icmp rate-limit unreachable [**df**]

Syntax Description

df	(Optional) Limits the rate ICMP destination unreachable messages are sent when code 4, fragmentation is needed and DF set, is specified in the IP header of the ICMP destination unreachable message.
milliseconds	Time limit (in milliseconds) in which one ICMP destination unreachable message is sent. The range is 1 millisecond to 4294967295 milliseconds.

Defaults

The default value is one ICMP destination unreachable message per 500 milliseconds.

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The **no ip icmp rate-limit unreachable** command turns off the previously configured rate limit. To re-set the rate limit to its default value, use the **default ip icmp rate-limit unreachable** command.

The Cisco IOS software maintains two timers: one for general destination unreachable messages and one for DF destination unreachable messages. Both share the same time limits and defaults. If the **df** option is not configured, the **ip icmp rate-limit unreachable** command sets the time values for DF destination unreachable messages. If the **df** option is configured, its time values remain independent from those of general destination unreachable messages.

Examples

The following example sets the rate of the ICMP destination unreachable message to one message every 10 milliseconds:

```
ip icmp rate-limit unreachable 10
```

The following example turns off the previously configured rate limit:

```
no ip icmp rate-limit unreachable
```

The following example sets the rate limit back to the default:

```
default ip icmp rate-limit unreachable
```

ip icmp redirect

To control the type of Internet Control Message Protocol (ICMP) redirect message that is sent by the Cisco IOS software, use the **ip icmp redirect** command in global configuration mode. To set the value back to the default, use the **no** form of this command.

ip icmp redirect [**host** | **subnet**]

no ip icmp redirect [**host** | **subnet**]

Syntax Description

host	(Optional) Sends ICMP host redirects.
subnet	(Optional) Sends ICMP subnet redirects.

Defaults

The router will send ICMP subnet redirect messages.

Because the **ip icmp redirect subnet** command is the default, the command will not be displayed in the configuration.

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

An ICMP redirect message can be generated by a router when a packet is received and transmitted on the same interface. In this situation, the router will forward the original packet and send a ICMP redirect message back to the sender of the original packet. This behavior allows the sender to bypass the router and forward future packets directly to the destination (or a router closer to the destination).

There are two types of ICMP redirect messages: redirect for a host address or redirect for an entire subnet.

The **ip icmp redirect** command determines the type of ICMP redirects sent by the system and is configured on a per system basis. Some hosts do not understand ICMP subnet redirects and need the router to send out ICMP host redirects. Use the **ip icmp redirect host** command to have the router send out ICMP host redirects. Use the **ip icmp redirect subnet** command to set the value back to the default, which is to send subnet redirects.

To prevent the router from sending ICMP redirects, use the **no ip redirects** interface configuration command.

Examples

The following example enables the router to send out ICMP host redirects:

```
ip icmp redirect hosts
```

The following example sets the value back to the default, which is subnet redirects:

```
ip icmp redirect subnet
```

Related Commands

Command	Description
ip redirects	Enables the sending of ICMP redirect messages.

ip mask-reply

To have the Cisco IOS software respond to Internet Control Message Protocol (ICMP) mask requests by sending ICMP mask reply messages, use the **ip mask-reply** command in interface configuration mode. To disable this function, use the **no** form of this command.

ip mask-reply

no ip mask-reply

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example enables the sending of ICMP mask reply messages on Ethernet interface 0:

```
interface ethernet 0
 ip address 131.108.1.0 255.255.255.0
 ip mask-reply
```

ip mtu

To set the maximum transmission unit (MTU) size of IP packets sent on an interface, use the **ip mtu** interface configuration command. To restore the default MTU size, use the **no** form of this command.

ip mtu *bytes*

no ip mtu

Syntax Description

bytes	MTU in bytes.

Defaults

Minimum is 128 bytes; maximum depends on the interface medium.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

If an IP packet exceeds the MTU set for the interface, the Cisco IOS software will fragment it.

All devices on a physical medium must have the same protocol MTU in order to operate.

Note Changing the MTU value (with the **mtu** interface configuration command) can affect the IP MTU value. If the current IP MTU value is the same as the MTU value, and you change the MTU value, the IP MTU value will be modified automatically to match the new MTU. However, the reverse is not true; changing the IP MTU value has no effect on the value for the **mtu** command.

Examples

The following example sets the maximum IP packet size for the first serial interface to 300 bytes:

```
interface serial 0
 ip mtu 300
```

Related Commands

Command	Description
mtu	Adjusts the maximum packet size or MTU size.

ip redirects

To enable the sending of Internet Control Message Protocol (ICMP) redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received, use the **ip redirects** interface configuration command. To disable the sending of redirect messages, use the **no** form of this command.

ip redirects

no ip redirects

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Previously, if the Hot Standby Router Protocol (HSRP) was configured on an interface, ICMP redirect messages were disabled by default for the interface. With Cisco IOS Release 12.1(3)T, ICMP redirect messages are enabled by default if HSRP is configured.

Examples

The following example enables the sending of ICMP redirect messages on Ethernet interface 0:

```
interface ethernet 0
 ip redirects
```

Related Commands

Command	Description
ip default-gateway	Defines a default gateway (router) when IP routing is disabled.
show ip redirects	Displays the address of a default gateway (router) and the address of hosts for which an ICMP redirect message has been received.

ip source-route

To allow the Cisco IOS software to handle IP datagrams with source routing header options, use the **ip source-route** global configuration command. To have the software discard any IP datagram containing a source-route option, use the **no** form of this command.

ip source-route

no ip source-route

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example enables the handling of IP datagrams with source routing header options:

```
ip source-route
```

Related Commands

Command	Description
ping (privileged)	Diagnoses basic network connectivity (in privileged EXEC mode) on Apollo, AppleTalk, CLNS, DECnet, IP, Novell IPX, VINES, or XNS networks.
ping (user)	Diagnoses basic network connectivity (in user EXEC mode) on Apollo, AppleTalk, CLNS, DECnet, IP, Novell IPX, VINES, or XNS networks.

ip tcp chunk-size

To alter the TCP maximum read size for Telnet or rlogin, use the **ip tcp chunk-size** global configuration command. To restore the default value, use the **no** form of this command.

ip tcp chunk-size *characters*

no ip tcp chunk-size

Syntax Description

characters	Maximum number of characters that Telnet or rlogin can read in one read instruction. The default value is 0, which Telnet and rlogin interpret as the largest possible 32-bit positive number.

Defaults

0, which Telnet and rlogin interpret as the largest possible 32-bit positive number.

Command Modes

Global configuration

Command History

Release	Modification
9.1	This command was introduced.

Usage Guidelines

It is unlikely you will need to change the default value.

Examples

The following example sets the maximum TCP read size to 64,000 bytes:

```
ip tcp chunk-size 64000
```

ip tcp compression-connections

To specify the total number of TCP header compression connections that can exist on an interface, use the **ip tcp compression-connections** interface configuration command. To restore the default, use the **no** form of this command.

ip tcp compression-connections *number*

no ip tcp compression-connections *number*

Syntax Description

number	Number of TCP header compression connections the cache supports, in the range from 3 to 1000. The default is 32 connections (16 calls).

Defaults

The default number is 32 connections.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	For Frame Relay, PPP, and High-Level Data Link Control (HDLC) encapsulation, the maximum number of compression connections increased to 256. For Frame Relay, the maximum value is fixed, not configurable.

Usage Guidelines

You should configure one connection for each TCP connection through the specified interface.

Each connection sets up a compression cache entry, so you are in effect specifying the maximum number of cache entries and the size of the cache. Too few cache entries for the specified interface can lead to degraded performance, and too many cache entries can lead to wasted memory.

Note Both ends of the serial connection must use the same number of cache entries.

Examples

The following example sets the first serial interface for header compression with a maximum of ten cache entries:

```
interface serial 0
 ip tcp header-compression
 ip tcp compression-connections 10
```

Related Commands

Command	Description
ip rtp header-compression	Enables RTP header compression.
ip tcp header-compression	Enables TCP header compression.
show ip rtp header-compression	Displays RTP header compression statistics.

ip tcp header-compression

To enable TCP header compression, use the **ip tcp header-compression** interface configuration command. To disable compression, use the **no** form of this command.

ip tcp header-compression [**passive**]

no ip tcp header-compression [**passive**]

Syntax Description

passive	(Optional) Compresses outgoing TCP packets only if incoming TCP packets on the same interface are compressed. If you do not specify the **passive** keyword, the Cisco IOS software compresses all traffic.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can compress the headers of your TCP/IP packets in order to reduce the size of your packets. TCP header compression is supported on serial lines using Frame Relay, HDLC, or PPP encapsulation. You must enable compression on both ends of a serial connection. RFC 1144 specifies the compression process. Compressing the TCP header can speed up Telnet connections dramatically. In general, TCP header compression is advantageous when your traffic consists of many small packets, not for traffic that consists of large packets. Transaction processing (usually using terminals) tends to use small packets and file transfers use large packets. This feature only compresses the TCP header, so it has no effect on UDP packets or other protocol headers.

When compression is enabled, fast switching is disabled. This condition means that fast interfaces like T1 can overload the router. Consider the traffic characteristics of your network before using this command.

Examples

The following example sets the first serial interface for header compression with a maximum of ten cache entries:

```
interface serial 0
 ip tcp header-compression
 ip tcp compression-connections 10
```

Related Commands

Command	Description
ip tcp header-compression	Specifies the total number of header compression connections that can exist on an interface.

ip tcp mss

To enable a maximum segment size (MSS) for TCP connections originating or terminating on a router, use the **ip tcp mss** command in global configuration mode. To disable the configuration of the MSS, use the **no** form of this command.

ip tcp mss *mss-value*

no ip tcp mss *mss-value*

Syntax Description

mss-value	Maximum segment size for TCP connections in bytes. The range is from 68 to 10000.

Defaults

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(05)S	This command was introduced.
12.1	This command was integrated into Cisco IOS Release 12.1.

Usage Guidelines

If this command is not enabled, the MSS value of 536 bytes is used if the destination is not on a LAN, otherwise the MSS value is 1460 for a local destination.

For connections originating from a router, the specified value is used directly as an MSS option in the synchronize (SYN) segment. For connections terminating on a router, the value is used only if the incoming SYN segment has an MSS option value higher than the configured value. Otherwise the incoming value is used as the MSS option in the SYN/acknowledge (ACK) segment.

Note The **ip tcp mss** command interacts with the **ip tcp path-mtu-discovery** command and not the **ip tcp header-compression** command. The **ip tcp path-mtu-discovery** command changes the default MSS to 1460 even for non-local nodes.

Examples

The following example sets the MSS value at 250:

```
ip tcp mss 250
```

Related Commands

Command	Description
ip tcp header-compression	Specifies the total number of header compression connections that can exist on an interface.

ip tcp path-mtu-discovery

To enable the Path MTU Discovery feature for all new TCP connections from the router, use the **ip tcp path-mtu-discovery** global configuration command. To disable the function, use the **no** form of this command.

ip tcp path-mtu-discovery [**age-timer** {*minutes* | **infinite**}]

no ip tcp path-mtu-discovery [**age-timer** {*minutes* | **infinite**}]

Syntax Description

age-timer *minutes*	(Optional) Time interval (in minutes) after which TCP re-estimates the path MTU with a larger maximum segment size (MSS). The maximum is 30 minutes; the default is 10 minutes.
age-timer infinite	(Optional) Turns off the age timer.

Defaults

Disabled. If enabled, the default *minutes* value is 10 minutes.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
11.2	The **age-timer** and **infinite** keywords were added.

Usage Guidelines

Path MTU Discovery is a method for maximizing the use of available bandwidth in the network between the endpoints of a TCP connection. It is described in RFC 1191. Existing connections are not affected when this feature is turned on or off.

Customers using TCP connections to move bulk data between systems on distinct subnets would benefit most by enabling this feature.

The age timer is a time interval for how often TCP re-estimates the path MTU with a larger MSS. When the age timer is used, TCP path MTU becomes a dynamic process. If the MSS used for the connection is smaller than what the peer connection can handle, a larger MSS is tried every time the age timer expires. The discovery process is stopped when either the send MSS is as large as the peer negotiated, or the user has disabled the timer on the router. You can turn off the age timer by setting it to infinite.

Examples

The following example enables Path MTU Discovery:

```
ip tcp path-mtu-discovery
```

ip tcp queuemax

To alter the maximum TCP outgoing queue per connection, use the **ip tcp queuemax** global configuration command. To restore the default value, use the **no** form of this command.

ip tcp queuemax *packets*

no ip tcp queuemax

Syntax Description

packets	Outgoing queue size of TCP packets. The default value is 5 segments if the connection has a TTY associated with it. If no TTY is associated with it, the default value is 20 segments.

Defaults

The default value is 5 segments if the connection has a TTY associated with it. If no TTY is associated with it, the default value is 20 segments.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Changing the default value changes the 5 segments, not the 20 segments.

Examples

The following example sets the maximum TCP outgoing queue to 10 packets:

```
ip tcp queuemax 10
```

ip tcp selective-ack

To enable TCP selective acknowledgment, use the **ip tcp selective-ack** global configuration command. To disable TCP selective acknowledgment, use the **no** form of this command.

ip tcp selective-ack

no ip tcp selective-ack

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

TCP might not experience optimal performance if multiple packets are lost from one window of data. With the limited information available from cumulative acknowledgments, a TCP sender can learn about only one lost packet per round-trip time. An aggressive sender could resend packets early, but such re-sent segments might have already been received.

The TCP selective acknowledgment mechanism helps overcome these limitations. The receiving TCP returns selective acknowledgment packets to the sender, informing the sender about data that has been received. The sender can then resend only the missing data segments.

TCP selective acknowledgment improves overall performance. The feature is used only when a multiple number of packets drop from a TCP window. There is no performance impact when the feature is enabled but not used.

This command becomes effective only on new TCP connections opened after the feature is enabled.

This feature must be disabled if you want TCP header compression. You might disable this feature if you have severe TCP problems.

Refer to RFC 2018 for more detailed information on TCP selective acknowledgment.

Examples

The following example enables the router to send and receive TCP selective acknowledgments:

```
ip tcp selective-ack
```

Related Commands

Command	Description
ip tcp header-compression	Enables TCP header compression.

ip tcp synwait-time

To set a period of time the Cisco IOS software waits while attempting to establish a TCP connection before it times out, use the **ip tcp synwait-time** global configuration command. To restore the default time, use the **no** form of this command.

ip tcp synwait-time *seconds*

no ip tcp synwait-time *seconds*

Syntax Description

seconds	Time (in seconds) the software waits while attempting to establish a TCP connection. It can be an integer from 5 to 300 seconds. The default is 30 seconds.

Defaults

The default time is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

In versions previous to Cisco IOS software Release 10.0, the system would wait a fixed 30 seconds when attempting to establish a TCP connection. If your network contains Public Switched Telephone Network (PSTN) dial-on-demand routing (DDR), the call setup time may exceed 30 seconds. This amount of time is not sufficient in networks that have dialup asynchronous connections because it will affect your ability to Telnet over the link (from the router) if the link must be brought up. If you have this type of network, you might want to set this value to the UNIX value of 75.

Because this is a host parameter, it does not pertain to traffic going *through* the router, just for traffic originated *at* this device. Because UNIX has a fixed 75-second timeout, hosts are unlikely to experience this problem.

Examples

The following example configures the Cisco IOS software to continue attempting to establish a TCP connection for 180 seconds:

```
ip tcp synwait-time 180
```

ip tcp timestamp

To enable TCP time stamp, use the **ip tcp timestamp** global configuration command. To disable TCP time stamp, use the **no** form of this command.

ip tcp timestamp

no ip tcp timestamp

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

TCP time stamp improves round-trip time estimates. Refer to RFC 1323 for more detailed information on TCP time stamp.

This feature must be disabled if you want to use TCP header compression.

Examples

The following example enables the router to send TCP time stamps:

```
ip tcp timestamp
```

Related Commands

Command	Description
ip tcp header-compression	Enables TCP header compression.

ip tcp window-size

To alter the TCP window size, use the **ip tcp window-size** global configuration command. To restore the default value, use the **no** form of this command.

ip tcp window-size *bytes*

no ip tcp window-size

Syntax Description

bytes	Window size (in bytes). The maximum is 65,535 bytes. The default value is 2144 bytes.

Defaults

The default size is 2144 bytes.

Command Modes

Global configuration

Command History

Release	Modification
9.1	This command was introduced.

Usage Guidelines

Do not use this command unless you clearly understand why you want to change the default value.

If your TCP window size is set to 1000 bytes, for example, you could have 1 packet of 1000 bytes or 2 packets of 500 bytes, and so on. However, there is also a limit on the number of packets allowed in the window. There can be a maximum of 5 packets if the connection has TTY; otherwise there can be 20 packets.

Examples

The following example sets the TCP window size to 1000 bytes:

```
ip tcp window-size 1000
```

ip unreachables

To enable the generation of Internet Control Message Protocol (ICMP) unreachable messages, use the **ip unreachables** interface configuration command. To disable this function, use the **no** form of this command.

ip unreachables

no ip unreachables

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

If the Cisco IOS software receives a nonbroadcast packet destined for itself that uses a protocol it does not recognize, it sends an ICMP unreachable message to the source.

If the software receives a datagram that it cannot deliver to its ultimate destination because it knows of no route to the destination address, it replies to the originator of that datagram with an ICMP host unreachable message.

This command affects all types of ICMP unreachable messages.

Examples

The following example enables the generation of ICMP unreachable messages, as appropriate, on an interface:

```
interface ethernet 0
 ip unreachables
```

permit (IP)

To set conditions for a named IP access list, use the **permit** access-list configuration command. To remove a condition from an access list, use the **no** form of this command.

permit *source* [*source-wildcard*]

no permit *source* [*source-wildcard*]

permit *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

no permit *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

Internet Control Message Protocol (ICMP)

For ICMP, you can also use the following syntax:

permit icmp *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*] | *icmp-message*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

Internet Group Management Protocol (IGMP)

For IGMP, you can also use the following syntax:

permit igmp *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

Transmission Control Protocol (TCP)

For TCP, you can also use the following syntax:

permit tcp *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

User Datagram Protocol UDP)

For UDP, you can also use the following syntax:

permit udp *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]

Syntax Description

source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part, dotted decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part, dotted decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
protocol	Name or number of an Internet protocol. It can be one of the keywords **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the **ip** keyword. Some protocols allow further qualifiers described later.
destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the **any** keyword as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part, dotted decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
precedence *precedence*	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7 or by name as listed in the section "Usage Guidelines."
tos *tos*	(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15, or by name as listed in the section "Usage Guidelines" of the **access-list** (IP extended) command.

log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. Use the **ip access-list log-update** command to generate logging messages when the number of matches reaches a configurable threshold (rather than waiting for a 5-minute interval). See the **ip access-list log-update** command for more information. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list. If you enable CEF and then create an access list that uses the **log** keyword, the packets that match the access list are not CEF switched. They are fast switched. Logging disables CEF.
time-range *time-range-name*	(Optional) Name of the time range that applies to this **permit** statement. The name of the time range and its restrictions are specified by the **time-range** and **absolute** or **periodic** commands, respectively.
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
icmp-code	(Optional) ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
icmp-message	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are found in the section "Usage Guidelines" of the **access-list** (IP extended) command.
igmp-type	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the section "Usage Guidelines" of the **access-list** (IP extended) command.
operator	(Optional) Compares source or destination ports. Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source* and *source-wildcard*, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard*, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number.

port	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the section "Usage Guidelines" of the **access-list** (IP extended) command. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
fragments	(Optional) The access list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List Processing of Fragments" and "Fragments and Policy Routing" sections in the "Usage Guidelines" section.

Defaults

There are no specific conditions under which a packet passes the named access list.

Command Modes

Access-list configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0(1)T	The **time-range** *time-range-name* keyword and argument were added.
12.0(11) and 12.1(2)	The **fragments** keyword was added.

Usage Guidelines

Use this command following the **ip access-list** command to define the conditions under which a packet passes the access list.

The **time-range** option allows you to identify a time range by name. The **time-range**, **absolute**, and **periodic** commands specify when this **permit** statement is in effect.

Access List Processing of Fragments

The behavior of access-list entries regarding the use or lack of the **fragments** keyword can be summarized as follows:

If the Access-List Entry has...	Then..
...no **fragments** keyword (the default behavior), and assuming all of the access-list entry information matches,	For an access-list entry containing only Layer 3 information: • The entry is applied to nonfragmented packets, initial fragments and noninitial fragments. For an access list entry containing Layer 3 and Layer 4 information: • The entry is applied to nonfragmented packets and initial fragments. – If the entry is a **permit** statement, the packet or fragment is permitted. – If the entry is a **deny** statement, the packet or fragment is denied. • The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access-list entry can be applied. If the Layer 3 portion of the access-list entry matches, and – If the entry is a **permit** statement, the noninitial fragment is permitted. – If the entry is a **deny** statement, the next access-list entry is processed. **Note** The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.
...the **fragments** keyword, and assuming all of the access-list entry information matches,	The access-list entry is applied only to noninitial fragments. **Note** The **fragments** keyword cannot be configured for an access-list entry that contains any Layer 4 information.

Be aware that you should not simply add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments** keyword, the packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword, and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases where

there are multiple **deny** access list entries for the same host but with different Layer 4 ports, a single **deny** access-list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets and each counts individually as a packet in access list accounting and access list violation counts.

Note The **fragments** keyword cannot solve all cases involving access lists and IP fragments.

Fragments and Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address**s command and the access list had entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy routed, even if the first fragment was not policy routed or the reverse.

By using the **fragments** keyword in access list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made and it is more likely policy routing will occur as intended.

Examples

The following example sets conditions for a standard access list named Internetfilter:

```
ip access-list standard Internetfilter
 deny 192.5.34.0  0.0.0.255
 permit 128.88.0.0  0.0.255.255
 permit 36.0.0.0  0.255.255.255
! (Note: all other access implicitly denied)
```

The following example permits Telnet traffic on Mondays, Tuesdays, and Fridays from 9:00 a.m. to 5:00 p.m.:

```
time-range testing
 periodic Monday Tuesday Friday 9:00 to 17:00
!
ip access-list extended legal
 permit tcp any any eq telnet time-range testing
!
interface ethernet 0
 ip access-group legal in
```

Related Commands

Command	Description
deny (IP)	Sets conditions under which a packet does not pass a named IP access list.
ip access-group	Controls access to an interface.
ip access-list	Defines an IP access list by name.
ip access-list log-update	Sets the threshold number of packets that cause a logging message.
show ip access-list	Displays the contents of all current IP access lists.
time-range	Specifies when an access list or other feature is in effect.

remark

To write a helpful comment (remark) for an entry in a named IP access list, use the **remark** access-list configuration command. To remove the remark, use the **no** form of this command.

remark *remark*

no remark *remark*

Syntax Description

remark	Comment that describes the access list entry, up to 100 characters long.

Defaults

The access list entries have no remarks.

Command Modes

Standard named or extended named access-list configuration

Command History

Release	Modification
12.0(2)T	This command was introduced.

Usage Guidelines

The remark can be up to 100 characters long; anything longer is truncated.

If you want to write a comment about an entry in a numbered IP access list, use the **access-list remark** command.

Examples

In the following example, the Jones subnet is not allowed to use outbound Telnet:

```
ip access-list extended telnetting
 remark Do not allow Jones subnet to telnet out
 deny tcp host 171.69.2.88 any eq telnet
```

Related Commands

Command	Description
access-list remark	Specifies a helpful comment (remark) for an entry in a numbered IP access list.
deny (IP)	Sets conditions under which a packet does not pass a named IP access list.
ip access-list	Defines an IP access list by name.
permit (IP)	Sets conditions under which a packet passes a named IP access list.

show access-lists

To display the contents of current access lists, use the **show access-lists** privileged EXEC command.

show access-lists [*access-list-number* | *access-list-name*]

Syntax Description

access-list-number	(Optional) Number of the access list to display. The system displays all access lists by default.
access-list-name	(Optional) Name of the IP access list to display.

Defaults

The system displays all access lists.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.1(5)T	The command output was modified to identify compiled access lists.

Examples

The following is sample output from the **show access-lists** command when access list 101 is specified:

```
Router# show access-lists 101

Extended IP access list 101
    permit tcp host 198.92.32.130 any established (4304 matches) check=5
    permit udp host 198.92.32.130 any eq domain (129 matches)
    permit icmp host 198.92.32.130 any
    permit tcp host 198.92.32.130 host 171.69.2.141 gt 1023
    permit tcp host 198.92.32.130 host 171.69.2.135 eq smtp (2 matches)
    permit tcp host 198.92.32.130 host 198.92.30.32 eq smtp
    permit tcp host 198.92.32.130 host 171.69.108.33 eq smtp
    permit udp host 198.92.32.130 host 171.68.225.190 eq syslog
    permit udp host 198.92.32.130 host 171.68.225.126 eq syslog
    deny   ip 150.136.0.0 0.0.255.255 224.0.0.0 15.255.255.255
    deny   ip 171.68.0.0 0.1.255.255 224.0.0.0 15.255.255.255 (2 matches) check=1
    deny   ip 172.24.24.0 0.0.1.255 224.0.0.0 15.255.255.255
    deny   ip 192.82.152.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.122.173.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.122.174.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.239.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.240.0 0.0.7.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.248.0 0.0.3.255 224.0.0.0 15.255.255.255
```

An access list counter counts how many packets are allowed by each line of the access list. This number is displayed as the number of matches. Check denotes how many times a packet was compared to the access list but did not match.

The following is sample output from the **show access-lists** command when the Turbo Access Control List (ACL) feature is configured on all of the following access lists.

Note The permit and deny information displayed by the **show access-lists** command may not be in the same order as that entered using the **access-list** command

```
Router# show access-lists
Standard IP access list 1 (Compiled)
    deny   any
Standard IP access list 2 (Compiled)
    deny   192.168.0.0, wildcard bits 0.0.0.255
    permit any
Standard IP access list 3 (Compiled)
    deny   0.0.0.0
    deny   192.168.0.1, wildcard bits 0.0.0.255
    permit any
Standard IP access list 4 (Compiled)
    permit 0.0.0.0
    permit 192.168.0.2, wildcard bits 0.0.0.255
```

For information on how to configure access lists, refer to the "Configuring IP Services" chapter of the *Cisco IOS IP Configuration Guide*.

For information on how to configure dynamic access lists, refer to the "Traffic Filtering and Firewalls" chapter of the *Cisco IOS Security Configuration Guide*.

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
clear access-list counters	Clears the counters of an access list.
clear access-template	Clears a temporary access list entry from a dynamic access list manually.
ip access-list	Defines an IP access list by name.
show access-lists	Displays the contents of all current IP access lists.

show access-list compiled

To display a table showing Turbo Access Control Lists (ACLs), use the **show access-list compiled** EXEC command.

show access-list compiled

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.1(1)E	This command was introduced for Cisco 7200 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

This command is used to display the status and condition of the Turbo ACL tables associated with each access list. The memory usage is displayed for each table; large and complex access lists may require substantial amounts of memory. If the memory usage is greater than the memory available, you can disable the Turbo ACL feature so that memory exhaustion does not occur, but the acceleration of the access lists is not then enabled.

Examples

The following is a partial sample output of the **show access-list compiled** command:

```
Router# show access-list compiled

Compiled ACL statistics:
12 ACLs loaded, 12 compiled tables
 ACL         State      Tables  Entries  Config  Fragment  Redundant  Memory
1           Operational    1        2        1         0          0      1Kb
2           Operational    1        3        2         0          0      1Kb
3           Operational    1        4        3         0          0      1Kb
4           Operational    1        3        2         0          0      1Kb
5           Operational    1        5        4         0          0      1Kb
9           Operational    1        3        2         0          0      1Kb
20          Operational    1        9        8         0          0      1Kb
21          Operational    1        5        4         0          0      1Kb
101         Operational    1       15        9         7          2      1Kb
102         Operational    1       13        6         6          0      1Kb
120         Operational    1        2        1         0          0      1Kb
199         Operational    1        4        3         0          0      1Kb
First level lookup tables:
Block      Use              Rows       Columns   Memory used
  0   TOS/Protocol            6/16      12/16      66048
  1   IP Source (MS)         10/16      12/16      66048
  2   IP Source (LS)         27/32      12/16      132096
  3   IP Dest (MS)            3/16      12/16      66048
  4   IP Dest (LS)            9/16      12/16      66048
```

```
5   TCP/UDP Src Port         1/16     12/16      66048
6   TCP/UDP Dest Port        3/16     12/16      66048
7   TCP Flags/Fragment       3/16     12/16      66048
```

Related Commands

Command	Description
access-list compiled	Enables the Turbo ACL feature.
access-list (extended)	Provides extended access lists that allow more detailed access lists.
access-list (standard)	Creates a standard access list.
clear access-list counters	Clears the counters of an access list.
clear access-temp	Manually clears a temporary access list entry from a dynamic access list.
ip access-list	Defines an IP access list by name.
show ip access-list	Displays the contents of all current IP access lists.

show interface mac

To display MAC accounting information for interfaces configured for MAC accounting, use the **show interface mac** EXEC command.

show interface [*type number*] **mac**

Syntax Description

type	(Optional) Interface type supported on your router.
number	(Optional) Port number of the interface. The syntax varies depending on the type router. For example, on a Cisco 7500 series router the syntax is 0/0/0, where 0 represents the slot, port adapter, and port number (the slash is required). Refer to the appropriate hardware manual for numbering information.

Command Modes

EXEC

Command History

Release	Modification
11.1 CC	This command was introduced.

Usage Guidelines

The **show interface mac** command displays information for all interfaces configured for MAC accounting. To display information for a single interface, use the **show interface** *type number* **mac** command.

For incoming packets on the interface, the accounting statistics are gathered before the CAR/DCAR feature is performed on the packet. For outgoing packets on the interface, the accounting statistics are gathered after output CAR, before output DCAR or DWRED or DWFQ feature is performed on the packet. Therefore, if a you are using DCAR or DWRED on the interface and packets are dropped, the dropped packets are still counted in the **show interface mac** command because the calculations are done prior to the features.

The maximum number of MAC addresses that can be stored for the input address is 512 and the maximum number of MAC address that can be stored for the output address is 512. After the maximum is reached, subsequent MAC addresses are ignored.

To clear the accounting statistics, use the **clear counter** EXEC command. To configure an interface for IP accounting based on the MAC address, use the **ip accounting mac-address** interface configuration command.

Examples

The following is sample output from the **show interface mac** command. This feature calculates the total packet and byte counts for the interface that receives (input) or sends (output) IP packets to or from a unique MAC address. It also records a timestamp for the last packet received or sent.

```
Router# show interface ethernet 0/1/1 mac
Ethernet0/1/1
  Input  (511 free)
    0007.f618.4449(228):  4 packets, 456 bytes, last: 2684ms ago
                  Total:  4 packets, 456 bytes
  Output  (511 free)
    0007.f618.4449(228):  4 packets, 456 bytes, last: 2692ms ago
                  Total:  4 packets, 456 bytes
```

Related Commands

Command	Description
ip accounting mac-address	Enables IP accounting on any interface based on the source and destination MAC address.

show interface precedence

To display precedence accounting information for interfaces configured for precedence accounting, use the **show interface precedence** EXEC command.

show interface [*type number*] **precedence**

Syntax Description

type	(Optional) Interface type supported on your router.
number	(Optional) Port number of the interface. The syntax varies depending on the type router. For example, on a Cisco 7500 series router the syntax is 0/0/0, where 0 represents the slot, port adapter, and port number (the slash is required). Refer to the appropriate hardware manual for numbering information.

Command Modes

EXEC

Command History

Release	Modification
11.1 CC	This command was introduced.

Usage Guidelines

The **show interface precedence** command displays information for all interfaces configured for IP precedence accounting. To display information for a single interface, use the **show interface** *type number* **precedence** command.

For incoming packets on the interface, the accounting statistics are gathered before input CAR/DCAR is performed on the packet. Therefore, if CAR/DCAR changes the precedence on the packet, it is counted based on the old precedence setting with the **show interface precedence** command.

For outgoing packets on the interface, the accounting statistics are gathered after output DCAR or DWRED or DWFQ feature is performed on the packet.

To clear the accounting statistics, use the **clear counter** EXEC command.

To configure an interface for IP accounting based on IP precedence, use the **ip accounting precedence** interface configuration command.

Examples

The following is sample output from the **show interface precedence** command. This feature calculates the total packet and byte counts for the interface that receives (input) or sends (output) IP packets and sorts the results based on IP precedence.

```
Router# show interface ethernet 0/1/1 precedence
Ethernet0/1/1
  Input
    Precedence 0:  4 packets, 456 bytes
  Output
    Precedence 0:  4 packets, 456 bytes
```

Related Commands

Command	Description
ip accounting precedence	Enables IP accounting on any interface based on IP precedence.

show ip access-list

To display the contents of all current IP access lists, use the **show ip access-list** EXEC command.

show ip access-list [*access-list-number* | *access-list-name*]

Syntax Description

access-list-number	(Optional) Number of the IP access list to display.
access-list-name	(Optional) Name of the IP access list to display.

Defaults

Displays all standard and extended IP access lists.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The **show ip access-list** command provides output identical to the **show access-lists** command, except that it is IP-specific and allows you to specify a particular access list.

Examples

The following is sample output from the **show ip access-list** command when all access lists are requested:

```
Router# show ip access-list

Extended IP access list 101
   deny udp any any eq ntp
   permit tcp any any
   permit udp any any eq tftp
   permit icmp any any
   permit udp any any eq domain
```

The following is sample output from the **show ip access-list** command when the name of a specific access list is requested:

```
Router# show ip access-list Internetfilter

Extended IP access list Internetfilter
   permit tcp any 171.69.0.0 0.0.255.255 eq telnet
   deny tcp any any
   deny udp any 171.69.0.0 0.0.255.255 lt 1024
   deny ip any any log
```

show ip accounting

To display the active accounting or checkpointed database or to display access list violations, use the **show ip accounting** EXEC command.

show ip accounting [**checkpoint**] [**output-packets** | **access-violations**]

Syntax Description

checkpoint	(Optional) Indicates that the checkpointed database should be displayed.
output-packets	(Optional) Indicates that information pertaining to packets that passed access control and were routed should be displayed. If neither the **output-packets** nor **access-violations** keyword is specified, **output-packets** is the default.
access-violations	(Optional) Indicates that information pertaining to packets that failed access lists and were not routed should be displayed. If neither the **output-packets** nor **access-violations** keyword is specified, **output-packets** is the default.

Defaults

If neither the **output-packets** nor **access-violations** keyword is specified, the **show ip accounting** command displays information pertaining to packets that passed access control and were routed.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
10.3	The **access-violations** and **output-packet** keywords were added.

Usage Guidelines

If you do not specify any keywords, the **show ip accounting** command displays information about the active accounting database, and traffic coming from a remote site and transiting through a router.

To display IP access violations, you must use the **access-violations** keyword. If you do not specify the keyword, the command defaults to displaying the number of packets that have passed access lists and were routed.

To use this command, you must first enable IP accounting on a per-interface basis.

Examples

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

```
Router# show ip accounting

   Source           Destination              Packets               Bytes
 131.108.19.40    192.67.67.20                   7                 306
 131.108.13.55    192.67.67.20                  67                2749
 131.108.2.50     192.12.33.51                  17                1111
 131.108.2.50     130.93.2.1                     5                 319
 131.108.2.50     130.93.1.2                   463               30991
 131.108.19.40    130.93.2.1                     4                 262
```

```
131.108.19.40    130.93.1.2                28              2552
131.108.20.2     128.18.6.100              39              2184
131.108.13.55    130.93.1.2                35              3020
131.108.19.40    192.12.33.51            1986             95091
131.108.2.50     192.67.67.20             233             14908
131.108.13.28    192.67.67.53             390             24817
131.108.13.55    192.12.33.51          214669           9806659
131.108.13.111   128.18.6.23            27739           1126607
131.108.13.44    192.12.33.51           35412           1523980
192.31.7.21      130.93.1.2                11              824
131.108.13.28    192.12.33.2               21             1762
131.108.2.166    192.31.7.130             797           141054
131.108.3.11     192.67.67.53               4              246
192.31.7.21      192.12.33.51           15696           695635
192.31.7.24      192.67.67.20              21              916
131.108.13.111   128.18.10.1               16             1137
accounting threshold exceeded for 7 packets and 433 bytes
```

The following is sample output from the **show ip accounting access-violations** command. The output pertains to packets that failed access lists and were not routed:

```
Router# show ip accounting access-violations

   Source           Destination      Packets        Bytes        ACL
131.108.19.40    192.67.67.20             7          306         77
131.108.13.55    192.67.67.20            67         2749        185
131.108.2.50     192.12.33.51            17         1111        140
131.108.2.50     130.93.2.1               5          319        140
131.108.19.40    130.93.2.1               4          262         77

Accounting data age is 41
```

The following is sample output from the **show ip accounting** command. The output shows the original source and destination addresses that are separated by three routers:

```
Router3# show ip accounting

Source                  Destination             Packets                 Bytes
10.225.231.154          172.16.10.2             44                      28160
10.76.97.34             172.16.10.2             44                      28160
10.10.11.1              172.16.10.2             507                     324480
10.10.10.1              172.16.10.2             507                     318396
10.100.45.1             172.16.10.2             508                     325120
10.98.32.5              172.16.10.2             44                      28160

Accounting data age is 2
```

Table 17 describes the significant fields shown in the displays.

Table 17 show ip accounting Field Descriptions

Field	Description
Source	Source address of the packet.
Destination	Destination address of the packet.
Packets	Number of packets sent from the source address to the destination address. With the **access-violations** keyword, the number of packets sent from the source address to the destination address that violated an Access Control List (ACL).

Table 17 show ip accounting Field Descriptions (continued)

Field	Description
Bytes	Sum of the total number of bytes (IP header and data) of all IP packets sent from the source address to the destination address. With the **access-violations** keyword, the total number of bytes sent from the source address to the destination address that violated an ACL.
ACL	Number of the access list of the last packet sent from the source to the destination that failed an access list filter.
accounting threshold exceeded...	Data for all packets that could not be entered into the accounting table when the accounting table is full. This data is combined into a single entry.

Related Commands

Command	Description
clear ip accounting	Clears the active or checkpointed database when IP accounting is enabled.
ip accounting	Enables IP accounting on an interface.
ip accounting-list	Defines filters to control the hosts for which IP accounting information is kept.
ip accounting-threshold	Sets the maximum number of accounting entries to be created.
ip accounting-transits	Controls the number of transit records that are stored in the IP accounting database.

show ip casa affinities

To display statistics about affinities, use the **show ip casa affinities** EXEC command.

show ip casa affinities [**stats**] | [**saddr** *ip-address* [**detail**]] | [**daddr** *ip-address* [**detail**]] | **sport** *source-port* [**detail**]] | **dport** *destination-port* [**detail**]] | **protocol** *protocol* [**detail**]]

Syntax Description

stats	(Optional) Displays limited statistics.
saddr *ip-address*	(Optional) Displays the source address of a given TCP connection.
detail	(Optional) Displays the detailed statistics.
daddr *ip-address*	(Optional) Displays the destination address of a given TCP connection.
sport *source-port*	(Optional) Displays the source port of a given TCP connection.
dport *destination-port*	(Optional) Displays the destination port of a given TCP connection.
protocol *protocol*	(Optional) Displays the protocol of a given TCP connection.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

The following is sample output of the **show ip casa affinities** command:

```
Router# show ip casa affinities

                        Affinity Table
Source Address  Port  Dest Address    Port  Prot
161.44.36.118   1118  172.26.56.13    19    TCP
172.26.56.13    19    161.44.36.118   1118  TCP
```

The following is sample output of the **show ip casa affinities detail** command:

```
Router# show ip casa affinities detail

                        Affinity Table
Source Address  Port  Dest Address    Port  Prot
161.44.36.118   1118  172.26.56.13    19    TCP
  Action Details:
    Interest Addr:          172.26.56.19      Interest Port: 1638
    Interest Packet: 0x0102 SYN FRAG
    Interest Tickle: 0x0005 FIN RST
    Dispatch (Layer 2):     YES               Dispatch Address: 172.26.56.33

Source Address  Port  Dest Address    Port  Prot
172.26.56.13    19    161.44.36.118   1118  TCP
  Action Details:
    Interest Addr:          172.26.56.19      Interest Port: 1638
    Interest Packet: 0x0104 RST FRAG
    Interest Tickle: 0x0003 FIN SYN
    Dispatch (Layer 2):     NO                Dispatch Address: 0.0.0.0
```

Table 18 describes the significant fields shown in the display.

Table 18 show ip casa affinities Field Descriptions

Field	Description
Source Address	Source address of a given TCP connection.
Port	Source port of a given TCP connection.
Dest Address	Destination address of a given TCP connection.
Port	Destination of a given TCP connection.
Prot	Protocol of a given TCP connection.
Action Details	Actions to be taken on a match.
Interest Addr	Services manager address that is to receive interest packets for this affinity.
Interest Port	Services manager port to which interest packets are sent.
Interest Packet	List of TCP packet types that the services manager is interested in.
Interest Tickle	List of TCP packet types for which the services manager wants the entire packet.
Dispatch (Layer 2)	Layer 2 destination information will be modified.
Dispatch Address	Address of the real server.

Related Commands

Command	Description
forwarding-agent	Specifies the port on which the Forwarding Agent will listen for wildcard and fixed affinities.
show ip casa oper	Displays operational information about the Forwarding Agent.

show ip casa oper

To display operational information about the Forwarding Agent, use the **show ip casa oper** EXEC command.

show ip casa oper

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

The following is sample output of the **show ip casa oper** command:

```
Router# show ip casa oper

Casa is Active
  Casa control address is 206.10.20.34/32
  Casa multicast address is 224.0.1.2
  Listening for wildcards on:
    Port:1637
      Current passwd:NONE Pending passwd:NONE
      Passwd timeout:180 sec (Default)
```

Table 19 describes the significant fields shown in the display.

Table 19 show ip casa oper Field Descriptions

Field	Description
Casa is Active	The Forwarding Agent is active.
Casa control address	Unique address for this Forwarding Agent.
Casa multicast address	Services manager broadcast address.
Listening for wildcards on	Port on which the Forwarding Agent will listen.
Port	Services manager broadcast port.
Current passwd	Current password.
Pending passwd	Password that will override the current password.
Passwd timeout	Interval after which the pending password becomes the current password.

Related Commands

Command	Description
show ip casa oper	Displays operational information about the Forwarding Agent.

show ip casa stats

To display statistical information about the Forwarding Agent, use the **show ip casa stats** EXEC command.

show ip casa stats

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

The following is sample output of the **show ip casa stats** command:

```
Router# show ip casa stats

Casa is active:
  Wildcard Stats:
    Wildcards:       6           Max Wildcards:    6
    Wildcard Denies: 0           Wildcard Drops:   0
    Pkts Throughput: 441         Bytes Throughput: 39120
  Affinity Stats:
    Affinities:      2           Max Affinities:   2
    Cache Hits:      444         Cache Misses:     0
    Affinity Drops:  0
  Casa Stats:
    Int Packet:      4           Int Tickle:       0
    Casa Denies:     0           Drop Count:       0
```

Table 20 describes the significant fields shown in the display.

Table 20 show ip casa stats Field Descriptions

Field	Description
Casa is Active	The Forwarding Agent is active.
Wildcard Stats	Wildcard statistics.
Wildcards	Number of current wildcards.
Max Wildcards	Maximum number of wildcards since the Forwarding Agent became active.
Wildcard Denies	Protocol violations.
Wildcard Drops	Not enough memory to install wildcard.
Pkts Throughput	Number of packets passed through all wildcards.
Bytes Throughput	Number of bytes passed through all wildcards.
Affinity Stats	Affinity statistics.

Table 20 show ip casa stats Field Descriptions (continued)

Field	Description
Affinities	Current number of affinities.
Max Affinities	Maximum number of affinities since the forwarding agent became active.
Cache Hits	Number of packets that match wildcards and fixed affinities.
Cache Misses	Matched wildcard, missed fix.
Affinity Drops	Number of times an affinity could not be created.
Casa Stats	Forwarding agent statistics.
Int Packet	Interest packets.
Int Tickle	Interest tickles.
Casa Denies	Protocol violation.
Security Drops	Packets dropped due to password or authentication mismatch.
Drop Count	Number of messages dropped.

Related Commands

Command	Description
show ip casa oper	Displays operational information about the Forwarding Agent.

show ip casa wildcard

To display information about wildcard blocks, use the **show ip casa wildcard** EXEC command.

show ip casa wildcard [**detail**]

Syntax Description

detail	(Optional) Displays detailed statistics.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

The following is sample output of the **show ip casa wildcard** command:

```
Router# show ip casa wildcard

Source Address  Source Mask     Port  Dest Address    Dest Mask       Port  Prot
0.0.0.0         0.0.0.0         0     172.26.56.2     255.255.255.255 0     ICMP
0.0.0.0         0.0.0.0         0     172.26.56.2     255.255.255.255 0     TCP
0.0.0.0         0.0.0.0         0     172.26.56.13    255.255.255.255 0     ICMP
0.0.0.0         0.0.0.0         0     172.26.56.13    255.255.255.255 0     TCP
172.26.56.2     255.255.255.255 0     0.0.0.0         0.0.0.0         0     TCP
172.26.56.13    255.255.255.255 0     0.0.0.0         0.0.0.0         0     TCP
```

The following is sample output of the **show ip casa wildcard detail** command:

```
router# show ip casa wildcard detail

Source Address  Source Mask     Port  Dest Address    Dest Mask       Port  Prot
0.0.0.0         0.0.0.0         0     172.26.56.2     255.255.255.255 0     ICMP
  Service Manager Details:
    Manager Addr:           172.26.56.19      Insert Time: 08:21:27 UTC 04/18/96
  Affinity Statistics:
    Affinity Count:         0                 Interest Packet Timeouts: 0
  Packet Statistics:
    Packets:                0                 Bytes: 0
  Action Details:
    Interest Addr:          172.26.56.19      Interest Port: 1638
    Interest Packet: 0x8000 ALLPKTS
    Interest Tickle: 0x0107 FIN SYN RST FRAG
    Dispatch (Layer 2):     NO                Dispatch Address: 0.0.0.0
    Advertise Dest Address: YES               Match Fragments:  NO

Source Address  Source Mask     Port  Dest Address    Dest Mask       Port  Prot
0.0.0.0         0.0.0.0         0     172.26.56.2     255.255.255.255 0     TCP
  Service Manager Details:
    Manager Addr:           172.26.56.19      Insert Time: 08:21:27 UTC 04/18/96
  Affinity Statistics:
    Affinity Count:         0                 Interest Packet Timeouts: 0
  Packet Statistics:
    Packets:                0                 Bytes: 0
  Action Details:
```

```
Interest Addr:          172.26.56.19      Interest Port: 1638
Interest Packet: 0x8102 SYN FRAG ALLPKTS
Interest Tickle: 0x0005 FIN RST
Dispatch (Layer 2):     NO                Dispatch Address: 0.0.0.0
Advertise Dest Address: YES               Match Fragments:  NO
```

Note If a filter is not set, the filter is not active.

Table 21 describes significant fields shown in the display.

Table 21 show ip casa wildcard Field Descriptions

Field	Description
Source Address	Source address of a given TCP connection.
Source Mask	Mask to apply to source address before matching.
Port	Source port of a given TCP connection.
Dest Address	Destination address of a given TCP connection.
Dest Mask	Mask to apply to destination address before matching.
Port	Destination port of a given TCP connection.
Prot	Protocol of a given TCP connection.
Service Manager Details	Services manager details.
Manager Addr	Source address of this wildcard.
Insert Time	System time at which this wildcard was inserted.
Affinity Statistics	Affinity statistics.
Affinity Count	Number of affinities created on behalf of this wildcard.
Interest Packet Timeouts	Number of unanswered interest packets.
Packet Statistics	Packet statistics.
Packets	Number of packets that match this wildcard.
Bytes	Number of bytes that match this wildcard.
Action Details	Actions to be taken on a match.
Interest Addr	Services manager that is to receive interest packets for this wildcard.
Interest Port	Services manager port to which interest packets are sent.
Interest Packet	List of packet types that the services manager is interested in.
Interest Tickle	List of packet types for which the services manager wants the entire packet.
Dispatch (Layer 2)	Layer 2 destination information will be modified.
Dispatch Address	Address of the real server.
Advertise Dest Address	Destination address.
Match Fragments	Does wildcard also match fragments? (boolean)

Related Commands

Command	Description
show ip casa oper	Displays operational information about the Forwarding Agent.

show ip drp

To display information about the Director Response Protocol (DRP) Server Agent for DistributedDirector, use the **show ip drp** EXEC command.

show ip drp

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2 F	This command was introduced.

Examples

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

```
Router# show ip drp

Director Responder Protocol Agent is enabled
717 director requests, 712 successful lookups, 5 failures, 0 no route
Authentication is enabled, using "test" key-chain
```

Table 22 describes the significant fields shown in the display.

Table 22 show ip drp Field Descriptions

Field	Description
director requests	Number of DRP requests that have been received (including any using authentication key-chain encryption that failed).
successful lookups	Number of successful DRP lookups that produced responses.
failures	Number of DRP failures (for various reasons including authentication key-chain encryption failures).

Related Commands

Command	Description
ip drp access-group	Controls the sources of DRP queries to the DRP Server Agent.
ip drp authentication key-chain	Configures authentication on the DRP Server Agent for DistributedDirector.

show ip redirects

To display the address of a default gateway (router) and the address of hosts for which an Internet Control Message Protocol (ICMP) redirect message has been received, use the **show ip redirects** EXEC command.

show ip redirects

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command displays the default router (gateway) as configured by the **ip default-gateway** command.

The **ip mtu** command enables the router to send ICMP redirect messages.

Examples

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

```
Router# show ip redirects

Default gateway is 160.89.80.29

Host               Gateway           Last Use    Total Uses  Interface
131.108.1.111      160.89.80.240         0:00             9  Ethernet0
128.95.1.4         160.89.80.240         0:00             4  Ethernet0
Router#
```

Related Commands

Command	Description
ip default-gateway	Defines a default gateway (router) when IP routing is disabled.
ip mtu	Enables the sending of ICMP redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received.

show ip sockets

To display IP socket information, use the **show ip sockets** command in privileged EXEC mode or user EXEC mode.

show ip sockets

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC
User EXEC

Command History

Release	Modification
10.0 T	This command was introduced.

Usage Guidelines

Use this command to verify that the socket being used is opening correctly. If there is a local and remote endpoint, a connection is established with the ports indicated.

Examples

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

```
Router# show ip sockets

Proto    Remote       Port      Local          Port  In Out Stat TTY OutputIF
 17       0.0.0.0        0    171.68.186.193    67   0   0    1   0
 17   171.68.191.135  514    171.68.191.129  1811   0   0    0   0
 17   172.16.135.20   514    171.68.191.1    4125   0   0    0   0
 17   171.68.207.163   49    171.68.186.193    49   0   0    9   0
 17       0.0.0.0      123    171.68.186.193   123   0   0    1   0
 88       0.0.0.0        0    171.68.186.193   202   0   0    0   0
 17   172.16.96.59  32856    171.68.191.1     161   0   0    1   0
 17     --listen--             --any--        496   0   0    1   0
```

Table 23 describes the significant fields shown in the display.

Table 23 show ip sockets Field Descriptions

Field	Description
Proto	Protocol number. For example, 17 is UDP, and 88 is EIGRP.
Remote	Remote address connected to this networking device. If the remote address is considered illegal, “--listen--” is displayed.
Port	Remote port. If the remote address is considered illegal, “--listen--” is displayed.
Local	Local address. If the local address is considered illegal or is the address 0.0.0.0, “--any--” displays.
Port	Local port.
In	Input queue size.
Out	Output queue size.
Stat	Various statistics for a socket.
TTY	The tty number for the creator of this socket.
OutputIF	Output IF string, if one exists.

show ip tcp header-compression

To display statistics about TCP header compression, use the **show ip tcp header-compression** EXEC command.

show ip tcp header-compression

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show ip tcp header-compression** command:

```
Router# show ip tcp header-compression

TCP/IP header compression statistics:
  Interface Serial1: (passive, compressing)
    Rcvd:    4060 total, 2891 compressed, 0 errors
             0 dropped, 1 buffer copies, 0 buffer failures
    Sent:    4284 total, 3224 compressed,
             105295 bytes saved, 661973 bytes sent
             1.15 efficiency improvement factor
    Connect: 16 slots, 1543 long searches, 2 misses, 99% hit ratio
             Five minute miss rate 0 misses/sec, 0 max misses/sec
```

Table 24 describes significant fields shown in the display.

Table 24 show ip tcp header-compression Field Descriptions

Field	Description
Rcvd:	
total	Total number of TCP packets received.
compressed	Total number of TCP packets compressed.
errors	Unknown packets.
dropped	Number of packets dropped due to invalid compression.
buffer copies	Number of packets that needed to be copied into bigger buffers for decompression.
buffer failures	Number of packets dropped due to a lack of buffers.
Sent:	
total	Total number of TCP packets sent.
compressed	Total number of TCP packets compressed.

Table 24 show ip tcp header-compression Field Descriptions (continued)

Field	Description
bytes saved	Number of bytes reduced.
bytes sent	Number of bytes sent.
efficiency improvement factor	Improvement in line efficiency because of TCP header compression.
Connect:	
slots	Size of the cache.
long searches	Indicates the number of times the software needed to look to find a match.
misses	Indicates the number of times a match could not be made. If your output shows a large miss rate, then the number of allowable simultaneous compression connections may be too low.
hit ratio	Percentage of times the software found a match and was able to compress the header.
Five minute miss rate	Calculates the miss rate over the previous 5 minutes for a longer-term (and more accurate) look at miss rate trends.
max misses/sec	Maximum value of the previous field.

Related Commands

Command	Description
ip tcp header-compression	Enables TCP header compression.

show ip traffic

To display statistics about IP traffic, use the **show ip traffic** command in user EXEC or privileged EXEC mode.

show ip traffic

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2	The output was enhanced to displays the number of keepalive, open, update, route-refresh request, and notification messages that have been received and sent by a Border Gateway Protocol (BGP) routing process.

Examples

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

```
Router# show ip traffic

IP statistics:
  Rcvd:  2961 total, 2952 local destination
         0 format errors, 0 checksum errors, 0 bad hop count
         0 unknown protocol, 9 not a gateway
         0 security failures, 0 bad options, 0 with options
  Opts:  0 end, 0 nop, 0 basic security, 0 loose source route
         0 timestamp, 0 extended security, 0 record route
         0 stream ID, 0 strict source route, 0 alert, 0 cipso, 0 ump
         0 other
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 fragments, 0 couldn't fragment
  Bcast: 9 received, 36 sent
  Mcast: 2294 received, 2293 sent
  Sent:  2935 generated, 0 forwarded
  Drop:  1 encapsulation failed, 0 unresolved, 0 no adjacency
         0 no route, 0 unicast RPF, 0 forced drop
         0 options denied
  Drop:  0 packets with source IP address zero
  Drop:  0 packets with internal loop back IP address

ICMP statistics:
  Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 0 unreachable
        0 echo, 0 echo reply, 0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp, 0 info request, 0 other
        0 irdp solicitations, 0 irdp advertisements
  Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
        0 mask requests, 0 mask replies, 0 quench, 0 timestamp
        0 info reply, 0 time exceeded, 0 parameter problem
        0 irdp solicitations, 0 irdp advertisements
```

```
UDP statistics:
  Rcvd: 0 total, 0 checksum errors, 0 no port
  Sent: 36 total, 0 forwarded broadcasts

TCP statistics:
  Rcvd: 654 total, 0 checksum errors, 0 no port
  Sent: 603 total

BGP statistics:
  Rcvd: 288 total, 8 opens, 0 notifications, 0 updates
        280 keepalives, 0 route-refresh, 0 unrecognized
  Sent: 288 total, 8 opens, 0 notifications, 0 updates
        280 keepalives, 0 route-refresh

OSPF statistics:
  Rcvd: 0 total, 0 checksum errors
        0 hello, 0 database desc, 0 link state req
        0 link state updates, 0 link state acks

  Sent: 0 total
        0 hello, 0 database desc, 0 link state req
        0 link state updates, 0 link state acks

IP-EIGRP statistics:
  Rcvd: 2303 total
  Sent: 2301 total

PIMv2 statistics: Sent/Received
  Total: 0/0, 0 checksum errors, 0 format errors
  Registers: 0/0 (0 non-rp, 0 non-sm-group), Register Stops: 0/0,  Hellos: 0/0
  Join/Prunes: 0/0, Asserts: 0/0, grafts: 0/0
  Bootstraps: 0/0, Candidate_RP_Advertisements: 0/0
  Queue drops: 0
  State-Refresh: 0/0

IGMP statistics: Sent/Received
  Total: 0/0, Format errors: 0/0, Checksum errors: 0/0
  Host Queries: 0/0, Host Reports: 0/0, Host Leaves: 0/0
  DVMRP: 0/0, PIM: 0/0
  Queue drops: 0

ARP statistics:
  Rcvd: 2 requests, 5 replies, 0 reverse, 0 other
  Sent: 1 requests, 3 replies (0 proxy), 0 reverse
```

Table 25 describes the significant fields shown in the display.

Table 25 show ip traffic Field Descriptions

Field	Description
IP statistics	Heading for IP statistics fields.
Total	Total number of packets.
Rcvd	Total received, and total destined for this device.
format errors	Indicates a gross error in the packet format, such as an impossible Internet header length.
checksum errors	Indicates that the packet has a bad checksum value in the header.
bad hop count	Occurs when a packet is discarded because its time-to-live (TTL) field was decremented to zero.

Table 25 show ip traffic Field Descriptions (continued)

Field	Description
unknown protocol	Indicates that the packet contains an unknown protocol value or type.
not a gateway	Non-routed packet.
security failures	Packets that with incorrect security values in the IP packet header.
bad options	Packets with incorrect options in the IP packet header.
with options	Packets with options configured in the IP packet header.
Opts	Field for IP packet options.
Frags	Field for packet fragmentation statistics.
Bcast	Field for broadcast packet statistics.
Mcast	Field for multicast packet statistics.
Sent	Field for transmitted packet statistics.
Drop	Field for dropped packet statistics.
encapsulation failed	Usually indicates that the router had no ARP request entry and therefore did not send a datagram.
no route	Counted when the Cisco IOS software discards a datagram it did not know how to route.
ICMP statistics	Heading for ICMP statistics.
UDP statistics	Field for UDP packet statistics.
TCP	Field for TCP packet statistics.
BGP	Field for BGP packet statistics.
OSPF	Field for OSPF packet statistics.
IP-EIGRP	Field for EIGRP packet statistics.
PIMv2	Field for PIM statistics.
IGMP	Field for IGMP statistics.
ARP	Field for ARP statistics.

show standby

To display Hot Standby Router Protocol (HSRP) information, use the **show standby** command in user EXEC or privileged EXEC mode.

show standby [*type number* [*group*]] [**all** | **brief**]

Syntax Description

type number	(Optional) Interface type and number for which output is displayed.
group	(Optional) Group number on the interface for which output is displayed.
all	(Optional) Displays information for groups that are learned or who do not have the **standby ip** command configured.
brief	(Optional) A single line of output summarizes each standby group.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(8)T	The output for the command was made clearer and easier to understand.

Usage Guidelines

To specify a group, you must specify an interface type and number.

Examples

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

```
Router# show standby

Ethernet0/1 - Group 1
  State is Active
    2 state changes, last state change 00:30:59
  Virtual IP address is 10.1.0.20
    Secondary virtual IP address 10.1.0.21
  Active virtual MAC address is 0004.4d82.7981
    Local virtual MAC address is 0004.4d82.7981 (bia)
  Hello time 4 sec, hold time 12 sec
    Next hello sent in 1.412 secs
  Preemption enabled, min delay 50 sec, sync delay 40 sec
  Active router is local
  Standby router is 10.1.0.6, priority 75 (expires in 9.184 sec)
  Priority 95 (configured 120)
    Tracking 2 objects, 0 up
      Down Interface Ethernet0/2, pri 15
      Down Interface Ethernet0/3
  IP redundancy name is "HSRP1", advertisement interval is 34 sec
```

The following is sample output from the **show standby** command with the **brief** keyword specified:

```
Router# show standby brief

Interface   Grp Prio P State    Active addr     Standby addr    Group addr
Et0         0   120    Init     10.0.0.1        unknown         10.0.0.12
```

Table 26 describes the significant fields shown in the displays.

Table 26 show standby Field Descriptions

Field	Description
Ethernet - Group	Interface type and number and Hot Standby group number for the interface.
State is	State of local router; can be one of the following: • Active—Indicates the current Hot Standby router. • Standby—Indicates the router next in line to be the Hot Standby router. • Speak—Router is sending packets to claim the active or standby role. • Listen—Router is neither in the active nor standby state, but if no messages are received from the active or standby router, it will start to speak. • Init or Disabled—Router is not yet ready or able to participate in HSRP, possibly because the associated interface is not up. HSRP groups configured on other routers on the network that are learned via snooping are displayed as being in the Init state. Locally configured groups with an interface that is down or groups without a specified interface IP address appear in the Init state. For these cases, the Active addr and Standby addr fields will show "unknown." The state is listed as disabled in the fields when the **standby ip** command has not been specified.
Virtual IP address is, secondary virtual IP addresses	All secondary virtual IP addresses are listed on separate lines. If one of the virtual IP addresses is a duplicate of an address configured for another device, it will be marked as "duplicate." A duplicate address indicates that the router has failed to defend its ARP (Address Resolution Protocol) cache entry.
Active virtual MAC address	Virtual MAC address being used by the current active router.
Local virtual MAC address	Virtual MAC address that would be used if this router became the active router. The origin of this address (displayed in parentheses) can be "default," "bia," (burned-in address) or "confgd" (configured).
Hello time, hold time	The hello time is the time between hello packets (in seconds) based on the command. The holdtime is the time (in seconds) before other routers declare the active or standby router to be down, based on the **standby timers** command. All routers in an HSRP group use the hello and hold- time values of the current active router. If the locally configured values are different, the variance appears in parentheses after the hello time and hold-time values.
Next hello sent in ...	Time in which the Cisco IOS software will send the next hello packet (in hours:minutes:seconds).
Preemption enabled, sync delay	Indicates whether preemption is enabled. If enabled, the minimum delay is the time a higher-priority nonactive router will wait before preempting the lower-priority active router. The sync delay is the maximum time a group will wait to synchronize with the IP redundancy clients.

Table 26 show standby Field Descriptions (continued)

Field	Description
Active router is	Value can be "local," "unknown," or an IP address. Address (and the expiration date of the address) of the current active Hot Standby router.
Standby router is	Value can be "local," "unknown," or an IP address. Address (and the expiration date of the address) of the "standby" router (the router that is next in line to be the Hot Standby router).
expires in	Time (in hours:minutes:seconds) in which the standby router will no longer be the standby router if the local router receives no hello packets from it.
Tracking	List of interfaces that are being tracked and their corresponding states. Based on the **standby track** command.
IP redundancy name is	The name of the HSRP group.
P	Indicates that the router is configured to preempt.

Related Commands

Command	Description
standby authentication	Configures an authentication string for the HSRP.
standby ip	Activates the HSRP.
standby mac-address	Specifies the virtual MAC address for the virtual router.
standby mac-refresh	Refreshes the MAC cache on the switch by periodically sending packets from the virtual MAC address.
standby preempt	Configures HSRP preemption and preemption delay.
standby priority	Configures Hot Standby priority of potential standby routers.
standby timers	Configures the time between hello messages and the time before other routers declare the active Hot Standby or standby router to be down.
standby track	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces.
standby use-bias	Configures HSRP to use the BIA of the interface as its virtual MAC address, instead of the preassigned MAC address (on Ethernet and FDDI) or the functional address (on Token Ring).

show standby capability

To display the limitation on how many virtual MAC addresses that some interfaces can listen to, use the **show standby capability** command in user EXEC or privileged EXEC mode.

show standby capability [*type number*]

Syntax Description

type number	(Optional) Interface type and number for which output is displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

HSRP allows up to 256 groups to be configured on each interface, but it is possible that the MAC address filter of the interface does not support that many entries. For example, Versatile Interface Processor (VIP) interfaces only support 32 MAC addresses in their MAC address filter. If more HSRP groups are created than there are address filter entries, then it is likely that the router will stop listening to packets sent to the MAC address of an active HSRP group.

Examples

The following is sample output from the **show standby capability** command:

```
Router# show standby capability
7206VXR * indicates hardware may support HSRP
                                                  |
Interface          Type                          H  Potential Max Groups
FastEthernet0/0    18  DEC21140A                 *  256  (0x60194B00,
0x60194BE8)
FastEthernet1/0    18  DEC21140A                 *  256  (0x60194B00,
0x60194BE8)
Ethernet2/0        61  AmdP2                     *  256  (0x601A252C,
0x601A25E4)
Ethernet2/1        61  AmdP2                     *  256  (0x601A252C,
0x601A25E4)
Ethernet2/2        61  AmdP2                     *  256  (0x601A252C,
0x601A25E4)
Ethernet2/3        61  AmdP2                     *  256  (0x601A252C,
0x601A25E4)
Ethernet2/4        61  AmdP2                     *  256  (0x601A252C,
0x601A25E4)
Ethernet2/5        61  AmdP2                     *  256  (0x601A252C,
0x601A25E4)
Ethernet2/6        61  AmdP2                     *  256  (0x601A252C,
0x601A25E4)
Ethernet2/7        61  AmdP2                     *  256  (0x601A252C,
0x601A25E4)
ATM3/0             74  ENHANCED ATM PA           *  256  LAN emulation
TokenRing4/0       66  HAWKEYE                   *  3    HSRP TR functional
```

```
addresses (0x6076A590)
TokenRing4/1       66  HAWKEYE               *  3    HSRP TR functional
addresses (0x6076A590)
TokenRing4/2       66  HAWKEYE               *  3    HSRP TR functional
addresses (0x6076A590)
TokenRing4/3       66  HAWKEYE               *  3    HSRP TR functional
addresses (0x6076A590)
Serial5/0          67  M4T                      -
Serial5/1          67  M4T                      -
Serial5/2          67  M4T                      -
Serial5/3          67  M4T                      -
FastEthernet6/0    18  DEC21140A             *  256  (0x60194B00,
0x60194BE8)
VoIP-Null0         102 VoIP-Null                -
```

Table 27 describes the significant fields in the display.

Table 27 show standby capability Field Descriptions

Field	Description
Interface	Interface type and number for the interface.
Type	Hardware type.
*	Indicates hardware may support HSRP.
Potential Max Groups	An estimate of the number of HSRP groups that a MAC address filter can process for an interface.

show standby delay

To display Hot Standby Router Protocol (HSRP) information about delay periods, use the **show standby delay** command in user EXEC or privileged EXEC mode.

show standby delay [*type number*]

Syntax Description

type number	(Optional) Interface type and number for which output is displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2	This command was introduced.

Examples

The following is sample output from the **show standby delay** command:

```
Router# show standby delay

 Interface          Minimum Reload
 Ethernet0/3        1       5
```

Related Commands

Command	Description
standby delay minimum reload	Delays the initialization of HSRP groups.

show standby internal

To display internal flags and conditions, use the **show standby internal** command in user EXEC or privileged EXEC mode.

show standby internal [*type number*]

Syntax Description

type number	(Optional) Interface type and number for which output is displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2	This command was introduced.

Examples

This example shows a configuration example and the output from the **show standby internal** command for the configuration:

```
interface Ethernet2/0
 ip address 10.0.0.254 255.255.0.0
 standby use-bia
 standby version 2
 standby 1 ip 10.0.0.1
 standby 1 timers 2 6
 standby 1 priority 110
 standby 1 preempt

Router# show standby internal

Global           Confg: 0000
Et2/0 If hw      AmdP2, State 0x210040
Et2/0 If hw      Confg: 0001, USEBIA
Et2/0 If hw      Flags: 0000
Et2/0 If sw      Confg: 0040, VERSION
Et2/0 If sw      Flags: 0001, USEBIA
Et2/0 Grp 1      Confg: 0072, IP_PRI, PRIORITY, PREEMPT, TIMERS
Et2/0 Grp 1      Flags: 0000
```

The above output shows internal flags and hardware and software information for Ethernet interface 2/0. The output shows that HSRP group 1 is configured for priority, preemption, and the **standby timers** and **standby-use bia** commands have been configured.

Related Commands

Command	Description
show standby	Displays HSRP information.

show standby redirect

To display Internet Control Message Protocol (ICMP) redirect information on interfaces configured with the Hot Standby Router Protocol (HSRP), use the **show standby redirect** command in user EXEC or privileged EXEC mode.

show standby redirect [*ip-address* | *interface-type interface-number* [**active** | **passive** | **timers**]]

Syntax Description

ip-address	(Optional) Router IP address.
interface-type interface-number	(Optional) Interface type and number for which output is displayed.
active	(Optional) Active HSRP routers on the subnet.
passive	(Optional) Passive HSRP routers on the subnet.
timers	(Optional) HSRP ICMP redirect timers.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2	This command was introduced.

Examples

The following is sample output from the **show standby redirect** command with no optional keywords:

```
Router# show standby redirect

Interface          Redirects Unknown   Adv      Holddown
Ethernet0/2        enabled   enabled   30       180
Ethernet0/3        enabled   disabled  30       180

Active          Hits   Interface          Group Virtual IP      Virtual MAC
10.19.0.7       0      Ethernet0/2        3     10.19.0.13      0000.0c07.ac03
local           0      Ethernet0/3        1     10.20.0.11      0000.0c07.ac01
local           0      Ethernet0/3        2     10.20.0.12      0000.0c07.ac02

Passive         Hits   Interface          Expires in
10.19.0.6       0      Ethernet0/2        151.800
```

Table 28 describes the significant fields in the display.

Table 28 show standby redirect Field Descriptions

Field	Description
Interface	Interface type and number for the interface.
Redirects	Indicates whether redirects are enabled or disabled on the interface.
Unknown	Indicates whether redirects to an unknown router are enabled or disabled on the interface.
Adv	Number indicating the passive router advertisement interval in seconds.
Holddown	Number indicating the passive router hold interval in seconds.
Active	Active HSRP routers on the subnet.
Hits	Number of address translations required for ICMP information.
Interface	Interface type and number for the interface on the active router.
Group	Hot standby group number.
Virtual IP	Virtual IP address of the active HSRP router.
Virtual MAC	Virtual MAC address of the active HSRP router.
Passive	Passive HSRP routers on the subnet.
Hits	Number of address translations required for ICMP information.
Interface	Interface type and number for the interface on the passive router.
Expires in	Time in seconds for a virtual IP to expire and the holddown time to apply for filtering routes to the standby router.

The following is sample output from the **show standby redirect** command with a specific interface Ethernet 0/3:

```
Router# show standby redirect e0/3

Interface          Redirects Unknown   Adv      Holddown
Ethernet0/3        enabled   disabled  30       180

Active          Hits   Interface          Group Virtual IP      Virtual MAC
local           0      Ethernet0/3        1     10.20.0.11      0000.0c07.ac01
local           0      Ethernet0/3        2     10.20.0.12      0000.0c07.ac02
```

The following is sample output from the **show standby redirect** command showing all active routers on interface Ethernet 0/3:

```
Router# show standby redirect e0/3 active

Active          Hits   Interface          Group Virtual IP      Virtual MAC
local           0      Ethernet0/3        1     10.20.0.11      0000.0c07.ac01
local           0      Ethernet0/3        2     10.20.0.12      0000.0c07.ac02
```

The following is sample output from the **show standby redirect** *ip-address* command, where the IP address is the real IP address of the router:

```
Router# show standby redirect 10.19.0.7

Active          Hits   Interface          Group Virtual IP      Virtual MAC
10.19.0.7       0      Ethernet0/2        3     10.19.0.13      0000.0c07.ac03
```

Related Commands

Command	Description
show standby	Displays the HSRP information.
standby redirect	Enables ICMP redirect messages to be sent when HSRP is configured on an interface.

show tcp statistics

To display TCP statistics, use the **show tcp statistics** EXEC command.

show tcp statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3	This command was introduced.

Examples

The following is sample output from the **show tcp statistics** command:

```
Router# show tcp statistics

Rcvd: 210 Total, 0 no port
      0 checksum error, 0 bad offset, 0 too short
      132 packets (26640 bytes) in sequence
      5 dup packets (502 bytes)
      0 partially dup packets (0 bytes)
      0 out-of-order packets (0 bytes)
      0 packets (0 bytes) with data after window
      0 packets after close
      0 window probe packets, 0 window update packets
      0 dup ack packets, 0 ack packets with unsend data
      69 ack packets (3044 bytes)
Sent: 175 Total, 0 urgent packets
      16 control packets (including 1 retransmitted)
      69 data packets (3029 bytes)
      0 data packets (0 bytes) retransmitted
      73 ack only packets (49 delayed)
      0 window probe packets, 17 window update packets
7 Connections initiated, 1 connections accepted, 8 connections established
8 Connections closed (including 0 dropped, 0 embryonic dropped)
1 Total rxmt timeout, 0 connections dropped in rxmt timeout
0 Keepalive timeout, 0 keepalive probe, 0 Connections dropped in keepalive
```

Table 29 describes the significant fields shown in the display.

Table 29 show tcp statistics Field Descriptions

Field	Description
Rcvd:	Statistics in this section refer to packets received by the router.
Total	Total number of TCP packets received.
no port	Number of packets received with no port.
checksum error	Number of packets received with checksum error.
bad offset	Number of packets received with bad offset to data.

Table 29 show tcp statistics Field Descriptions (continued)

Field	Description
too short	Number of packets received that were too short.
packets in sequence	Number of data packets received in sequence.
dup packets	Number of duplicate packets received.
partially dup packets	Number of packets received with partially duplicated data.
out-of-order packets	Number of packets received out of order.
packets with data after window	Number of packets received with data that exceeded the window size of the receiver.
packets after close	Number of packets received after the connection was closed.
window probe packets	Number of window probe packets received.
window update packets	Number of window update packets received.
dup ack packets	Number of duplicate acknowledgment packets received.
ack packets with unsend data	Number of acknowledgment packets received with unsent data.
ack packets	Number of acknowledgment packets received.
Sent:	Statistics in this section refer to packets sent by the router.
Total	Total number of TCP packets sent.
urgent packets	Number of urgent packets sent.
control packets	Number of control packets (SYN, FIN, or RST) sent.
data packets	Number of data packets sent.
data packets retransmitted	Number of data packets re-sent.
ack only packets	Number of packets sent that are acknowledgments only.
window probe packets	Number of window probe packets sent.
window update packets	Number of window update packets sent.
Connections initiated	Number of connections initiated.
connections accepted	Number of connections accepted.
connections established	Number of connections established.
Connections closed	Number of connections closed.
Total rxmt timeout	Number of times the router tried to resend, but timed out.
connections dropped in rxmit timeout	Number of connections dropped in the resend timeout.
Keepalive timeout	Number of keepalive packets in the timeout.
keepalive probe	Number of keepalive probes.
Connections dropped in keepalive	Number of connections dropped in the keepalive.

Related Commands

Command	Description
clear tcp statistics	Clears TCP statistics.

standby authentication

To configure an authentication string for the Hot Standby Router Protocol (HSRP), use the **standby authentication** interface configuration command. To delete an authentication string, use the **no** form of this command.

standby [*group-number*] **authentication** [**mode text**] *string*

no standby [*group-number*] **authentication** [**mode text**] *string*

Syntax Description

group-number	(Optional) Group number on the interface to which this authentication string applies.
mode text	(Optional) Indicates use of a plain text authentication mode.
string	Authentication string. It can be up to eight characters long. The default string is **cisco**.

Defaults

The default group number is 0. The default string is **cisco**.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1	The **mode** and **text** keywords were added.

Usage Guidelines

HSRP ignores unauthenticated HSRP messages.

The authentication string is sent unencrypted in all HSRP messages. The same authentication string must be configured on all routers and access servers on a cable to ensure interoperation. Authentication mismatch prevents a device from learning the designated Hot Standby IP address and the Hot Standby timer values from other routers configured with HSRP.

When group number 0 is used, no group number is written to NVRAM, providing backward compatibility.

Examples

The following example configures “company1” as the authentication string required to allow Hot Standby routers in group 1 to interoperate:

```
interface ethernet 0
 standby 1 authentication mode text company1
```

standby delay minimum reload

To configure the delay period before the initialization of Hot Standby Router Protocol (HSRP) groups, use the **standby delay minimum reload** interface configuration command. To disable the delay period, use the **no** form of this command.

standby delay minimum *min-delay* **reload** *reload-delay*

no standby delay minimum *min-delay* **reload** *reload-delay*

Syntax Description

min-delay	Minimum time (in seconds) to delay HSRP group initialization after an interface comes up. This minimum delay period applies to all subsequent interface events.
reload-delay	Time (in seconds) to delay after the router has reloaded. This delay period only applies to the first interface-up event after the router has reloaded.

Defaults

The default minimum delay is 1 second.

The default reload delay is 5 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

If the active router fails or is removed from the network, then the standby router will automatically become the new active router. If the former active router comes back online, you can control whether it takes over as the active router by using the **standby preempt** command.

However, in some cases, even if the **standby preempt** command is not configured, the former active router will resume the active role after it reloads and comes back online. Use the **standby delay minimum reload** command to set a delay period for HSRP group initialization. This command allows time for the packets to get through before the router resumes the active role.

We recommend that you use the **standby delay minimum reload** command if the **standby timers** command is configured in milliseconds or if HSRP is configured on a VLAN interface of a switch.

In most configurations, the default values provide sufficient time for the packets to get through and it is not necessary to configure longer delay values.

The delay will be cancelled if an HSRP packet is received on an interface.

You can view the delays with the **show standby delay** command.

Examples

The following example sets the minimum delay period to 30 seconds and the delay period after the first reload to 120 seconds:

```
interface ethernet 0
```

```
ip address 10.20.0.7 255.255.0.0
standby delay minimum 30 reload 120
standby 3 ip 10.20.0.21
standby 3 timers msec 300 msec 700
standby 3 priority 100
```

Related Commands

Command	Description
show standby delay	Displays HSRP information about delay periods.
standby preempt	Configures the HSRP preemption and preemption delay.
standby timers	Configures the time between hello packets and the time before other routers declare the active HSRP or standby router to be down.

standby ip

To activate the Hot Standby Router Protocol (HSRP), use the **standby ip** interface configuration command. To disable HSRP, use the **no** form of this command.

standby [*group-number*] **ip** [*ip-address* [**secondary**]]

no standby [*group-number*] **ip** [*ip-address*]

Syntax Description

group-number	(Optional) Group number on the interface for which HSRP is being activated. The default is 0.
ip-address	(Optional) IP address of the Hot Standby router interface.
secondary	(Optional) Indicates the IP address is a secondary Hot Standby router interface. Useful on interfaces with primary and secondary addresses; you can configure primary and secondary HSRP addresses.

Defaults

The default group number is 0.

HSRP is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The *group-number* argument was added.
11.1	The **secondary** keyword was added.

Usage Guidelines

The **standby ip** command activates HSRP on the configured interface. If an IP address is specified, that address is used as the designated address for the Hot Standby group. If no IP address is specified, the designated address is learned through the standby function. For HSRP to elect a designated router, at least one router on the cable must have been configured with, or have learned, the designated address. Configuring the designated address on the active router always overrides a designated address that is currently in use.

When the **standby ip** command is enabled on an interface, the handling of proxy ARP requests is changed (unless proxy ARP was disabled). If the Hot Standby state of the interface is active, proxy ARP requests are answered using the MAC address of the Hot Standby group. If the interface is in a different state, proxy ARP responses are suppressed.

When group number 0 is used, no group number is written to NVRAM, providing backward compatibility.

Examples

The following example activates HSRP for group 1 on Ethernet interface 0. The IP address used by the Hot Standby group will be learned using HSRP.

```
interface ethernet 0
 standby 1 ip
```

In the following example, all three virtual IP addresses appear in the ARP table using the same (single) virtual MAC address. All three virtual IP addresses are using the same HSRP group (group 0).

```
ip address 1.1.1.1. 255.255.255.0
ip address 1.2.2.2. 255.255.255.0 secondary
ip address 1.3.3.3. 255.255.255.0 secondary
ip address 1.4.4.4. 255.255.255.0 secondary
standby ip 1.1.1.254
standby ip 1.2.2.254 secondary
standby ip 1.3.3.254 secondary
```

standby mac-address

To specify a virtual MAC address for the Hot Standby Router Protocol (HSRP), use the **standby mac-address** interface configuration command. To revert to the standard virtual MAC address (0000.0C07.AC*xy*), use the **no** form of this command.

standby [*group-number*] **mac-address** *mac-address*

no standby [*group-number*] **mac-address**

Syntax Description

group-number	(Optional) Group number on the interface for which HSRP is being activated. The default is 0.
mac-address	MAC address.

Defaults

If this command is not configured, and the **standby use-bia** command is not configured, the standard virtual MAC address is used: 0000.0C07.AC*xy*, where *xy* is the group number in hexadecimal. This address is specified in RFC 2281, *Cisco Hot Standby Router Protocol (HSRP)*.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command cannot be used on a Token Ring interface.

HSRP is used to help end stations locate the first hop gateway for IP routing. The end stations are configured with a default gateway. However, HSRP can provide first-hop redundancy for other protocols. Some protocols, such as Advanced Peer-to-Peer Networking (APPN), use the MAC address to identify the first hop for routing purposes. In this case, it is often necessary to be able to specify the virtual MAC address; the virtual IP address is unimportant for these protocols. Use the **standby mac-address** command to specify the virtual MAC address.

The MAC address specified is used as the virtual MAC address when the router is active.

This command is intended for certain APPN configurations. The parallel terms are shown in Table 30.

Table 30 Parallel Terms Between APPN and IP

APPN	IP
End node	Host
Network node	Router or gateway

In an APPN network, an end node is typically configured with the MAC address of the adjacent network node. Use the **standby mac-address** command in the routers to set the virtual MAC address to the value used in the end nodes.

Examples

If the end nodes are configured to use 4000.1000.1060 as the MAC address of the network node, the following example shows the command used to configure HSRP group 1 with the virtual MAC address:

```
standby 1 mac-address 4000.1000.1060
```

Related Commands

Command	Description
show standby	Displays HSRP information.
standby use-bia	Configures HSRP to use the burned-in address of the interface as its virtual MAC address.

standby mac-refresh

To change the interval at which packets are sent to refresh the MAC cache when the Hot Standby Router Protocol (HSRP) is running over FDDI, use the **standby mac-refresh** interface configuration command. To restore the default value, use the **no** form of this command.

standby mac-refresh *seconds*

no standby mac-refresh

Syntax Description

seconds	Number of seconds in the interval at which a packet is sent to refresh the MAC cache. The maximum value is 255 seconds. The default is 10 seconds.

Defaults

The default interval is 10 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command applies to HSRP running over FDDI only. Packets are sent every 10 seconds to refresh the MAC cache on learning bridges or switches. By default, the MAC cache entries age out in 300 seconds (5 minutes).

All other routers participating in HSRP on the FDDI ring receive the refresh packets, although the packets are intended only for the learning bridge or switch. Use this command to change the interval. Set the interval to 0 if you want to prevent refresh packets (if you have FDDI but do not have a learning bridge or switch).

Examples

The following example changes the MAC refresh interval to 100 seconds. Therefore, a learning bridge would need to miss three packets before the entry ages out.

```
standby mac-refresh 100
```

standby name

To configure the name of the standby group, use the **standby name** interface configuration command. To disable the name, use the **no** form of this command.

standby name *group-name*

no standby name *group-name*

Syntax Description

group-name	Specifies the name of the standby group.

Defaults

The Hot Standby Router Protocol (HSRP) is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(2)T	This command was introduced.

Usage Guidelines

The name specifies the HSRP group used.

Examples

The following example specifies the standby name as SanJoseHA:

```
interface ethernet0
 ip address 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA
 standby preempt delay sync 100
 standby priority 110
```

Related Commands

Command	Description
ip mobile home-agent standby	Configures the Home Agent for redundancy.

standby preempt

To configure Hot Standby Router Protocol (HSRP) preemption and preemption delay, use the **standby preempt** command in interface configuration mode. To restore the default values, use the **no** form of this command.

standby [*group-number*] **preempt** [**delay**{**minimum** *delay* | **reload** *delay* | **sync** *delay*}]

no standby [*group-number*] **preempt** [**delay**{**minimum** *delay* | **reload** *delay* | **sync** *delay*}]

Syntax Description

group-number	(Optional) Group number on the interface to which the other arguments in this command apply.
delay	(Optional) Required if either the **minimum**, **reload**, or **sync** keywords are specified.
minimum *delay*	(Optional) Specifies the minimum delay period in *delay* seconds. The *delay* argument causes the local router to postpone taking over the active role for *delay* (minimum) seconds since that router was last restarted. The range is from 0 to 3600 seconds (1 hour). The default is 0 seconds (no delay).
reload *delay*	(Optional) Specifies the preemption delay period after a reload only. This delay period applies only to the first interface-up event after the router has reloaded.
sync *delay*	(Optional) Specifies the maximum synchronization period for IP redundancy clients in *delay* seconds.

Defaults

The default group number is 0.
The default delay is 0 seconds; if the router wants to preempt, it will do so immediately.
By default, the router that comes up later becomes the standby.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(2)T	The **minimum** and **sync** keywords were added.
12.2	The behavior of the command changed such that **standby preempt** and **standby priority** must be entered as separate commands.
12.2	The **reload** keyword was added.

Usage Guidelines

When this command is configured, the router is configured to preempt, which means that when the local router has a Hot Standby priority higher than the current active router, the local router should attempt to assume control as the active router. If preemption is not configured, the local router assumes control as the active router only if it receives information indicating no router is in the active state (acting as the designated router).

When a router first comes up, it does not have a complete routing table. If it is configured to preempt, it will become the active router, yet it is unable to provide adequate routing services. Solve this problem by configuring a delay before the preempting router actually preempts the currently active router.

When group number 0 is used, no group number is written to NVRAM, providing backward compatibility.

IP redundancy clients can prevent preemption from taking place. The **standby preempt delay sync** *delay* command specifies a maximum number of seconds to allow IP redundancy clients to prevent preemption. When this expires, then preemption takes place regardless of the state of the IP redundancy clients.

The **standby preempt delay reload** *delay* command allows preemption to occur only after a router reloads. This provides stabilization of the router at startup. After this initial delay at startup, the operation returns to the default behavior.

The **no standby preempt delay** command will disable the preemption delay but preemption will remain enabled. The **no standby preempt delay minimum** *delay* command will disable the minimum delay but leave any synchronization delay if it was configured.

Examples

In the following example, the router will wait for 300 seconds (5 minutes) before attempting to become the active router:

```
interface ethernet 0
 standby ip 172.19.108.254
 standby preempt delay minimum 300
```

standby priority

To configure Hot Standby Router Protocol (HSRP) priority, use the **standby priority** command in interface configuration mode. To restore the default values, use the **no** form of this command.

standby [*group-number*] **priority** *priority*

no standby [*group-number*] **priority** *priority*

Syntax Description

group-number	(Optional) Group number on the interface to which the other arguments in this command apply.
priority	Priority value that prioritizes a potential Hot Standby router. The range is from 1 to 255, where 1 denotes the lowest priority and 255 denotes the highest priority. The default priority value is 100. The router in the HSRP group with the highest priority value becomes the active router.

Defaults

The default group number is 0.

The default priority is 100.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(2)T	The **minimum** and **sync** keywords were added.
12.2	The behavior of the command changed such that **standby preempt** and **standby priority** must be entered as separate commands.

Usage Guidelines

When group number 0 is used, no group number is written to NVRAM, providing backward compatibility.

The assigned priority is used to help select the active and standby routers. Assuming preemption is enabled, the router with the highest priority becomes the designated active router. In case of ties, the primary IP addresses are compared, and the higher IP address has priority.

Note that the priority of the device can change dynamically if an interface is configured with the **standby track** command and another interface on the router goes down.

Examples

In the following example, the router has a priority of 120 (higher than the default value):

```
interface ethernet 0
 standby ip 172.19.108.254
 standby priority 120
 standby preempt delay 300
```

Related Commands

Command	Description
standby track	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces.

standby redirect

To enable Hot Standby Router Protocol (HSRP) filtering of Internet Control Message Protocol (ICMP) redirect messages, use the **standby redirects** command in interface configuration mode. To disable the HSRP filtering of ICMP redirect messages, use the **no** form of this command.

standby redirect [**enable** | **disable**] [**timers** *advertisement holddown*] [**unknown**]

no standby redirects [**unknown**]

Syntax Description

enable	(Optional) Allows the filtering of ICMP redirect messages on interfaces configured with HSRP, where the next hop IP address may be changed to an HSRP virtual IP address.
disable	(Optional) Disables the filtering of ICMP redirect messages on interfaces configured with HSRP.
timers	(Optional) Adjusts HSRP router advertisement timers.
advertisement	(Optional) HSRP Router advertisement interval in seconds. This is an integer from 10 to 180. The default is 60 seconds.
holddown	(Optional) HSRP router holddown interval in seconds. This is an integer from 61 to 3600. The default is 180 seconds.
unknown	(Optional) Allows sending of ICMP packets when the next hop IP address contained in the packet is unknown in the HSRP table of real IP addresses and active virtual IP addresses. The **no standby redirect unknown** command stops the redirects from being sent.

Defaults

HSRP filtering of ICMP redirect messages is enabled if HSRP is configured on an interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2	The following keywords and arguments were added to the command: • **timers** *advertisement holdtime* • **unknown**

Usage Guidelines

The **standby redirect** command can be configured globally or on a per-interface basis. When HSRP is first configured on an interface, the setting for that interface will inherit the global value. If the filtering of ICMP redirects is explicitly disabled on an interface, then the global command cannot reenable this functionality.

The **no standby redirect** command is the same as the **standby redirect disable** command. However, it is not desirable to save the **no** form of this command to NVRAM. Because the command is enabled by default, it is preferable to use the **standby redirect disable** command to disable the functionality.

With the **standby redirect** command enabled, the real IP address of a router can be replaced with a virtual IP address in the next hop address or gateway field of the redirect packet. HSRP looks up the next hop IP address in its table of real IP addresses versus virtual IP addresses. If HSRP does not find a match, the HSRP router allows the redirect packet to go out unchanged. The host HSRP router is redirected to a router that is unknown, that is, a router with no active HSRP groups. You can specify the **no standby redirect unknown** command to stop these redirects from being sent.

Examples

The following example allows HSRP to filter ICMP redirect messages on interface Ethernet 0:

```
Router(config)# interface ethernet 0
Router(config-if)# ip address 10.0.0.1 255.0.0.0
Router(config-if)# standby redirect
Router(config-if)# standby 1 ip 10.0.0.11
```

The following example shows how to change the HSRP router advertisement interval to 90 seconds and the holddown timer to 270 seconds on interface Ethernet 0:

```
Router(config)# interface ethernet 0
Router(config-if)# ip address 10.0.0.1 255.0.0.0
Router(config-if)# standby redirect timers 90 270
Router(config-if)# standby 1 ip 10.0.0.11
```

Related Commands

Command	Description
show standby	Displays the HSRP information.
show standby redirect	Displays ICMP redirect information on interfaces configured with the HSRP.

standby timers

To configure the time between hello packets and the time before other routers declare the active Hot Standby or standby router to be down, use the **standby timers** interface configuration command. To restore the timers to their default values, use the **no** form of this command.

standby [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime*

no standby [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime*

Syntax Description

group-number	(Optional) Group number on the interface to which the timers apply. The default is 0.
msec	(Optional) Interval in milliseconds. Millisecond timers allow for faster failover.
hellotime	Hello interval (in seconds). This is an integer from 1 to 254. The default is 3 seconds. If the **msec** option is specified, hello interval is in milliseconds. This is an integer from 15 to 999.
holdtime	Time (in seconds) before the active or standby router is declared to be down. This is an integer from *y* to 255. The default is 10 seconds. If the **msec** option is specified, holdtime is in milliseconds. This is an integer from *x* to 3000. Where: • *y* is the hellotime + 50 milliseconds, then rounded up to the nearest 1 second • *x* is greater than or equal to 3 times the hellotime and is not less than 50 milliseconds.

Defaults

The default group number is 0.

The default hello interval is 3 seconds.

The default hold time is 10 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The **msec** keyword was added.
12.2	The minimum values of hellotime and holdtime in milliseconds changed.

Usage Guidelines

The **standby timers** command configures the time between standby hello packets and the time before other routers declare the active or standby router to be down. Routers or access servers on which timer values are not configured can learn timer values from the active or standby router. The timers configured on the active router always override any other timer settings. All routers in a Hot Standby group should

use the same timer values. Normally, holdtime is greater than or equal to three times the value of hellotime. The range of values for holdtime force the holdtime to be greater than the hellotime. If the timer values are specified in milliseconds, the holdtime is required to be at least three times the hellotime value and not less than 50 milliseconds.

Some HSRP state flapping can occasionally occur if the holdtime is set to less than 250 milliseconds, and the processor is busy. It is recommended that a holdtime value less than 250 millisecond only be used on 7200 platforms or better, and on fast-ethernet or FDDI interfaces or better. Setting the **process-max-time** command to a suitable value may also help with flapping.

The value of the standby timer will not be learned through HSRP hellos if it is less than 1 second.

When group number 0 is used, no group number is written to NVRAM, providing backward compatibility.

Examples

The following example sets, for group number 1 on Ethernet interface 0, the time between hello packets to 5 seconds, and the time after which a router is considered to be down to 15 seconds:

```
interface ethernet 0
 standby 1 ip
 standby 1 timers 5 15
```

The following example sets, for the Hot Router interface located at 172.19.10.1 on Ethernet interface 0, the time between hello packets to 300 milliseconds, and the time after which a router is considered to be down to 900 milliseconds.

```
interface ethernet 0
 standby ip 172.19.10.1
 standby timers msec 300 msec 900
```

The following example sets, for the Hot Router interface located at 172.18.10.1 on Ethernet interface 0, the time between hello packets to 15 milliseconds, and the time after which a router is considered to be down to 50 milliseconds. Note that the holdtime is larger than three times the hellotime because the minimum holdtime value in milliseconds is 50.

```
interface ethernet 0
 standby ip 172.18.10.1
 standby timers msec 15 msec 50
```

standby track

To configure an interface so that the Hot Standby priority changes based on the availability of other interfaces, use the **standby track** interface configuration command. To remove the tracking, use the **no** form of this command.

standby [*group-number*] **track** *interface-type interface-number* [*interface-priority*]

no standby [*group-number*] **track** *interface-type interface-number* [*interface-priority*]

Syntax Description

group-number	(Optional) Group number on the interface to which the tracking applies.
interface-type	Interface type (combined with interface number) that will be tracked.
interface-number	Interface number (combined with interface type) that will be tracked.
interface-priority	(Optional) Amount by which the Hot Standby priority for the router is decremented (or incremented) when the interface goes down (or comes back up). The default value is 10.

Defaults

The default group number is 0.

The default interface priority is 10.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This command ties the Hot Standby priority of the router to the availability of its interfaces. It is useful for tracking interfaces that are not configured for the Hot Standby Router Protocol (HSRP).

When a tracked interface goes down, the Hot Standby priority decreases by 10. If an interface is not tracked, its state changes do not affect the Hot Standby priority. For each interface configured for Hot Standby, you can configure a separate list of interfaces to be tracked.

The optional *interface-priority* argument specifies by how much to decrement the Hot Standby priority when a tracked interface goes down. When the tracked interface comes back up, the priority is incremented by the same amount.

When multiple tracked interfaces are down, the decrements are cumulative whether configured with *interface-priority* values or not.

A tracked interface is considered down if the IP address is disabled on that interface.

If HSRP is configured to track an interface, and that interface is physically removed as in the case of an online insertion and removal (OIR) operation, then HSRP will regard the interface as always down. Further, it will not be possible to remove the HSRP interface tracking configuration. To prevent this problem, use the **no standby track** i*nterface-type interface-number* command before you physically remove the interface.

Use the **no standby** *group-number* **track** command to delete all tracking configuration for a group.

When group number 0 is used, no group number is written to NVRAM, providing backward compatibility.

Examples

In the following example, Ethernet interface 1 tracks Ethernet interface 0 and serial interface 0. If one or both of these two interfaces go down, the Hot Standby priority of the router decreases by 10. Because the default Hot Standby priority is 100, the priority becomes 90 when one or both of the tracked interfaces go down.

```
interface ethernet 1
 ip address 198.92.72.37 255.255.255.240
 no ip redirects
 standby track ethernet 0
 standby track serial 0
 standby preempt
 standby ip 198.92.72.46
```

Related Commands

Command	Description
show standby	Displays HSRP information.
standby preempt	Configures HSRP preemption and preemption delay.
standby priority	Configures Hot Standby priority of potential standby routers.

standby use-bia

To configure the Hot Standby Router Protocol (HSRP) to use the burned-in address of the interface as its virtual MAC address, instead of the preassigned MAC address (on Ethernet and FDDI) or the functional address (on Token Ring), use the **standby use-bia** interface configuration command. To restore the default virtual MAC address, use the **no** form of this command.

standby use-bia [**scope interface**]

no standby use-bia

Syntax Description

scope interface	(Optional) Specifies that this command is configured just for the subinterface on which it was entered, instead of the major interface.

Defaults

HSRP uses the preassigned MAC address on Ethernet and FDDI, or the functional address on Token Ring.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.1	The behavior was modified to allow multiple standby groups to be configured for an interface configured with this command

Usage Guidelines

For an interface with this command configured, multiple standby group can be configured. Hosts on the interface must have a default gateway configured. We recommend that you set the **no ip proxy-arp** command on the interface. It is desirable to configure the **standby use-bia** command on a Token Ring interface if there are devices that reject ARP replies with source hardware addresses set to a functional address.

When HSRP runs on a multiple-ring, source-routed bridging environment and the HRSP routers reside on different rings, configuring the **standby use-bia** command can prevent confusion about the routing information field (RFI).

Without the **scope interface** keywords, the **standby use-bia** command applies to all subinterfaces on the major interface. The **standby use-bia** command may not be configured both with and without the **scope interface** keywords at the same time.

Examples

In the following example, the burned-in address of Token Ring interface 4/0 will be the virtual MAC address mapped to the virtual IP address:

```
interface token4/0
 standby use-bia
```

start-forwarding-agent

To start the Forwarding Agent, use the **start-forwarding-agent** CASA-port configuration command.

start-forwarding-agent *port-number* [*password* [*timeout*]]

Syntax Description

port-number	Port numbers on which the Forwarding Agent will listen for wildcards broadcast from the services manager. This must match the port number defined on the services manager.
password	(Optional) Text password used for generating the MD5 digest.
timeout	(Optional) Duration (in seconds) during which the Forwarding Agent will accept the new and old password. Valid range is from 0 to 3600 seconds. The default is 180 seconds.

Defaults

The default initial number of affinities is 5000.

The default maximum number of affinities is 30,000.

Command Modes

CASA-port configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

The Forwarding Agent must be started before you can configure any port information for the forwarding agent.

Examples

The following example specifies that the forwarding agent will listen for wildcard and fixed affinities on port 1637:

```
start-forwarding-agent 1637
```

Related Commands

Command	Description
forwarding-agent	Specifies the port on which the Forwarding Agent will listen for wildcard and fixed affinities.

transmit-interface

To assign a transmit interface to a receive-only interface, use the **transmit-interface** interface configuration command. To return to normal duplex Ethernet interfaces, use the **no** form of this command.

transmit-interface *type number*

no transmit-interface

Syntax Description

type	Transmit interface type to be linked with the (current) receive-only interface.
number	Transmit interface number to be linked with the (current) receive-only interface.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

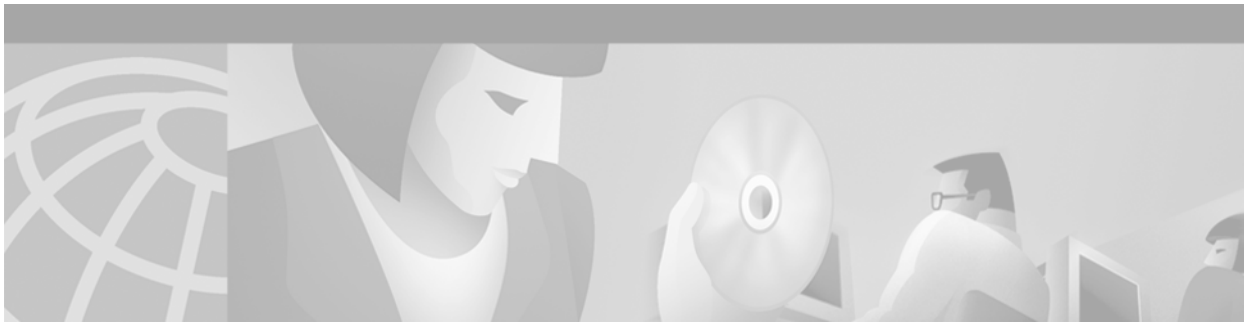
Usage Guidelines

Receive-only interfaces are used commonly with microwave Ethernet links.

Examples

The following example specifies Ethernet interface 0 as a simplex Ethernet interface:

```
interface ethernet 1
 ip address 128.9.1.2
 transmit-interface ethernet 0
```



Server Load Balancing Commands

Use the commands in this chapter to configure the IOS Server Load Balancing (SLB) feature. For configuration information and examples, refer to the "Configuring Server Load Balancing" chapter of the *Cisco IOS IP Configuration Guide*.

advertise

To control the installation of a static route to the Null0 interface for a virtual server address, use the **advertise** SLB virtual server configuration command. To prevent the installation of a static route for the virtual server IP address, use the **no** form of this command.

advertise

no advertise

Syntax Description

This command has no arguments or keywords.

Defaults

The SLB virtual server IP address is added to the routing table.

Command Modes

SLB virtual server configuration

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.

Usage Guidelines

By default, virtual server addresses are *advertised*. That is, static routes to the Null0 interface are installed for the virtual server addresses.

Advertisement of this static route using the routing protocol requires that you configure redistribution of static routes for the routing protocol.

Examples

The following example prevents advertisement of the IP address of the virtual server in routing protocol updates:

```
ip slb vserver PUBLIC_HTTP
no advertise
```

Related Commands

Command	Description
show ip slb vservers	Displays information about the virtual servers.

agent

To configure a Dynamic Feedback Protocol (DFP) agent, use the **agent** SLB DFP configuration command. To remove an agent definition from the DFP configuration, use the **no** form of this command.

agent *ip-address port* [*timeout* [*retry-count* [*retry-interval*]]]

no agent *ip-address port*

Syntax Description

ip-address	Agent IP address.
port	Agent port number.
timeout	(Optional) Time period (in seconds) during which the DFP manager must receive an update from the DFP agent. The default is 0 seconds, which means there is no timeout.
retry-count	(Optional) Number of times the DFP manager attempts to establish the TCP connection to the DFP agent. The default is 0 retries, which means there are infinite retries.
retry-interval	(Optional) Interval (in seconds) between retries. The default is 180 seconds.

Defaults

The default timeout is 0 seconds (no timeout).

The default retry count is 0 (infinite retries).

The default retry interval is 180 seconds.

Command Modes

SLB DFP configuration

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.

Usage Guidelines

You can configure up to 1024 agents.

A DFP agent collects status information about the load capability of a server and reports that information to a load manager. The DFP agent may reside on the server, or it may be a separate device that collects and consolidates the information from several servers before reporting to the load manager.

Examples

The following example configures a DFP agent on the DFP manager, sets the DFP password to Cookies and the timeout to 360 seconds, changes the configuration mode to DFP configuration mode, sets the IP address of the DFP agent to 10.1.1.1, and sets the port number of the DFP agent to 2221 (FTP):

```
ip slb dfp password Cookies 360
agent 10.1.1.1 2221
```

Related Commands

Command	Description
ip slb dfp	Configures the IOS SLB DFP.

bindid

To configure a bind ID, use the **bindid** SLB server farm configuration command. To remove a bind ID from the server farm configuration, use the **no** form of this command.

bindid [*bind-id*]

no bindid [*bind-id*]

Syntax Description

bind-id	(Optional) Bind ID number. The default bind ID is 0.

Defaults

The default bind ID is 0.

Command Modes

SLB server farm configuration

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.

Usage Guidelines

You can configure one bind ID on each **bindid** command.

The bind ID allows a single physical server to be bound to multiple virtual servers and report a different weight for each one. Thus, the single real server is represented as multiple instances of itself, each having a different bind ID. DFP uses the bind ID to identify for which instance of the real server a given weight is specified.

Examples

The following example configures bind ID 309:

```
ip slb serverfarm PUBLIC
bindid 309
```

Related Commands

Command	Description
ip slb dfp	Configures the IOS SLB DFP.

clear ip slb

To clear IP IOS SLB connections or counters, use the **clear ip slb** privileged EXEC command.

clear ip slb {**connections** [**serverfarm** *farm-name* | **vserver** *server-name*] | **counters**}

Syntax Description

connections	Clears the IP IOS SLB connection database.
serverfarm	(Optional) Clears the connection database for the server farm named.
farm-name	(Optional) Character string used to identify the server farm.
vserver	(Optional) Clears the connection database for the virtual server named.
server-name	(Optional) Character string used to identify the virtual server.
counters	Clears the IP IOS SLB counters.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)E	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Examples

The following example clears the connection database of the server farm named FARM1:

```
Router# clear ip slb connections serverfarm FARM1
```

The following example clears the connection database of the virtual server named VSERVER1:

```
Router# clear ip slb connections vserver VSERVER1
```

The following example clears the IOS SLB counters:

```
Router# clear ip slb counters
```

Related Commands

Command	Description
show ip slb conns	Displays information about the IOS SLB connections.
show ip slb serverfarms	Displays information about the IOS SLB server farms.
show ip slb vservers	Displays information about the IOS SLB virtual servers.

client

To define which clients are allowed to use the virtual server, use the **client** SLB virtual server configuration command. You can use more than one client command to define more than one client. To remove a client definition from the IOS SLB configuration, use the **no** form of this command.

client *ip-address network-mask*

no client *ip-address network-mask*

Syntax Description

ip-address	Client IP address. The default is 0.0.0.0 (all clients).
network-mask	Client IP network mask. The default is 0.0.0.0 (all subnetworks).

Defaults

The default IP address is 0.0.0.0 (all clients).

The default network mask is 0.0.0.0 (all subnetworks).

Taken together, the default is **client 0.0.0.0 0.0.0.0** (allows all clients on all subnetworks to use the virtual server).

Command Modes

SLB virtual server configuration

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.

Usage Guidelines

The *network-mask* value is applied to the source IP address of incoming connections. The result must match the *ip-address* value for the client to be allowed to use the virtual server.

Examples

The following example allows only clients from 10.4.4.x access to the virtual server:

```
ip slb vserver PUBLIC_HTTP
 client 10.4.4.0 255.255.255.0
```

Related Commands

Command	Description
show ip slb vservers	Displays information about the virtual servers.
virtual	Configures the virtual server attributes.

delay (virtual server)

To change the amount of time the IOS SLB feature maintains TCP connection context after a connection has terminated, use the **delay** SLB virtual server configuration command. To restore the default delay timer, use the **no** form of this command.

delay *duration*

no delay

Syntax Description

duration	Delay timer duration in seconds. The valid range is from 1 to 600 seconds. The default value is 10 seconds.

Defaults

The default duration is 10 seconds.

Command Modes

SLB virtual server configuration

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.

Usage Guidelines

The delay timer allows out-of-sequence packets and final acknowledgments (ACKs) to be delivered after a TCP connection ends.

Do not set this value to zero (0).

If you are configuring a delay timer for HTTP flows, choose a low number such as 5 seconds as a starting point.

Examples

The following example specifies that the IOS SLB feature maintains TCP connection context for 30 seconds after a connection has terminated:

```
ip slb vserver PUBLIC_HTTP
 delay 30
```

Related Commands

Command	Description
show ip slb vservers	Displays information about the virtual servers.
virtual	Configures the virtual server attributes.

faildetect

To specify the conditions that indicate a server failure, use the **faildetect** SLB real server configuration command. To restore the default values that indicate a server failure, use the **no** form of this command.

faildetect numconns *number-conns* [**numclients** *number-clients*]

no faildetect

Syntax Description

numconns	Number of consecutive TCP connection reassignments allowed before a real server is considered to have failed.
number-conns	Connection reassignment threshold value in the range from 1 to 255. The default is 8 connection failures.
numclients	(Optional) Number of unique client connection failures allowed before a real server is considered to have failed.
number-clients	(Optional) Client connection reassignment threshold value in the range from 1 to 8. The default is 2 client connection failures.

Defaults

If you do not specify the **faildetect** command, the default value of the connection reassignment threshold is 8.

If you do not specify the **numclients** keyword, the default value of the unique client failure threshold is 2.

Command Modes

SLB real server configuration

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.

Examples

In the following example the connection reassignment threshold is set to 16 and, because the **numclients** keyword is not configured, the threshold for unique client connection failure is set to the default value 8. The real server is considered to have failed when 8 unique clients have had connection failures and there have been 16 connection reassignments.

```
ip slb serverfarm PUBLIC
 real 10.10.1.1
 faildetect numconns 16
```

Related Commands

Command	Description
real	Identifies a real server.
show ip slb reals	Displays information about the real servers.
show ip slb serverfarms	Displays information about the server farm configuration.

idle

To specify the minimum amount of time for which IOS SLB maintains connection information in the absence of packet activity, use the **idle** virtual server configuration command. To restore the default idle duration value, use the **no** form of this command.

idle *duration*

no idle

Syntax Description

duration	Idle connection timer duration (in seconds). Valid values range from 10 to 65535. The default is 3600 seconds (1 hour).

Defaults

The default duration is 3600 seconds.

Command Modes

SLB virtual server configuration

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.

Usage Guidelines

TCP connections that do not send flows or keepalives before the idle timer expires are assumed to be inactive and are reset (RST).

If you are configuring an idle timer for HTTP flows, choose a low number such as 120 seconds as a starting point. A low number ensures that the IOS SLB connection database maintains a manageable size if problems at the server, client, or network result in a large number of connections. However, do not choose a value under 60 seconds; such a low value can reduce the efficiency of the IOS SLB feature.

Examples

The following example instructs the IOS SLB feature to maintain connection information for an idle connection for 120 seconds:

```
ip slb vserver PUBLIC_HTTP
 idle 120
```

Related Commands

Command	Description
show ip slb vservers	Displays information about the virtual servers.
virtual	Configures the virtual server attributes.

inservice (real server)

To enable the real server for use by the IOS SLB feature, use the **inservice** SLB real server configuration command. To remove the real server from service, use the **no** form of this command.

inservice

no inservice

Syntax Description

This command has no arguments or keywords.

Defaults

If you do not specify the **inservice** command, the real server is defined to IOS SLB but is not used.

Command Modes

SLB real server configuration

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.

Examples

The following example enables the real server for use by the IOS SLB feature:

```
ip slb serverfarm PUBLIC
 real 10.10.1.1
 inservice
```

Related Commands

Command	Description
real	Identifies a real server.
show ip slb reals	Displays information about the real servers.
show ip slb serverfarms	Displays information about the server farm configuration.

inservice (virtual server)

To enable the virtual server for use by the IOS SLB feature, use the **inservice** SLB virtual server configuration command. To remove the virtual server from service, use the **no** form of this command.

inservice [**standby** *group-name*]

no inservice [**standby** *group-name*]

Syntax Description

standby	(Optional) Configures the Hot Standby Router Protocol (HSRP) standby virtual server.
group-name	(Optional) Specifies the HSRP group name with which the IOS SLB virtual server is associated.

Defaults

If you do not specify the **inservice** command, the virtual server is defined to IOS SLB but is not used.

Command Modes

SLB virtual server configuration

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(1)E	The **standby** keyword and *group-name* argument were added.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Examples

The following example enables the real server for use by the IOS SLB feature:

```
ip slb vserver PUBLIC_HTTP
 inservice
```

Related Commands

Command	Description
show ip slb vservers	Displays information about the virtual servers.
virtual	Configures the virtual server attributes.

ip slb dfp

To configure the Dynamic Feedback Protocol (DFP) and supply an optional password, use the **ip slb dfp** global configuration command. To remove the DFP configuration, use the **no** form of this command.

ip slb dfp [**password** *password* [*timeout*]]

no ip slb dfp

Syntax Description

password	(Optional) Specifies a password for MD5 authentication.
password	(Optional) Password value for MD5 authentication. This password must match the password configured on the host agent.
timeout	(Optional) Delay period (in seconds) during which both the old password and the new password are accepted. The default value is 180 seconds.

Defaults

The password timeout default is 180 seconds.

Command Modes

Global configuration

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.

Usage Guidelines

The optional password, if configured, must match the password configured on the host agent.

The *timeout* option allows you to change the password without stopping messages between the DFP agent and its manager. The default value is 180 seconds.

During the timeout, the agent sends packets with the old password (or null, if there is no old password), and receives packets with either the old or new password. After the timeout expires, the agent sends and receives packets only with the new password; received packets that use the old password are discarded.

If you are changing the password for an entire load-balanced environment, set a longer timeout. This setting allows enough time for you to update the password on all agents and servers before the timeout expires. It also prevents mismatches between agents and servers that have begun running the new password and agents, and servers on which you have not yet changed the old password.

Examples

The following example configures DFP, sets the password to flounder, configures a timeout period of 60 seconds, and changes to DFP configuration mode:

```
ip slb dfp flounder 60
```

Related Commands

Command	Description
agent	Configures a DFP agent.

ip slb serverfarm

To identify a server farm and enter SLB server farm configuration mode, use the **ip slb serverfarm** global configuration command. To remove the server farm from the IOS SLB configuration, use the **no** form of this command.

ip slb serverfarm *serverfarm-name*

no ip slb serverfarm *serverfarm-name*

Syntax Description

serverfarm-name	Character string used to identify the server farm. The character string is limited to 15 characters.

Defaults

No default behavior or values.

Command Modes

Global configuration

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.

Examples

The following example identifies a server farm named PUBLIC:

```
ip slb serverfarm PUBLIC
```

Related Commands

Command	Description
real	Identifies a real server.

ip slb vserver

To identify a virtual server and enter SLB virtual server configuration mode, use the **ip slb vserver** global configuration command. To remove a virtual server from the IOS SLB configuration, use the **no** form of this command.

ip slb vserver *virtserver-name*

no ip slb vserver *virtserver-name*

Syntax Description

virtserver-name	Character string used to identify the virtual server. The character string is limited to 15 characters.

Defaults

No default behavior or values.

Command Modes

Global configuration

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.

Examples

The following example identifies a virtual server named PUBLIC_HTTP:

```
ip slb vserver PUBLIC_HTTP
```

Related Commands

Command	Description
serverfarm	Associates a real server farm with a virtual server.
show ip slb vservers	Displays information about the virtual servers.

maxconns

To limit the number of active connections to the real server, use the **maxconns** SLB real server configuration command. To restore the default of no limit, use the **no** form of this command.

maxconns *maximum-number*

no maxconns

Syntax Description

maximum-number	Maximum number of simultaneous active connections on the real server. Valid values range from 1 to 4294967295. The default is 4294967295.

Defaults

The default maximum number is 4294967295.

Command Modes

SLB real server configuration

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.

Examples

The following example limits the real server to a maximum of 1000 simultaneous active connections:

```
ip slb serverfarm PUBLIC
real 10.10.1.1
maxconns 1000
```

Related Commands

Command	Description
real	Identifies a real server.
show ip slb reals	Displays information about the real servers.
show ip slb serverfarms	Displays information about the server farm configuration.

nat

To configure IOS SLB Network Address Translation (NAT) and specify a NAT mode, use the **nat** SLB server farm configuration command. To remove a NAT configuration, use the **no** form of this command.

nat server

no nat server

Syntax Description

server	Specifies that the destination address in load-balanced packets sent to the real server is the address of the real server chosen by the server farm load-balancing algorithm.

Defaults

No default behavior or values.

Command Modes

SLB server farm configuration

Command History

Release	Modification
12.1(1)E	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

The **no nat** command is allowed only if the virtual server was removed from service with the **no inservice** command.

Examples

The following example changes to IOS SLB server farm configuration mode and configures NAT mode as server address translation on the server farm named FARM2:

```
ip slb serverfarm FARM2
 nat server
```

Related Commands

Command	Description
ip slb serverfarm	Associates a real server farm with a virtual server.
real	Identifies a real server as a member of a server farm.
show ip slb serverfarms	Displays information about the server farm configuration.

predictor

To specify the load-balancing algorithm for selecting a real server in the server farm, use the **predictor** SLB server farm configuration command. To restore the default load-balancing algorithm of weighted round robin, use the **no** form of this command.

predictor [**roundrobin** | **leastconns**]

no predictor

Syntax Description

roundrobin	(Optional) Use the weighted round robin algorithm for selecting the real server to handle the next new connection for the server farm.
leastconns	(Optional) Use the weighted least connections algorithm for selecting the real server to handle the next new connection for this server farm.

Defaults

The default predictor is weighted round robin.

Command Modes

SLB server farm configuration

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.

Examples

The following example specifies the weighted least connections algorithm:

```
ip slb serverfarm PUBLIC
 predictor leastconns
```

Related Commands

Command	Description
show ip slb serverfarms	Displays information about the server farm configuration.
weight	Specifies the capacity of the real server, relative to other real servers in the server farm.

real

To identify a real server as a member of a server farm, use the **real** SLB server farm configuration command. To remove the real server from the IOS SLB configuration, use the **no** form of this command.

real *ip-address*

no real *ip-address*

Syntax Description

ip-address	Real server IP address.

Defaults

No default behavior or values.

Command Modes

SLB server farm configuration

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.

Examples

The following example identifies a real server as a member of the server farm:

```
ip slb serverfarm PUBLIC
 real 10.1.1.1
```

Related Commands

Command	Description
inservice (real server)	Enables the real server for use by IOS SLB.
show ip slb serverfarms	Displays information about the server farm configuration.
show ip slb reals	Displays information about the real servers.

reassign

To specify the threshold of consecutive unanswered synchronizations that, if exceeded, results in an attempted connection to a different real server, use the **reassign** SLB real server configuration command. To restore the default reassignment threshold, use the **no** form of this command.

reassign *threshold*

no reassign

Syntax Description

threshold	Number of unanswered TCP SYNs that are directed to a real server before the connection is reassigned to a different real server. An unanswered SYN is one for which no SYN or ACK is detected before the next SYN arrives from the client. IOS SLB allows 30 seconds for the connection to be established or for a new SYN to be received. If neither of these events occurs within that time, the connection is removed from the IOS SLB database. The 30-second timer is restarted for each SYN as long as the number of connection reassignments specified on the **faildetect** command's **numconns** keyword is not exceeded. See the **faildetect** command for more information. Valid threshold values range from 1 to 4 SYNs. The default value is 3.

Defaults

The default threshold is three SYNs.

Command Modes

SLB real server configuration

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.

Examples

The following example sets the threshold of unanswered SYNs to 2:

```
ip slb serverfarm PUBLIC
 real 10.10.1.1
 reassign 2
```

Related Commands

Command	Description
real	Identifies a real server.
show ip slb reals	Displays information about the real servers.
show ip slb serverfarms	Displays information about the server farm configuration.

retry (real server)

To specify how long to wait before a new connection is attempted to a failed server, use the **retry** SLB real server configuration command. To restore the default retry value, use the **no** form of this command.

retry *retry-value*

no retry

Syntax Description

retry-value	Time, in seconds, to wait after the detection of a server failure before a new connection to the server is attempted. If the new connection attempt succeeds, the real server is placed in OPERATIONAL state. If the connection attempt fails, the timer is reset, the connection is reassigned, and the process repeats until it is successful or until the server is placed OUTOFSERVICE by the network administrator. Valid values range from 1 to 3600. The default value is 60 seconds. A value of 0 means do not attempt a new connection to the server when it fails.

Defaults

The *retry-value* default is 60 seconds.

Command Modes

SLB real server configuration

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.

Examples

The following example specifies that 120 seconds must elapse after the detection of a server failure before a new connection is attempted:

```
ip slb serverfarm PUBLIC
 real 10.10.1.1
 retry 120
```

Related Commands

Command	Description
real	Identifies a real server.
show ip slb reals	Displays information about the real servers.
show ip slb serverfarms	Displays information about the server farm configuration.

serverfarm

To associate a real server farm with a virtual server, use the **serverfarm** SLB virtual server configuration command. To remove the server farm association from the virtual server configuration, use the **no** form of this command.

serverfarm *serverfarm-name*

no serverfarm

Syntax Description

serverfarm-name	Name of a server farm that has already been defined using the **ip slb serverfarm** command.

Defaults

No default behavior or values.

Command Modes

SLB virtual server configuration

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.

Examples

The following example shows how the **ip slb vserver**, **virtual**, and **serverfarm** commands are used to associate the real server farm named PUBLIC with the virtual server named PUBLIC_HTTP:

```
ip slb vserver PUBLIC_HTTP
 virtual 10.0.0.1 tcp www
 serverfarm PUBLIC
```

Related Commands

Command	Description
show ip slb vservers	Displays information about the virtual servers.
virtual	Configures the virtual server attributes.

show ip slb conns

To display the active IOS SLB connections, use the **show ip slb conns** privileged EXEC command.

show ip slb conns [**vserver** *virtserver-name*] [**client** *ip-address*] [**detail**]

Syntax Description

vserver	(Optional) Displays only those connections associated with a particular virtual server.
virtserver-name	(Optional) Name of the virtual server to be monitored.
client	(Optional) Displays only those connections associated with a particular client IP address.
ip-address	(Optional) IP address of the client to be monitored.
detail	(Optional) Displays detailed connection information.

Defaults

If no options are specified, the command displays output for all active IOS SLB connections.

Command Modes

Privileged EXEC

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.

Examples

The following example shows IOS SLB active connection data:

```
router# show ip slb conns

vserver          prot   client               real                 state
---------------------------------------------------------------------------
TEST             TCP    7.150.72.183:328     80.80.90.25:80       CLOSING
TEST             TCP    7.250.167.226:423    80.80.90.26:80       CLOSING
TEST             TCP    7.234.60.239:317     80.80.90.26:80       CLOSING
TEST             TCP    7.110.233.96:747     80.80.90.26:80       CLOSING
TEST             TCP    7.162.0.201:770      80.80.90.30:80       CLOSING
TEST             TCP    7.22.225.219:995     80.80.90.26:80       CLOSING
TEST             TCP    7.2.170.148:169      80.80.90.30:80       CLOSING
```

Table 31 describes the significant fields shown in the display.

Table 31 show ip slb conns Field Descriptions

Field	Description
vserver	Name of the virtual server whose connections are being monitored and displayed. Information about each connection is displayed on a separate line.
prot	Protocol being used by the connection.
client	Client IP address being used by the connection.
real	Real IP address of the connection.
state	Current state of the connection: • CLOSING—IOS SLB TCP connection deactivated (awaiting a delay timeout before cleaning up the connection). • ESTAB—IOS SLB TCP connection processed a SYN-SYN/ACK exchange between the client and server. • FINCLIENT—IOS SLB TCP connection processed a FIN from the client. • FINSERVER—IOS SLB TCP connection processed a FIN from the server. • INIT—Initial state of the IOS SLB TCP connection. • SYNBOTH—IOS SLB TCP connection processed one or more TCP SYNs from both the client and the server. • SYNCLIENT—IOS SLB TCP connection processed one or more client TCP SYNs. • SYNSERVER—IOS SLB TCP connection processed one or more server 1 TCP SYNs. • ZOMBIE—Destruction of the IOS SLB TCP connection failed, possibly because of bound flows. Destruction will proceed when the flows are unbound.

show ip slb dfp

To display DFP manager and agent information such as passwords, timeouts, retry counts, and weights, use the **show ip slb dfp** privileged EXEC command.

show ip slb dfp [**agent** *ip-address port-number* | **detail** | **weights**]

Syntax Description

agent	(Optional) Displays information about an agent.
ip-address	(Optional) Agent IP address.
port-number	(Optional) Agent port number.
detail	(Optional) Displays all data available.
weights	(Optional) Displays information about weights assigned to real servers for load balancing.

Defaults

If no options are specified, the command displays summary information.

Command Modes

Privileged EXEC

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.

Examples

The following example shows IOS SLB DFP data:

```
router# show ip slb dfp detail

DFP Manager:
      Current passwd:NONE Pending passwd:NONE
      Passwd timeout:0 sec
      Uned errors:0
DFP Agent 161.44.2.34:61936 Connection state:Connected
   Timeout = 0      Retry Count = 0      Interval = 180   (Default)
   Security errors = 0
   Last message received:10:20:26 UTC 11/02/99
   Last reported Real weights for Protocol TCP, Port www
      Host 17.17.17.17 1      Weight 1
      Host 68.68.68.68   Bind ID 4      Weight 4
      Host 85.85.85.85   Bind ID 5      Weight 5
   Last reported Real weights for Protocol TCP, Port 22
      Host 17.17.17.17   Bind ID 111    Weight 111


router# show ip slb dfp weights

Real IP Address 17.17.17.17 Protocol TCP Port 22 Bind_ID 111 Weight 111
      Set by Agent 161.44.2.3458490 at 132241 UTC 12/03/99
Real IP Address 17.17.17.17 Protocol TCP Port www Bind_ID 1 Weight 1
      Set by Agent 161.44.2.3458490 at 132241 UTC 12/03/99
```

```
Real IP Address 68.68.68.68 Protocol TCP Port www Bind_ID 4 Weight 4
      Set by Agent 161.44.2.3458490 at 132241 UTC 12/03/99
Real IP Address 85.85.85.85 Protocol TCP Port www Bind_ID 5 Weight 5
      Set by Agent 161.44.2.3458490 at 132241 UTC 12/03/99


router# show ip slb dfp

DFP Manager:
      Current passwd:NONE Pending passwd:NONE
      Passwd timeout:0 sec

Agent IP          Port    Timeout   Retry Count   Interval
-----------------------------------------------------------------
161.44.2.34       61936   0         0             180 (Default)
```

Table 32 describes the significant fields shown in the display.

Table 32 show ip slb dfp Field Descriptions

Field	Description
Agent IP	IP address of the agent about which information is being displayed.
Port	Port number of the agent.
Timeout	Time period (in seconds) during which the DFP manager must receive an update from the DFP agent. A value of 0 means there is no timeout.
Retry Count	Number of times the DFP manager attempts to establish the TCP connection to the DFP agent. A value of 0 means there are infinite retries.
Interval	Interval (in seconds) between retries.

show ip slb reals

To display information about the real servers, use the **show ip slb reals** privileged EXEC command.

show ip slb reals [**vserver** *virtserver-name*] [**detail**]

Syntax Description

vserver	(Optional) Displays information about only those real servers associated with a particular virtual server.
virtserver-name	(Optional) Name of the virtual server.
detail	(Optional) Displays detailed information.

Defaults

If no options are specified, the command displays information about all real servers.

Command Modes

Privileged EXEC

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.

Examples

The following example shows IOS SLB real server data:

```
router# show ip slb reals

real            server farm      weight   state           conns
-------------------------------------------------------------------------
80.80.2.112     FRAG             8        OUTOFSERVICE    0
80.80.5.232     FRAG             8        OPERATIONAL     0
80.80.15.124    FRAG             8        OUTOFSERVICE    0
80.254.2.2      FRAG             8        OUTOFSERVICE    0
80.80.15.124    LINUX            8        OPERATIONAL     0
80.80.15.125    LINUX            8        OPERATIONAL     0
80.80.15.126    LINUX            8        OPERATIONAL     0
80.80.90.25     SRE              8        OPERATIONAL     220
80.80.90.26     SRE              8        OPERATIONAL     216
80.80.90.27     SRE              8        OPERATIONAL     216
80.80.90.28     SRE              8        TESTING         1
80.80.90.29     SRE              8        OPERATIONAL     221
80.80.90.30     SRE              8        OPERATIONAL     224
80.80.30.3      TEST             100      READY_TO_TEST   0
80.80.30.4      TEST             100      READY_TO_TEST   0
80.80.30.5      TEST             100      READY_TO_TEST   0
80.80.30.6      TEST             100      READY_TO_TEST   0
```

Table 33 describes significant fields shown in the display.

Table 33 show ip slb reals Field Descriptions

Field	Description
real	IP address of the real server about which information is being displayed. Used to identify each real server. Information about each real server is displayed on a separate line.
server farm	Name of the server farm to which the real server is associated.
weight	Weight assigned to the real server. The weight identifies the capacity of the real server, relative to other real servers in the server farm.
state	Current state of the real server: • DFP_THROTTLED—DFP agent sent a weight of **0** for this real server (send no further connections to this real server). • FAILED—Removed from use by the predictor algorithms; retry timer started. • MAXCONNS—Maximum number of simultaneous active connections reached. • OPERATIONAL—Functioning properly. • OUTOFSERVICE—Removed from the load-balancing predictor lists. • READY_TO_TEST—Queued for testing. • TESTING—Queued for assignment.

show ip slb serverfarms

To display information about the server farms, use the **show ip slb serverfarms** privileged EXEC command.

show ip slb serverfarms [**name** *serverfarm-name*] [**detail**]

Syntax Description

name	(Optional) Displays information about only a particular server farm.
serverfarm-name	(Optional) Name of the server farm.
detail	(Optional) Displays detailed server farm information.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

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.

Examples

The following example shows IOS SLB server farm data:

```
router# show ip slb serverfarms

server farm      predictor     reals   bind id
-------------------------------------------------
FRAG             ROUNDROBIN    4       0
LINUX            ROUNDROBIN    3       0
SRE              ROUNDROBIN    6       0
TEST             ROUNDROBIN    4       0
```

Table 34 describes the significant fields shown in the display.

Table 34 show ip slb serverfarms Field Descriptions

Field	Description
server farm	Name of the server farm about which information is being displayed. Information about each server farm is displayed on a separate line.
predictor	Type of load-balancing algorithm (ROUNDROBIN or LEASTCONNS) used by the server farm.
reals	Number of real servers configured in the server farm.
bind id	Bind ID configured on the server farm.

show ip slb stats

To display IOS SLB statistics, use the **show ip slb stats** privileged EXEC command.

show ip slb stats

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

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.

Examples

The following example shows IOS SLB statistics:

```
router# show ip slb stats

Pkts via normal switching: 530616
Pkts via special switching:1812710
Connections Created:       783774
Connections Established:   633418
Connections Destroyed:     782752
Connections Reassigned:    0
Zombie Count:              0
```

Table 35 describes the significant fields shown in the display.

Table 35 show ip slb stats Field Descriptions

Field	Description
Pkts via normal switching	Number of packets handled by the IOS SLB feature via normal switching since the last time counters were cleared.
Pkts via special switching	Number of packets handled by the IOS SLB feature via special switching since the last time counters were cleared.
Connections Created	Number of connections created since the last time counters were cleared.
Connections Established	Number of connections created that have become established since the last time counters were cleared.
Connections Destroyed	Number of connections destroyed since the last time counters were cleared.

Table 35 show ip slb stats Field Descriptions (continued)

Connections Reassigned	Number of connections reassigned to a different real server since the last time counters were cleared.
Zombie Count	Number of connections currently pending destruction, awaiting a timeout or some other condition to be met.

show ip slb sticky

To display the entries in the IOS SLB sticky database, use the **show ip slb sticky** privileged EXEC command.

show ip slb sticky [**client** *ip-address*]

Syntax Description

client	(Optional) Displays only those sticky database entries associated with a particular client IP address.
ip-address	(Optional) IP address of the client.

Defaults

If no options are specified, the command displays information about all virtual servers.

Command Modes

Privileged EXEC

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.

Examples

The following example shows the entries in the IOS SLB sticky database:

```
router# show ip slb sticky

client            group   real              conns     ftp-cntrl
------------------------------------------------------------
10.10.2.12        4097      10.10.3.2         1         0
```

Table 36 describes the significant fields shown in the display.

Table 36 show ip slb sticky Field Descriptions

Field	Description
client	Client IP address that is bound to this sticky assignment.
group	Group ID for this sticky assignment.
real	Real server used by all clients connecting with the client IP address detailed on this line.
conns	Number of connections currently sharing this sticky assignment.
ftp-cntrl	Number of FTP control connections currently using this sticky assignment.

show ip slb vservers

To display information about the virtual servers, use the **show ip slb vservers** privileged EXEC command.

show ip slb vservers [**name** *virtserver-name*] [**detail**]

Syntax Description

name	(Optional) Displays information about only this virtual server.
virtserver-name	(Optional) Name of the virtual server.
detail	(Optional) Displays detailed virtual server information.

Defaults

If no options are specified, the command displays information about all virtual servers.

Command Modes

Privileged EXEC

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.

Examples

The following example shows virtual server data:

```
router# show ip slb vservers

slb vserver      prot   virtual              state          conns
---------------------------------------------------------------------
TEST             TCP    80.80.254.3:80       OPERATIONAL    1013
TEST21           TCP    80.80.254.3:21       OUTOFSERVICE   0
TEST23           TCP    80.80.254.3:23       OUTOFSERVICE   0
```

Table 37 describes the significant fields shown in the display.

Table 37 show ip slb vservers Field Descriptions

Field	Description
slb vserver	Name of the virtual server about which information is being displayed. Information about each virtual server is displayed on a separate line.
prot	Protocol being used by the virtual server detailed on a given line.
virtual	Virtual IP address of the virtual server detailed on a given line.
state	Current state of the virtual server detailed on a given line.
conns	Number of connections associated with the virtual server detailed on a given line.

sticky

To assign all connections from a client to the same real server, use the **sticky** virtual server configuration command. To remove the client/server coupling, use the **no** form of this command.

sticky *duration* [**group** *group-id*]

no sticky

Syntax Description

duration	Sticky timer duration (in seconds). Valid values range from 0 to 65535.
group	(Optional) Places the virtual server in a sticky group, for coupling of services.
group-id	(Optional) Number identifying the sticky group to which the virtual server belongs. Valid values range from 0 to 255.

Defaults

Sticky connections are not tracked.

Virtual servers are not associated with any groups.

Command Modes

SLB virtual server configuration

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.

Usage Guidelines

The last real server that was used for a connection from a client is stored for the set *duration* seconds. If a new connection from the client to the virtual server is initiated during that time, the same real server that was used for the previous connection is chosen for the new connection. If two virtual servers are placed in the same group, coincident connection requests for those services from the same IP address are handled by the same real server.

Examples

The following example specifies that if a subsequent request from a client for a virtual server is made within 60 seconds of the previous request, then the same real server is used for the connection. This example also places the virtual server in group 10.

```
ip slb vserver VS1
sticky 60 group 10
```

Related Commands

Command	Description
show ip slb sticky	Displays information about the virtual server or firewall farm sticky configuration.
show ip slb vservers	Displays information about the virtual servers.
virtual	Configures the virtual server attributes.

synguard

To limit the rate of TCP SYNs handled by a virtual server to prevent an SYN flood Denial-of-Service attack, use the **synguard** virtual server configuration command. To remove the threshold, use the **no** form of this command.

synguard *syn-count* [*interval*]

no synguard

Syntax Description

syn-count	Number of unanswered SYNs that are allowed to be outstanding to a virtual server. Valid values range from 0 (off) to 4294967295. The default is 0.
interval	(Optional) Interval (in milliseconds) for SYN threshold monitoring. Valid values range from 50 to 5000. The default is 100 ms.

Defaults

The default SYN count is 0 (off).

The default interval is 100 ms.

Command Modes

SLB virtual server configuration

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.

Examples

The following example sets the threshold of unanswered SYNs to 50:

```
ip slb vserver PUBLIC_HTTP
synguard 50
```

Related Commands

Command	Description
show ip slb vservers	Displays information about the virtual servers.
virtual	Configures the virtual server attributes.

virtual

To configure virtual server attributes, use the **virtual** virtual server configuration command. To remove the attributes, use the **no** form of this command.

virtual *ip-address* {**tcp** | **udp**} *port-number* [**service** *service-name*]

no virtual

Syntax Description

ip-address	IP address for this virtual server instance, used by clients to connect to the server farm.
tcp	Performs load balancing for only TCP connections.
udp	Performs load balancing for only UDP connections.
port-number	(Optional) 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-number* argument are as follows: • Domain Name System: **dns 53** • File Transfer Protocol: **ftp 21** • HTTP over Secure Socket Layer: **https 443** • 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** • 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).
service	(Optional) Couple connections associated with a given service, such as HTTP or Telnet, so all related connections from the same client use the same real server.
service-name	(Optional) Type of connection coupling. Currently, the only choice is **ftp**. Couple FTP data connections with the control session that created them.

Defaults

No default behavior or values.

Command Modes

SLB virtual server configuration

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.

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 the IOS SLB feature. 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**.

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.

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.

```
ip slb vserver PUBLIC_HTTP
virtual 10.0.0.1 tcp www
```

Related Commands

Command	Description
ip slb vserver	Identifies a virtual server.
show ip slb vservers	Displays information about the virtual servers.

weight

To specify the capacity of a real server relative to other real servers in the server farm, use the **weight** real server configuration command. To restore the default weight value, use the **no** form of this command.

weight *weighting-value*

no weight

Syntax Description

weighting-value	Weighting value to use for real server predictor algorithm. Valid values range from 1 to 155. The default weighting value is 8.

Defaults

The default weighting value is 8.

Command Modes

SLB real server configuration

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.

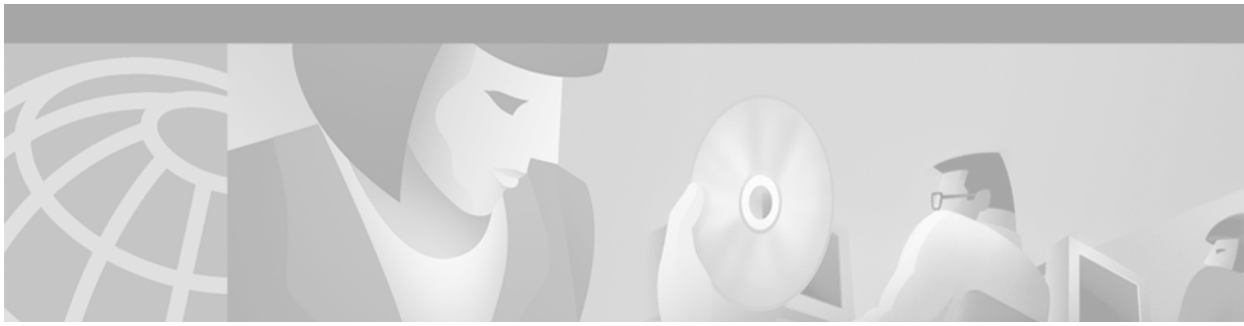
Examples

The following example specifies the relative weighting values of three real servers as 16, 8 (by default), and 24, respectively:

```
ip slb serverfarm PUBLIC
real 10.10.1.1                          First real server
weight 16                               Assigned weight of 16
inservice                               Enabled
exit
real 10.10.1.2                          Second real server
inservice                               Enabled; default weight
exit
real 10.10.1.3                          Third real server
weight 24                               Assigned weight of 24;
```

Related Commands

Command	Description
real	Identifies a real server.
show ip slb reals	Displays information about the real servers.
show ip slb serverfarms	Displays information about the server farm configuration.



Mobile IP Commands

Use the commands in this chapter to configure and monitor Mobile IP. For Mobile IP configuration information and examples, refer to the "Configuring Mobile IP" chapter of the *Cisco IOS IP Configuration Guide*.

aaa authorization ipmobile

To authorize Mobile IP to retrieve security associations from the AAA server using TACACS+ or RADIUS, use the **aaa authorization ipmobile** global configuration command. 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*	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 suppported.

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.

clear ip mobile binding

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

clear ip mobile binding {**all** [**load** *standby-group-name*] | [*ip-address*]}

Syntax Description

all	Clears all mobility bindings.
load	(Optional) Downloads mobility bindings for a standby group after clear.
standby-group-name	(Optional) Name of the standby group.
ip-address	(Optional) IP address of a mobile node.

Command Modes

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*

Usage Guidelines

The home agent creates a mobility binding for each roaming mobile node. The mobility binding allows the mobile node to exchange packets with the correspondent 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. There should be no need to clear the binding because it expires after lifetime is reached or when the mobile node deregisters.

When the mobility binding is removed, 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.

Use this command with care, because it may terminate any sessions used by the mobile node. After using this command, the visitor will need to reregister to continue roaming.

Examples

The following example administratively stops mobile node 10.0.0.1 from roaming:

```
Router# clear ip mobile binding 10.0.0.1

Router# show ip mobile binding

Mobility Binding List:
Total 1
10.0.0.1:
    Care-of Addr 68.0.0.31, Src Addr 68.0.0.31,
    Lifetime granted 02:46:40 (10000), remaining 02:46:32
    Flags SbdmGvt, Identification B750FAC4.C28F56A8,
    Tunnel100 src 66.0.0.5 dest 68.0.0.31 reverse-allowed
    Routing Options - (G)GRE
```

Related Commands

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

clear ip mobile secure

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

clear ip mobile secure {**host** *lower* [*upper*] | **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 addresses.
upper	(Optional) Upper end of range of IP addresses.
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.

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 10.0.0.1 after registration:

```
Router# show ip mobile secure host 10.0.0.1

Security Associations (algorithm,mode,replay protection,key):
10.0.0.1:
    SPI 300,  MD5, Prefix-suffix, Timestamp +/- 7,
    Key 'oldkey' 1230552d39b7c1751f86bae5205ec0c8
```

The security association of the AAA server changes as follows:

```
Router# clear ip mobile secure host 10.0.0.1 load

Router# show ip mobile secure host 10.0.0.1
```

```
10.0.0.1:
    SPI 300,  MD5, Prefix-suffix, Timestamp +/- 7,
    Key 'newkey' 1230552d39b7c1751f86bae5205ec0c8
```

Related Commands

Command	Description
ip mobile secure aaa-download	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** EXEC command.

clear ip mobile traffic [**undo**]

Syntax Description

undo	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 (this is useful for debugging). See the **show ip mobile traffic** command for a description of all counters.

Examples

The following example shows how the 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.

clear ip mobile visitor

To remove visitor information, use the **clear ip mobile visitor** EXEC command.

clear ip mobile visitor [*ip-address*]

Syntax Description

ip-address	(Optional) IP address. If not specified, visitor information will be removed for all addresses.

Command Modes

EXEC

Command History

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

Usage Guidelines

The foreign agent creates a visitor entry for each accepted visitor. The visitor entry allows the mobile node to receive packets while in a visited network. Associated with the visitor entry is the ARP entry for the visitor. There should be no need to clear the entry because it expires after lifetime is reached or when the mobile node deregisters.

When a visitor entry is removed, the number of users on the tunnel is decremented and the ARP entry is removed from the ARP cache. The visitor is not notified.

Use this command with care because it may terminate any sessions used by the mobile node. After using this command, the visitor will need to reregister to continue roaming.

Examples

The following example administratively stops visitor 10.0.0.1 from visiting:

```
Router# clear ip mobile visitor 10.0.0.1
```

Related Commands

Command	Description
show ip mobile visitor	Displays the table containing the visitor list of the foreign agent.

ip mobile foreign-agent

To enable foreign agent service, use the **ip mobile foreign-agent** global configuration command. To disable this service, use the **no** form of this command.

ip mobile foreign-agent [**care-of** *interface* | **reg-wait** *seconds*]

no ip mobile foreign-agent [**care-of** *interface* | **reg-wait** *seconds*]

Syntax Description

care-of *interface*	(Optional) IP address of the interface. Sets the care-of address on the foreign agent. Multiple care-of addresses can be configured.
reg-wait *seconds*	(Optional) Pending registration expires after the specified number of seconds if no reply is received. Range is from 5 to 600. Default is 15.

Defaults

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command enables foreign agent service when at least one care-of address is configured. When no care-of address exists, foreign agent service is disabled.

The foreign agent is responsible for relaying the registration request to the home agent, setting up tunnel to the home agent, and forwarding packets to the mobile node. The **show** commands used to display relevant information are shown in parentheses in the following paragraph.

When a registration request comes in, the foreign agent will ignore requests when foreign agent service is not enabled on interface or no care-of address is advertised. If a security association exists for a visiting mobile node, the visitor is authenticated (**show ip mobile secure visitor** command). The registration bitflag is handled as described in Table 38 (**show ip mobile interface** command). The foreign agent checks the validity of the request. If successful, the foreign agent relays the request to the home agent, appending an FH authentication extension if a security association for the home agent exists. The pending registration timer of 15 seconds is started (**show ip mobile visitor pending** command). At most, five outstanding pending requests per mobile node are allowed. If a validity check fails, the foreign agent sends a reply with error code to the mobile node (reply codes are listed in Table 39). A security violation is logged when visiting mobile node authentication fails (**show ip mobile violation** command). (Violation reasons are listed in Table 43.)

When a registration reply comes in, the home agent is authenticated (**show ip mobile secure home-agent** command) if a security association exists for the home agent (IP source address or home agent address in reply). The reply is relayed to the mobile node.

When registration is accepted, the foreign agent creates or updates the visitor table, which contains the expiration timer. If no binding existed before this registration, a virtual tunnel is created, a host route to the mobile node via the interface (of the incoming request) is added to the routing table (**show ip route mobile** command), and an ARP entry is added to avoid sending ARP requests for the visiting mobile node. Visitor binding is removed (along with its associated host route, tunnel, and ARP entry) when the registration lifetime expires or deregistration is accepted.

When registration is denied, the foreign agent will remove the request from the pending registration table. The table and timers of the visitor will be unaffected.

When a packet destined for the mobile node arrives on the foreign agent, the foreign agent will deencapsulates the packet and forwards it out its interface to the visiting mobile node, without sending ARP requests.

The care-of address must be advertised by the foreign agent. This is used by the mobile node to register with the home agent. The foreign agent and home agent use this address as the source and destination point of tunnel, respectively. The foreign agent is not enabled until at least one care-of address is available. The foreign agent will advertise on interfaces configured with the **ip mobile foreign-service** command.

Only care-of addresses with interfaces that are up are considered available.

Table 38 lists foreign agent registration bitflags.

Table 38 Foreign Agent Registration Bitflags

Bit Set	Registration Request
S	No operation. Not applicable to foreign agent.
B	No operation. Not applicable to foreign agent.
D	Make sure source IP address belongs to the network of the interface.
M	Deny request. Minimum IP encapsulation is not supported.
G	No operation. GRE encapsulation is supported.
V	Deny request. Van Jacobson Header compression is not supported.
T	Deny request. Reverse tunnel is not supported.
reserved	Deny request. Reserved bit must not be set.

Table 39 lists foreign agent reply codes.

Table 39 Foreign Agent Reply Codes

Code	Reason
64	Reason unspecified.
65	Administratively prohibited.
66	Insufficient resource.
67	Mobile node failed authentication.
68	Home agent failed authentication.
69	Requested lifetime is too long.
70	Poorly formed request.
71	Poorly formed reply.

Table 39 Foreign Agent Reply Codes (continued)

Code	Reason
72	Requested encapsulation is unavailable.
73	Requested Van Jacobson Header compression is unavailable.
74	Reverse tunnel unsupported.
80-95	ICMP Unreachable message code 0 to 15.

Examples

The following example enables foreign agent service on interface Ethernet1, advertising 1.0.0.1 as the care-of address:

```
ip mobile foreign-agent care-of Ethernet0
interface Ethernet0
 ip address 1.0.0.1 255.0.0.0
interface Ethernet1
 ip mobile foreign-service
```

Related Commands

Command	Description
debug ip mobile advertise	Displays advertisement information.
ip mobile foreign-service	Enables foreign agent service on an interface if care-of addresses are configured.
show ip mobile globals	Displays global information for mobile agents.
show ip mobile interface	Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes.
show ip mobile secure	Displays mobility security associations for mobile host, mobile visitor, foreign agent, or home agent.
show ip mobile violation	Displays information about security violations.
show ip mobile visitor	Displays the table containing the visitor list of the foreign agent.

ip mobile foreign-service

To enable foreign agent service on an interface if care-of addresses are configured, use the **ip mobile foreign-service** interface configuration command. To disable this service, use the **no** form of this command.

ip mobile foreign-service [**home-access** *acl*] [**limit** *number*] [**registration-required**]

no ip mobile foreign-service [**home-access** *acl*] [**limit** *number*] [**registration-required**]

Syntax Description

home-access *acl*	(Optional) Controls which home agent addresses mobile nodes can be used to register. The access list can be a string or number from 1 to 99. You cannot use this keyword when you enable foreign agent service on a subinterface.
limit *number*	(Optional) Number of visitors allowed on interface. The Busy (B) bit will be advertised when the number of registered visitors reach this limit. Range is from 1 to 1000. Default is no limit. You cannot use this keyword when you enable foreign agent service on a subinterface.
registration-required	(Optional) Solicits registration from the mobile node even if it uses colocated care-of addresses. The Registration-required (R) bit will be advertised. You cannot use this keyword when you enable foreign agent service on a subinterface.

Defaults

Disabled. Default is no limit to the number of visitors allowed on an interface.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command enables foreign agent service on the interface. The foreign agent (F) bit will be set in the agent advertisement, which is appended to the IRDP router advertisement whenever the foreign agent or home agent service is enabled on the interface.

Note The Registration-required bit only tells the visiting mobile node to register even if the visiting mobile node is using a colocated care-of address. You must set up packet filters to enforce this. For example, you could deny packets destined for port 434 from the interface of this foreign agent.

Table 40 lists the advertised bitflags.

Table 40 Foreign Agent Advertisement Bitflags

Bit Set	Service Advertisement
R	Set if the **registration-required** parameter is enabled.
B	Set if the number of visitors reached the **limit** parameter.
H	Set if the interface is the home link to the mobile host (group).
F	Set if foreign-agent service is enabled.
M	Never set.
G	Always set.
V	Never set.
reserved	Never set.

Examples

The following example enables foreign agent service for up to 100 visitors:

```
interface Ethernet 0
 ip mobile foreign-service limit 100 registration-required
```

Related Commands

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

ip mobile home-agent

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

ip mobile home-agent [**address** *ip-address*][**broadcast**] [**care-of-access** *acl*] [**lifetime** *number*] [**replay** *seconds*] [**reverse-tunnel-off**] [**roam-access** *acl*] [**suppress-unreachable**]

no ip mobile home-agent [**broadcast**] [**care-of-access** *acl*] [**lifetime** *number*] [**replay** *seconds*] [**reverse-tunnel-off**] [**roam-access** *acl*] [**suppress-unreachable**]

Syntax Description

address *ip-address*	(Optional) Specifies the IP address of the home agent. This option is only applicable when home agent redundancy is used for virtual networks.
broadcast	(Optional) Enables broadcast datagram routing. By default, broadcasting is disabled.
care-of-access *acl*	(Optional) Controls which care-of addresses (in registration request) are permitted by the home agent. By default, all care-of addresses are permitted. The access control list can be a string or number from 1 to 99.
lifetime *number*	(Optional) Specifies the global registration lifetime for a mobile node. Note that this can be overridden by the individual mobile node configuration. Range is from 3 to 65535 (infinity). Default is 36000 seconds (10 hours). Registrations requesting a lifetime greater than this value will still be accepted, but will use this lifetime value.
replay *seconds*	(Optional) Sets the replay protection time-stamp value. Registration received within this time is valid.
reverse-tunnel-off	(Optional) Disables support of reverse tunnel by the home agent. By default, reverse tunnel support is enabled.
roam-access *acl*	(Optional) Controls which mobile nodes are permitted or denied to roam. By default, all specified mobile nodes can roam.
suppress-unreachable	(Optional) Disables sending ICMP unreachable messages to the source when a mobile node on the virtual network is not registered, or when a packet came in from a tunnel interface created by the home agent (in the case of a reverse tunnel). By default, ICMP unreachable messages are sent.

Defaults

Disabled. Broadcasting is disabled by default. Reverse tunnel support is enabled by default. ICMP Unreachable messages are sent by default.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

The home agent is responsible for processing registration requests from the mobile node and setting up tunnels and routes to the care-of address. Packets to the mobile node are forwarded to the visited network.

The home agent will forward broadcast packets to mobile nodes if they registered with the service. However, heavy broadcast traffic utilizes the CPU of the router. The home agent can control where the mobile nodes roam by the **care-of-access** parameter, and which mobile node is allowed to roam by the **roam-access** parameter.

When a registration request comes in, the home agent will ignore requests when home agent service is not enabled or the security association of the mobile node 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 foreign agent (IP source address or care-of address in request), the foreign agent is authenticated, and then the mobile node is authenticated. The Identification field is verified to protect against replay attack. The home agent checks the validity of the request (see Table 41) and sends a reply. (Replay codes are listed in Table 42.) A security violation is logged when foreign agent authentication, MH authentication, or Identification verification fails. (The violation reasons are listed in Table 43.)

After registration is accepted, the home agent creates or updates the mobility binding of the mobile node, which contains the expiration timer. If no binding existed before this registration, a virtual tunnel is created, a host route to the mobile node 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 mobile nodes are using it), and gratuitous ARPs are sent out if the mobile node is back home. Mobility binding is removed (along with its associated host route and tunnel) when registration lifetime expires or deregistration is accepted.

When the packet destined for the mobile node arrives on the home agent, the home agent encapsulates the packet and tunnels it to the care-of address. If the Don't fragment bit is set in the packet, the outer bit of the IP header is also set. 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 sent to the source. If the home agent loses the route to the tunnel endpoint, the host route to the mobile node will be removed from the routing table until tunnel route is available. Packets destined for the mobile node without a host route will be sent out the interface (home link) or to the virtual network (see the description of **suppress-unreachable** keyword). For subnet-directed broadcasts to the home link, the home agent will send a copy to all mobile nodes registered with the broadcast routing option.

Table 41 describes how the home agent treats registrations with various bits set when authentication and identification are passed.

Table 41 Home Agent Registration Bitflags

Bit Set	Registration Reply
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	Ignore. Van Jacobsen Header compression is not supported.

Table 41 Home Agent Registration Bitflags (continued)

Bit Set	Registration Reply
T	Accept if **reverse-tunnel-off** parameter is not set.
reserved	Deny. Reserved bit must not be set.

Table 42 lists the home agent registration reply codes.

Table 42 Home Agent Registration Reply Codes

Code	Reason
0	Accept.
1	Accept, no simultaneous bindings.
128	Reason unspecified.
129	Administratively prohibited.
130	Insufficient resource.
131	Mobile node failed authentication.
132	Foreign agent failed authentication.
133	Registration identification mismatched.
134	Poorly formed request.
136	Unknown home agent address.
137	Reverse tunnel is unavailable.
139	Unsupported encapsulation.

Table 43 lists security violation codes.

Table 43 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.

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
show ip mobile globals	Displays global information for mobile agents.

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 *sec*

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

Syntax Description

sec	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 standby

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

ip mobile home-agent standby *hsrp-group-name* [[**virtual-network**] **address** *address*]

no ip mobile home-agent standby *hsrp-group-name* [[**virtual-network**] **address** *address*]

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

No global home agent addresses are specified.

Command Modes

Global configuration

Command History

Release	Modification
12.0(2)T	This command was introduced.

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.

Examples

The following example specifies an HSRP group named SanJoseHA:

```
ip mobile home-agent standby SanJoseHA
```

Related Commands

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

ip mobile host

To configure the mobile host or mobile node group, use the **ip mobile host** global configuration command.

ip mobile host *lower* [*upper*] {**interface** *name* | **virtual-network** *net mask*} [**aaa** [**load-sa**]] [**care-of-access** *acl*] [**lifetime** *number*]

no ip mobile host *lower* [*upper*] {**interface** *name* | **virtual-network** *net mask*} [**aaa** [**load-sa**]] [**care-of-access** *acl*] [**lifetime** *number*]

Syntax Description

lower [*upper*]	Range of mobile host or mobile node group IP addresses.
interface *name*	Mobile node that belongs to the specified interface.
virtual-network *net mask*	The wireless mobile node resides in the virtual network created using the **ip mobile virtual-network** command.
aaa	(Optional) Retrieves security associations froma AAA (TACACS+ or RADIUS) server.
load-sa	(Optional) Stores security associations in memory after retrieval.
care-of-access *acl*	(Optional) Access list. This can be a string or number from 1 to 99. Controls where mobile nodes roam—the acceptable care-of addresses.
lifetime *number*	(Optional) Lifetime (in seconds). The lifetime for each mobile node (group) can be set to override the global value. Range is from 3 to 65535.

Defaults

No host is configured.

Command Modes

Global configuration

Command History

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

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 an AAA server. When using an AAA server, the router will attempt to download all security associations when the command is entered. If no security associations are retrieved, retrieval will be attempted when a registration request arrives or the **clear ip mobile secure** command is entered.

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 44 are based on the assumption of one security association per mobile node.

Security associations can be stored using one of three methods:

- On the router
- On the AAA server, retrieve security association each time registration comes in
- On the AAA server, retrieve and store security association

Each method has advantages and disadvantages, which are described in Table 44.

Table 44 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 only need memory to load in a security association, and then release the memory when done. Router can support unlimited number of mobile nodes.	• 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 44 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.

Examples

The following example configures a mobile node group to reside on virtual network 20.0.0.0 and store its security associations on the AAA server:

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

Related Commands

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

ip mobile prefix-length

To append the prefix-length extension to the advertisement, use the **ip mobile prefix-length** interface configuration command. To restore the default, use the **no** form of this command.

ip mobile prefix-length

no ip mobile prefix-length

Syntax Description

This command has no arguments or keywords.

Defaults

The prefix-length extension is not appended.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The prefix-length extension is used for movement detection. When a mobile node registered with one foreign agent receives an agent advertisement from another foreign agent, the mobile node uses the prefix-length extension to determine whether the advertisements arrived on the same network. The mobile node needs to register with the second foreign agent if it is on a different network. If the second foreign agent is on the same network, reregistration is not necessary.

Examples

The following example appends the prefix-length extension to agent advertisements sent by a foreign agent:

```
ip mobile prefix-length
```

Related Commands

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

ip mobile registration-lifetime

To set the registration lifetime value advertised, use the **ip mobile registration-lifetime** interface configuration command.

ip mobile registration-lifetime *seconds*

Syntax Description

seconds	Lifetime in seconds. Range is from 3 to 65535 (infinity).

Defaults

36000 seconds

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command allows an administrator to control the advertised lifetime on the interface. The foreign agent uses this command to control duration of registration. Visitors requesting longer lifetimes will be denied.

Examples

The following example sets the registration lifetime to 10 minutes on interface Ethernet 1 and 1 hour on interface Ethernet 2:

```
interface e1
 ip mobile registration-lifetime 600
interface e2
 ip mobile registration-lifetime 3600
```

Related Commands

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

ip mobile secure aaa-download

To specify that authentication, authorization, and accounting (AAA) mobility security associations (SAs) are downloaded from the AAA server and at what rate the information is downloaded, use the **ip mobile secure aaa-download** command in global configuration mode. To delete the AAA download rate, use the **no** form of this command.

ip mobile secure aaa-download rate *seconds*

no ip mobile secure aaa-download rate *seconds*

Syntax Description

rate	Rate at which the AAA SA is downloaded. • *seconds*—Download rate, in seconds. The range is from 1 to 100.

Defaults

No AAA SAs are downloaded.

Command Modes

Global configuration

Command History

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

Usage Guidelines

SAs are downloaded from a AAA server on the first use. This command allows the home agent (HA) to prepopulate an SA table.

Examples

The following example shows a download rate of 35 seconds:

```
ip mobile secure aaa-download rate 35
```

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.
ip mobile secure foreign-agent	Configures the mobility SAs for an FA.
ip mobile secure home-agent	Configures the mobility SAs for an HA.
ip mobile secure host	Configures the mobility SAs for a mobile host.
ip mobile secure mn-aaa	Specifies non-standard SPI values in the MN-AAA authentication extension that need to be accepted by the home agent or the foreign agent.

Command	Description
ip mobile secure proxy-host	Configures the mobility SAs for a proxy host.
ip mobile secure visitor	Configures the mobility SAs for a visitor.

ip mobile secure foreign-agent

To specify the mobility security associations (SAs) for a foreign agent (FA), use the **ip mobile secure foreign-agent** command in global configuration mode. To remove the mobility SAs, use the **no** form of this command.

ip mobile secure foreign-agent *lower-address* [*upper-address*] {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix** | **hmac-md5**}]

no ip mobile secure foreign-agent *lower-address* [*upper-address*] {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix** | **hmac-md5**}]

Syntax Description

lower-address	IP address of a FA or lower range of IP address pool. • *upper-address*—(Optional) Upper range of IP address pool. If specified, SAs for multiple FAs are configured. **Note** The *upper-address* value must be greater than the *lower-address* value.
inbound-spi	Bidirectional 4-byte security parameter index (SPI) used for authenticating inbound registration packets. • *spi-in*—Index for inbound registration packets. The range is from 100 to ffffffff.
outbound-spi	SPI used for calculating the authenticator in outbound registration packets. • *spi-out*—Index for outbound registration packets. The range is from 100 to ffffffff.
spi	SPI authenticates a peer. The argument and keyword are as follows: • *hex-value*—SPI expressed as a hexadecimal. The range is from 100 to ffffffff. **Note** Cisco recommends that you use hexadecimal values instead of decimal values for interoperability. • **decimal**—Decimal SPI. The argument is as follows: – *decimal-value*—SPI expressed as a decimal number. The range is from 256 to 4294967295.
key	Security key. The arguments and keywords are as follows: • **ascii** *string*—Security key expressed as an ASCII string. A maximum of 32 characters is allowed. No spaces are allowed. • **hex** *string*—Security key expressed in hexadecimal digits. A maximum of 32 hex digits is allowed. The range is from 100 to ffffffff. No spaces are allowed.

replay timestamp	(Optional) Specifies the number of seconds that the router uses for replay protection. • *seconds*—Time, in seconds, that a router uses for replay protection. The range is from plus or minus 255. The default is plus or minus 7. **Note** The registration packet is considered "not replayed" if the time stamp in the packet is within plus or minus the configured number of seconds of the router clock.
algorithm	(Optional) Algorithm used to authenticate messages during registration. The keywords are as follows: • **md5 mode**—Message Digest 5 (MD5) mode used to authenticate packets during registration. • **prefix-suffix**—Wrapped registration information for authentication (for example, key registration information key) that calculates the message digest. **Note** Cisco no longer recommends this method of authentication, but it is retained for backward compatibility. • **hmac-md5**—Hash-based Message Authentication Code (HMAC) MD5. **Note** The HMAC-MD5 authentication algorithm or MD5 (prefix-suffix) authentication algorithm is mandatory for mobile-home authentication (MHAE), mobile-foreign authentication (MFAE), or foreign-home authentication (FHAE).

Defaults

No SA is specified for FAs.

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(13)T	The **hmac-md5** keyword was added.

Usage Guidelines

The SA consists of an entity address, SPI, key, replay protection method, authentication algorithm, and authentication algorithm mode (prefix-suffix).

On a FA, the SA of the visiting mobile host and the SA of the home agent (HA) are optional. Multiple SAs for each entity can be configured.

The SA of a visiting mobile host on the MFAE and the SA of the HA on the FHAE are optional on the FA as long as they are not specified on the other entity. Multiple SAs for each entity can be configured.

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

Examples

The following example shows the configuration of SAs for an FA with an IP address of 209.165.200/254:

```
ip mobile secure foreign-agent 209.165.200/254 inbound-spi 203 outbound-spi 150 key
hex ffffffff
```

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.
ip mobile secure aaa-download	Configures the rate at which AAA security associations are downloaded.
ip mobile secure home-agent	Configures the mobility SAs for an HA.
ip mobile secure host	Configures the mobility SAs for a mobile host.
ip mobile secure mn-aaa	Specifies non-standard SPI values in the MN-AAA authentication extension that need to be accepted by the home agent or the foreign agent.
ip mobile secure proxy-host	Configures the mobility SAs for a proxy host.
ip mobile secure visitor	Configures the mobility SAs for a visitor.

ip mobile secure home-agent

To specify the mobility security associations (SAs) for a home agent (HA), use the **ip mobile secure home-agent** command in global configuration mode. To remove the mobility SAs, use the **no** form of this command.

ip mobile secure home-agent *lower-address* [*upper-address*] {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix** | **hmac-md5**}]

no ip mobile secure home-agent *lower-address* [*upper-address*] {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix** | **hmac-md5**}]

Syntax Description

lower-address	IP address of an HA or lower range of IP address pool. • *upper-address*—(Optional) Upper range of IP address pool. If specified, SAs for multiple HAs are configured. **Note** The *upper-address* value must be greater than the *lower-address* value.
inbound-spi	Bidirectional 4-byte security parameter index (SPI) used for authenticating inbound registration packets. • *spi-in*—Index for inbound registration packets. The range is from 100 to ffffffff.
outbound-spi	SPI used for calculating the authenticator in outbound registration packets. • *spi-out*—Index for outbound registration packets. The range is from 100 to ffffffff.
spi	SPI authenticates a peer. The argument and keyword are as follows: • *hex-value*—SPI expressed as a hexadecimal. The range is from 100 to ffffffff. **Note** Cisco recommends that you use hexadecimal values instead of decimal values for interoperability. • **decimal**—Decimal SPI. The argument is as follows: – *decimal-value*—SPI expressed as a decimal number. The range is from 256 to 4294967295.
key	Security key. The arguments and keywords are as follows: • **ascii** *string*—Security key expressed as an ASCII string. A maximum of 32 characters is allowed. No spaces are allowed. • **hex** *string*—Security key expressed in hexadecimal digits. A maximum of 32 hex digits is allowed. The range is from 100 to ffffffff. No spaces are allowed.

replay timestamp	(Optional) Specifies the number of seconds that the router uses for replay protection. • *seconds*—Time, in seconds, that a router uses for replay protection. The range is from plus or minus 255. The default is plus or minus 7. **Note** The registration packet is considered "not replayed" if the time stamp in the packet is within plus or minus the configured number of seconds of the router clock.
algorithm	(Optional) Algorithm used to authenticate messages during registration. The keywords are as follows: • **md5 mode**—Message Digest 5 (MD5) mode used to authenticate packets during registration. • **prefix-suffix**—Wrapped registration information for authentication (for example, key registration information key) that calculates the message digest. **Note** Cisco no longer recommends this method of authentication, but it is retained for backward compatibility. • **hmac-md5**—Hash-based Message Authentication Code (HMAC) MD5. **Note** The HMAC-MD5 authentication algorithm or MD5 (prefix-suffix) authentication algorithm is mandatory for mobile-home authentication (MHAE), mobile-foreign authentication (MFAE), or foreign-home authentication (FHAE).

Defaults

No SA is specified for HAs.

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(13)T	The **hmac-md5** keyword was added.

Usage Guidelines

The SA consists of an entity address, SPI, key, replay protection method, authentication algorithm, and authentication algorithm mode (prefix-suffix).

The HA may have multiple SAs for each peer. The SPI specifies which SA to use for the peer and selects the specific security parameters to be used to authenticate the peer.

On an HA, the SA of the mobile host is mandatory for mobile host authentication and allows the HA to compute the MHAE for mobile host authentication. If desired, configure a foreign agent (FA) SA on your HA.

The mobile IP protocol automatically synchronizes the time stamp used by the mobile node (MN) in its registration requests. If the MN registration request time stamp is outside the HA permitted replay protection time interval, the HA will respond with the number of seconds by which the MN time stamp is off relative to the HA clock. This allows the MN to adjust its time stamp and use synchronized time stamps in subsequent registration attempts.

If you prefer that the MN first registration attempt always falls within the HA replay protection time interval, use Network Time Protocol (NTP) to synchronize the MN and HA.

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

Examples

The following example shows the configuration of an SA for an HA with an IP address of 10.0.0.4:

```
ip mobile secure home-agent 10.0.0.4 spi 100 key hex ffffffff
```

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.
ip mobile secure aaa-download	Configures the rate at which AAA security associations are downloaded.
ip mobile secure foreign-agent	Configures the mobility SAs for an FA.
ip mobile secure host	Configures the mobility SAs for a mobile host.
ip mobile secure mn-aaa	Specifies non-standard SPI values in the MN-AAA authentication extension that need to be accepted by the home agent or the foreign agent.
ip mobile secure proxy-host	Configures the mobility SAs for a proxy host.
ip mobile secure visitor	Configures the mobility SAs for a visitor.

ip mobile secure host

To specify the mobility security associations (SAs) for a mobile host, use the **ip mobile secure host** command in global configuration mode. To remove the mobility SAs, use the **no** form of this command.

ip mobile secure host {*lower-address* [*upper-address*] | **nai** *nai-string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix** | **hmac-md5**}]

no ip mobile secure host {*lower-address* [*upper-address*] | **nai** *nai-string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix** | **hmac-md5**}]

Syntax Description

lower-address	IP address of a host or lower range of IP address pool. • *upper-address*—(Optional) Upper range of IP address pool. If specified, SAs for multiple hosts are configured. **Note** The *upper-address* value must be greater than the *lower-address* value.
nai	Network access identifier (NAI) of the mobile node (MN). • *nai-string*—NAI username or username@realm.
inbound-spi	Bidirectional 4-byte security parameter index (SPI) used for authenticating inbound registration packets. • *spi-in*—Index for inbound registration packets. The range is from 100 to ffffffff.
outbound-spi	SPI used for calculating the authenticator in outbound registration packets. • *spi-out*—Index for outbound registration packets. The range is from 100 to ffffffff.
spi	SPI authenticates a peer. The argument and keyword are as follows: • *hex-value*—SPI expressed as a hexadecimal. The range is from 100 to ffffffff. **Note** Cisco recommends that you use hexadecimal values instead of decimal values for interoperability. • **decimal**—Decimal SPI. The argument is as follows: – *decimal-value*—SPI expressed as a decimal number. The range is from 256 to 4294967295.
key	Security key. The arguments and keywords are as follows: • **ascii** *string*—Security key expressed as an ASCII string. A maximum of 32 characters is allowed. No spaces are allowed. • **hex** *string*—Security key expressed in hexadecimal digits. A maximum of 32 hex digits is allowed. The range is from 100 to ffffffff. No spaces are allowed.

replay timestamp	(Optional) Specifies the number of seconds that the router uses for replay protection. • *seconds*—Time, in seconds, that a router uses for replay protection. The range is from plus or minus 255. The default is plus or minus 7. **Note** The registration packet is considered "not replayed" if the time stamp in the packet is within plus or minus the configured number of seconds of the router clock.
algorithm	(Optional) Algorithm used to authenticate messages during registration. The keywords are as follows: • **md5 mode**—Message Digest 5 (MD5) mode used to authenticate packets during registration. • **prefix-suffix**—Wrapped registration information for authentication (for example, key registration information key) that calculates the message digest. **Note** Cisco no longer recommends this method of authentication, but it is retained for backward compatibility. • **hmac-md5**—Hash-based Message Authentication Code (HMAC) MD5. **Note** The HMAC-MD5 authentication algorithm or MD5 (prefix-suffix) authentication algorithm is mandatory for mobile-home authentication (MHAE), mobile-foreign authentication (MFAE), or foreign-home authentication (FHAE).

Defaults

No SA is specified for mobile hosts.

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.

Usage Guidelines

The SA consists of an entity address, SPI, key, replay protection method, authentication algorithm, and authentication algorithm mode (prefix-suffix).

The SA of a visiting mobile host on the MFAE and the SA of the home agent (HA) on the FHAE are optional as long as they are not specified on the other entity. Multiple SAs for each entity can be configured.

The HMAC-MD5 authentication algorithm is mandatory for MHAE, MFAE, and FHAE.

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

Examples

The following example shows the configuration of an SA for a host:

```
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.
ip mobile secure aaa-download	Configures the rate at which AAA security associations are downloaded.
ip mobile secure foreign-agent	Configures the mobility SAs for an FA.
ip mobile secure home-agent	Configures the mobility SAs for an HA.
ip mobile secure mn-aaa	Specifies non-standard SPI values in the MN-AAA authentication extension that need to be accepted by the home agent or the foreign agent.
ip mobile secure proxy-host	Configures the mobility SAs for a proxy host.
ip mobile secure visitor	Configures the mobility SAs for a visitor.

ip mobile secure mn-aaa

To specify non-standard security parameter index (SPI) values in the MN-AAA authentication extension that need to be accepted by the home agent or the foreign agent, use the **ip mobile secure mn-aaa** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip mobile secure mn-aaa spi {*hex-value* | **decimal** *decimal-value*} **algorithm md5 mode ppp-chap-style**

no ip mobile secure mn-aaa spi {*hex-value* | **decimal** *decimal-value*} **algorithm md5 mode ppp-chap-style**

Syntax Description

spi	Bidirectional security parameter index (SPI). The index can be a hexadecimal or decimal value. The arguments and keyword are as follows: • *hex-value*—SPI expressed in hexadecimal digits. The range is from 100 to ffffffff. No spaces are allowed. The maximum is 32 characters. • **decimal** *decimal-value*—SPI expressed as a decimal number. The range is from 256 to 4294967295. No spaces are allowed. The maximum is 32 characters.
algorithm md5 mode ppp-chap-style	Message Digest 5 (MD5) authentication algorithm used during authentication by the Challenge-Handshake Authentication Protocol (CHAP).

Defaults

The home agent or foreign agent only accept the standard SPI value in the MN-AAA authentication extension that specifes CHAP-style authentication using MD5. The standard value for the SPI is 2.

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

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.

A mobile node configured to be authenticated via an MN-AAA authentication extension is required to use an SPI value of 2 to indicate CHAP-style authentication using MD5 as specified by RFC 3012, *Mobile IPv4 Challenge/Response Extensions.*

Some network implementations need the flexibility to allow an SPI value other than 2 even though the mobile node is authenticated using CHAP. The **ip mobile secure mn-aaa** command maps new SPI values in the MN-AAA extension of the registration message to the SPI value pre-defined by RFC 3012. When a registration request arrives at the foreign agent or home agent with the MN-AAA extension containing an SPI value specified by the **ip mobile secure mn-aaa** command, the foreign agent or home agent will process it as if the value was 2 instead of rejecting the request.

Use this command with caution because it is non-standard behavior. For example, different vendors might use the same non-standard SPI to denote different authentication methods and this could affect interoperability. In general, Cisco recommends the use of standard SPI values to be used in the MN-AAA authentication extension by the mobile node.

Examples

In the following example, the foreign agent or home agent will process the registration request even though the CHAP SPI value is not 2:

```
ip mobile secure mn-aaa spi 1234 algorithm md5 mode ppp-chap-style
```

ip mobile secure proxy-host

To specify the mobility security associations (SAs) for a proxy host, use the **ip mobile secure proxy-host** command in global configuration mode. To remove the mobility SAs, use the **no** form of this command.

ip mobile secure proxy-host {*lower-address* [*upper-address*] | **nai** *nai-string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix** | **hmac-md5**}]

no ip mobile secure proxy-host {*lower-address* [*upper-address*] | **nai** *nai-string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix** | **hmac-md5**}]

Syntax Description

lower-address	IP address of a proxy host or lower range of IP address pool. • *upper-address*—(Optional) Upper range of IP address pool. If specified, SAs for multiple proxy hosts are configured. **Note** The *upper-address* value must be greater than the *lower-address* value.
nai	Network access identifier (NAI) of the mobile node (MN). • *nai-string*—NAI username or username@realm.
inbound-spi	Bidirectional 4-byte security parameter index (SPI) used for authenticating inbound registration packets. • *spi-in*—Index for inbound registration packets. The range is from 100 to ffffffff.
outbound-spi	SPI used for calculating the authenticator in outbound registration packets. • *spi-out*—Index for outbound registration packets. The range is from 100 to ffffffff.
spi	SPI authenticates a peer. The argument and keyword are as follows: • *hex-value*—SPI expressed as a hexadecimal. The range is from 100 to ffffffff. **Note** Cisco recommends that you use hexadecimal values instead of decimal values for interoperability. • **decimal**—Decimal SPI. The argument is as follows: – *decimal-value*—SPI expressed as a decimal number. The range is from 256 to 4294967295.
key	Security key. The arguments and keywords are as follows: • **ascii** *string*—Security key expressed as an ASCII string. A maximum of 32 characters is allowed. No spaces are allowed. • **hex** *string*—Security key expressed in hexadecimal digits. A maximum of 32 hex digits is allowed. The range is from 100 to ffffffff. No spaces are allowed.

replay timestamp	(Optional) Specifies the number of seconds that the router uses for replay protection. • *seconds*—Time that a router uses for replay protection. The range is from plus or minus 255 seconds. The default is plus or minus 7 seconds. **Note** The registration packet is considered "not replayed" if the time stamp in the packet is within plus or minus the configured number of seconds of the router clock.
algorithm	(Optional) Algorithm used to authenticate messages during registration. The keywords are as follows: • **md5 mode**—Message Digest 5 (MD5) mode used to authenticate packets during registration. • **prefix-suffix**—Wrapped registration information for authentication (for example, key registration information key) that calculates the message digest. **Note** Cisco no longer recommends this method of authentication, but it is retained for backward compatibility. • **hmac-md5**—Hash-based Message Authentication Code (HMAC) MD5. **Note** The HMAC-MD5 authentication algorithm or MD5 (prefix-suffix) authentication algorithm is mandatory for mobile-home authentication (MHAE), mobile-foreign authentication (MFAE), or foreign-home authentication (FHAE).

Defaults

No SA is specified for proxy hosts.

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.
12.3(4)T	The **proxy-host** keyword was added for Packet Data Serving Node (PDSN) platforms only.

Usage Guidelines

The SA consists of an entity address, SPI, key, replay protection method, authentication algorithm, and authentication algorithm mode (prefix-suffix).

The HMAC-MD5 authentication algorithm is mandatory for MHAE, MFAE, and FHAE.

Note The **proxy-host** keyword is available only on PDSN platforms that are running specific PDSN code images; consult Cisco 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 the configuration of an SA for a proxy host:

```
ip mobile secure proxy-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.
ip mobile secure aaa-download	Configures the rate at which AAA security associations are downloaded.
ip mobile secure foreign-agent	Configures the mobility SAs for an FA.
ip mobile secure home-agent	Configures the mobility SAs for an HA.
ip mobile secure host	Configures the mobility SAs for a mobile host.
ip mobile secure mn-aaa	Specifies non-standard SPI values in the MN-AAA authentication extension that need to be accepted by the home agent or the foreign agent.
ip mobile secure visitor	Configures the mobility SAs for a visitor.
ntp server	Allows the system clock to be synchronized by a time server.
show ip mobile secure	Displays the mobility SAs for a mobile host, mobile visitor, FA, or HA.

ip mobile secure visitor

To specify the mobility security associations (SAs) for a visitor, use the **ip mobile secure visitor** command in global configuration mode. To remove the mobility security associations, use the **no** form of this command.

ip mobile secure visitor {*lower-address* [*upper-address*] | **nai** *nai-string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix** | **hmac-md5**}]

no ip mobile secure visitor {*lower-address* [*upper-address*] | **nai** *nai-string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix** | **hmac-md5**}]

Syntax Description

lower-address	IP address of a visitor or lower range of IP address pool. • *upper-address*—(Optional) Upper range of IP address pool. If specified, SAs for multiple visitors are configured. **Note** The *upper-address* value must be greater than the *lower-address* value.
nai	Network access identifier (NAI) of the mobile node (MN). • *nai-string*—NAI username or username@realm.
inbound-spi	Bidirectional 4-byte security parameter index (SPI) used for authenticating inbound registration packets. • *spi-in*—Index for inbound registration packets. The range is from 100 to ffffffff.
outbound-spi	SPI used for calculating the authenticator in outbound registration packets. • *spi-out*—Index for outbound registration packets. The range is from 100 to ffffffff.
spi	SPI authenticates a peer. The argument and keyword are as follows: • *hex-value*—SPI expressed as a hexadecimal. The range is from 100 to ffffffff. **Note** Cisco recommends that you use hexadecimal values instead of decimal values for interoperability. • **decimal**—Decimal SPI. The argument is as follows: – *decimal-value*—SPI expressed as a decimal number. The range is from 256 to 4294967295.
key	Security key. The arguments and keywords are as follows: • **ascii** *string*—Security key expressed as an ASCII string. A maximum of 32 characters is allowed. No spaces are allowed. • **hex** *string*—Security key expressed in hexadecimal digits. A maximum of 32 hex digits is allowed. The range is from 100 to ffffffff. No spaces are allowed.

replay timestamp	(Optional) Specifies the number of seconds that the router uses for replay protection. • *seconds*—Time, in seconds, that a router uses for replay protection. The range is from plus or minus 255. The default is plus or minus 7. **Note** The registration packet is considered "not replayed" if the time stamp in the packet is within plus or minus the configured number of seconds of the router clock.
algorithm	(Optional) Algorithm used to authenticate messages during registration. The keywords are as follows: • **md5 mode**—Message Digest 5 (MD5) mode used to authenticate packets during registration. • **prefix-suffix**—Wrapped registration information for authentication (for example, key registration information key) that calculates the message digest. **Note** Cisco no longer recommends this method of authentication, but it is retained for backward compatibility. • **hmac-md5**—Hash-based Message Authentication Code (HMAC) MD5. **Note** The HMAC-MD5 authentication algorithm or MD5 (prefix-suffix) authentication algorithm is mandatory for mobile-home authentication (MHAE), mobile-foreign authentication (MFAE), or foreign-home authentication (FHAE).

Defaults

No SA is specified for visitors.

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.

Usage Guidelines

The SA consists of an entity address, SPI, key, replay protection method, authentication algorithm, and authentication algorithm mode (prefix-suffix).

The SA of a visiting mobile host on the MFAE and the SA of the home agent (HA) on the FHAE are optional as long as they are not specified on the other entity. Multiple SAs for each entity can be configured.

The Mobile IP protocol automatically synchronizes the time stamp used by the MN in its registration requests. If the MN registration request time stamp is outside the visitor permitted replay protection time interval, the visitor will respond with the number of seconds the MN time stamp is off relative to the visitor clock. This allows the MN to adjust its time stamp and use synchronized time stamps in subsequent registration attempts.

If you prefer that the MN first registration attempt always fall within the visitor replay protection time interval, use Network Time Protocol (NTP) to synchronize the MN and visitor.

The HMAC-MD5 authentication algorithm is mandatory for MHAE, MFAE, and FHAE.

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

Examples

The following example shows the configuration of an SA for a visitor:

```
ip mobile secure visitor 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.
ip mobile secure aaa-download	Configures the rate at which AAA security associations are downloaded.
ip mobile secure foreign-agent	Configures the mobility SAs for an FA.
ip mobile secure home-agent	Configures the mobility SAs for an HA.
ip mobile secure host	Configures the mobility SAs for a mobile host.
ip mobile secure mn-aaa	Specifies non-standard SPI values in the MN-AAA authentication extension that need to be accepted by the home agent or the foreign agent.
ip mobile secure proxy-host	Configures the mobility SAs for a proxy host.
ntp server	Allows the system clock to be synchronized by a time server.
show ip mobile secure	Displays the mobility SAs for a mobile host, mobile visitor, FA, or HA.

ip mobile tunnel

To specify the settings of tunnels created by Mobile IP, use the **ip mobile tunnel** global configuration command.

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

Syntax Description

route-cache	Sets tunnels to default or process switching mode.
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.

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 following keywords were added: • **nat** • **inside** • **outside**

Usage Guidelines

Path MTU Discovery is used by end stations to find a packet size that does not need fragmentation between them. 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.

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
show ip mobile tunnel	Displays active tunnels.

ip mobile virtual-network

To define a virtual network, use the **ip mobile virtual-network** global configuration command. 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 following keyword and argument were added: • **address** • *address*

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 addr 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 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.

router mobile

To enable Mobile IP on the router, use the **router mobile** global configuration command. 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, use the **show ip mobile binding** EXEC command.

show ip mobile binding [**home-agent** *address* | **summary**]

Syntax Description

home-agent *address*	(Optional) IP address of mobile node.
summary	(Optional) Total number of bindings in the table.

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.

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
20.0.0.1:
    Care-of Addr 68.0.0.31, Src Addr 68.0.0.31,
    Lifetime granted 02:46:40 (10000), remaining 02:46:32
    Flags SbdmGvt, Identification B750FAC4.C28F56A8,
    Tunnel100 src 66.0.0.5 dest 68.0.0.31 reverse-allowed
    Routing Options - (G)GRE
```

Table 45 describes the significant fields shown in the display.

Table 45 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.

Table 45 show ip mobile binding Field Descriptions (continued)

Field	Description
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 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. See Table 41 for a description of each bit.
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** EXEC command.

show ip mobile globals

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

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

Usage Guidelines

This command shows the services provided by the home agent or foreign agent. Note the deviation from RFC 2006: 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 in this chapter), 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
    Virtual networks
        20.0.0.0/8

Foreign Agent is not enabled, no care-of address

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

Table 46 describes the significant fields shown in the display.

Table 46 show ip mobile globals Field Descriptions

Field	Description
Home Agent	
Registration lifetime	Default lifetime 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	Broadcast enabled or disabled.
Reverse tunnel	Reverse tunnel enabled or disabled.
ICMP Unreachable	Sends ICMP unreachable messages, which are enabled or disabled for virtual network.
Virtual networks	Lists virtual networks serviced by the home agent. Displayed if defined.
Foreign Agent	
Care-of addresses advertised	Lists care-of addresses (interface is up or down). Displayed if defined.
Mobility Agent	
Number of interfaces providing service	See the **show ip mobile interface** command for more information on advertising. Agent advertisements are sent when IRDP is enabled.
Encapsulations supported	IPIP and GRE.
Tunnel fast switching	Tunnel fast switching is enabled or disabled.
Discovered tunnel MTU	Aged out after amount of time.

show ip mobile host

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

show ip mobile host [*address* | **interface** *interface* | **network** *address* | **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) All mobile nodes whose home network is on this interface.
network *address*	(Optional) All mobile nodes residing on this network or virtual network.
group	(Optional) All mobile node groups configured using the **ip mobile host** command.
summary	(Optional) All values in the table.

Command Modes

EXEC

Command History

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

Examples

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

```
Router# show ip mobile host

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
```

Table 47 describes the significant fields shown in the display.

Table 47 show ip mobile host Field Descriptions

Field	Description
<IP address>	Home IP address of the mobile node.
Allowed lifetime	Allowed lifetime 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.

Table 47 show ip mobile host Field Descriptions (continued)

Field	Description
Home link	Interface or virtual network.
Accepted	Total number of service requests for the mobile node accepted by the home agent (Code 0 + Code 1).
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 home agent last rebooted.
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). See Table 41 for a list of codes.
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 MN	Number of packets and bytes tunneled to mobile node.
Reverse tunnel from MN	Number of packets and bytes reverse tunneled from mobile node.

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 48 describes the significant fields shown in the display.

Table 48 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
show ip mobile binding	Displays the mobility binding table.

show ip mobile interface

To display advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes, use the **show ip mobile interface** EXEC command.

show ip mobile interface [*interface*]

Syntax Description

interface	(Optional) IP address of mobile node. If not specified, all interfaces are shown.

Command Modes

EXEC

Command History

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

Examples

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

```
Router# show ip mobile interface

IP Mobility interface information:
IRDP disabled
Interface Ethernet3:
    Prefix Length not advertised
    Lifetime is 36000 seconds
    Home Agent service provided
```

Table 49 describes the significant fields shown in the display.

Table 49 show ip mobile interface Field Descriptions

Field	Description
Interface	Name of the interface.
IRDP	IRDP (includes agent advertisement) enabled or disabled. IRDP must be enabled for an advertisement to be sent out. Use the **ip irdp** command to enable IRDP.
Prefix Length	Prefix-length extension to be included or not in the advertisement.
Lifetime	Advertised registration lifetime.
Home Agent service provided	Displayed if home agent service is enabled on the interface.
Foreign Agent service provided	Displayed if foreign agent service is enabled on the interface.
Registration required	Foreign agent requires registration even from those mobile nodes that have acquired their own, colocated care-of address.
Busy	Foreign agent is busy for this interface.
Home Agent access list	Which home agent is allowed.

Table 49 show ip mobile interface Field Descriptions (continued)

Field	Description
Maximum number of visitors allowed	Displayed if defined.
Current number of visitors	Number of visitors on interface.

Related Commands

Command	Description
ip mobile foreign-agent	Enables foreign agent service.
ip mobile host	Configures the mobile host or mobile node group.
ip mobile prefix-length	Appends the prefix-length extension to the advertisement.
show ip irdp	Displays IRDP values.

show ip mobile secure

To display the mobility security associations for the mobile host, mobile visitor, foreign agent, or home agent, use the **show ip mobile secure** EXEC command.

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

Syntax Description

host	Security association of the mobile host on the home agent.
visitor	Security association of the mobile visitor on the foreign agent.
foreign-agent	Security association of the remote foreign agents on the home agent.
home-agent	Security association of the remote home agent on the foreign agent.
summary	All values in the table.
address	IP address.

Command Modes

EXEC

Command History

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

Usage Guidelines

Multiple security associations can exist for each entity.

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):
20.0.0.6
    SPI 300,  MD5, Prefix-suffix, Timestamp +/- 7,
    Key 00112233445566778899001122334455
```

Table 50 describes the significant fields shown in the display.

Table 50 show ip mobile secure Field Descriptions

Field	Description
20.0.0.6	IP address.
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.

Table 50 show ip mobile secure Field Descriptions (continued)

Field	Description
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** EXEC command.

show ip mobile traffic

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

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

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:
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
    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
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
    Replies in 0
    Forwarded 0, Bad 0, Ignored 0
    Authentication failed MN 0, HA 0
```

Table 51 describes the significant fields shown in the display.

Table 51 show ip mobile traffic Field Descriptions

Field	Description
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).
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).
Unavailable reverse tunnel	Total number of Registration Requests denied by the home agent—reverse tunnel unavailable (Code 137).

Table 51 show ip mobile traffic Field Descriptions (continued)

Field	Description
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.
Foreign Agent	
Request in	Total number of Registration Requests received by the foreign agent.
Forwarded	Total number of Registration Requests relayed to 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).
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).
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.

Table 51 show ip mobile traffic Field Descriptions (continued)

Field	Description
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).

show ip mobile tunnel

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

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.

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 68.0.0.32, dest 68.0.0.48
    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
```

Table 52 describes the significant fields shown in the display.

Table 52 show ip mobile tunnel Field Descriptions

Field	Description
src	Tunnel source IP address.
dest	Tunnel destination IP address.
encap	Tunnel encapsulation type.
mode	Either reverse-allowed or reverse-off for reverse tunnel mode.
tunnel-users	Number of users on tunnel.
HA created	Home agent created.
fast switching	Enabled or disabled.

Table 52 show ip mobile tunnel Field Descriptions (continued)

Field	Description
ICMP unreachable	Enabled or disabled.
packets input	Number of packets in.
bytes	Number of bytes in.
0 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 deencapsulated packets back to the home agent.
packets output	Number of packets output.
bytes	Number of bytes output.

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 of the visitor list of the foreign agent.

show ip mobile violation

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

show ip mobile violation [*address*]

Syntax Description

address	(Optional) Displays violations from a specific IP address.

Command Modes

EXEC

Command History

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

Usage Guidelines

The most recent violation is saved for all the mobile nodes. A circular log holds up to 50 unknown requesters, violators without security association. 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 53 describes significant fields shown in the display.

Table 53 show ip mobile violation Field Descriptions

Field	Description
20.0.0.1	IP address of the violator.
Violations	Total number of security violations for this peer.
Last time	Time of the most recent security violation for this peer.
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.

Table 53 show ip mobile violation Field Descriptions (continued)

Field	Description
Identification	Identification used in request or reply of the most recent security violation for this peer.
Error Code	Error code in request or reply. See Table 51 for list of error codes.
Reason	Reason for the most recent security violation for this peer. Possible reasons are: • No mobility security association • Bad authenticator • Bad identifier • Bad SPI • Missing security extension • Other

show ip mobile visitor

To display the table containing the visitor list of the foreign agent, use the **show ip mobile visitor** EXEC command.

show ip mobile visitor [**pending**] [*address* | **summary**]

Syntax Description

pending	(Optional) Pending registration table.
address	(Optional) IP address.
summary	(Optional) All values in the table.

Command Modes

EXEC

Command History

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

Usage Guidelines

The foreign agent updates the table containing the visitor list of the foreign agent in response to registration events from mobile nodes.

Examples

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

```
Router# show ip mobile visitor
Mobile Visitor List:
Total 1
20.0.0.1:
    Interface Ethernet1/2, MAC addr 0060.837b.95ec
    IP src 20.0.0.1, dest 67.0.0.31, UDP src port 434
    HA addr 66.0.0.5, Identification B7510E60.64436B38
    Lifetime 08:20:00 (30000) Remaining 08:19:16
    Tunnel100 src 68.0.0.31, dest 66.0.0.5, reverse-allowed
    Routing Options - (T)Reverse-tunnel
```

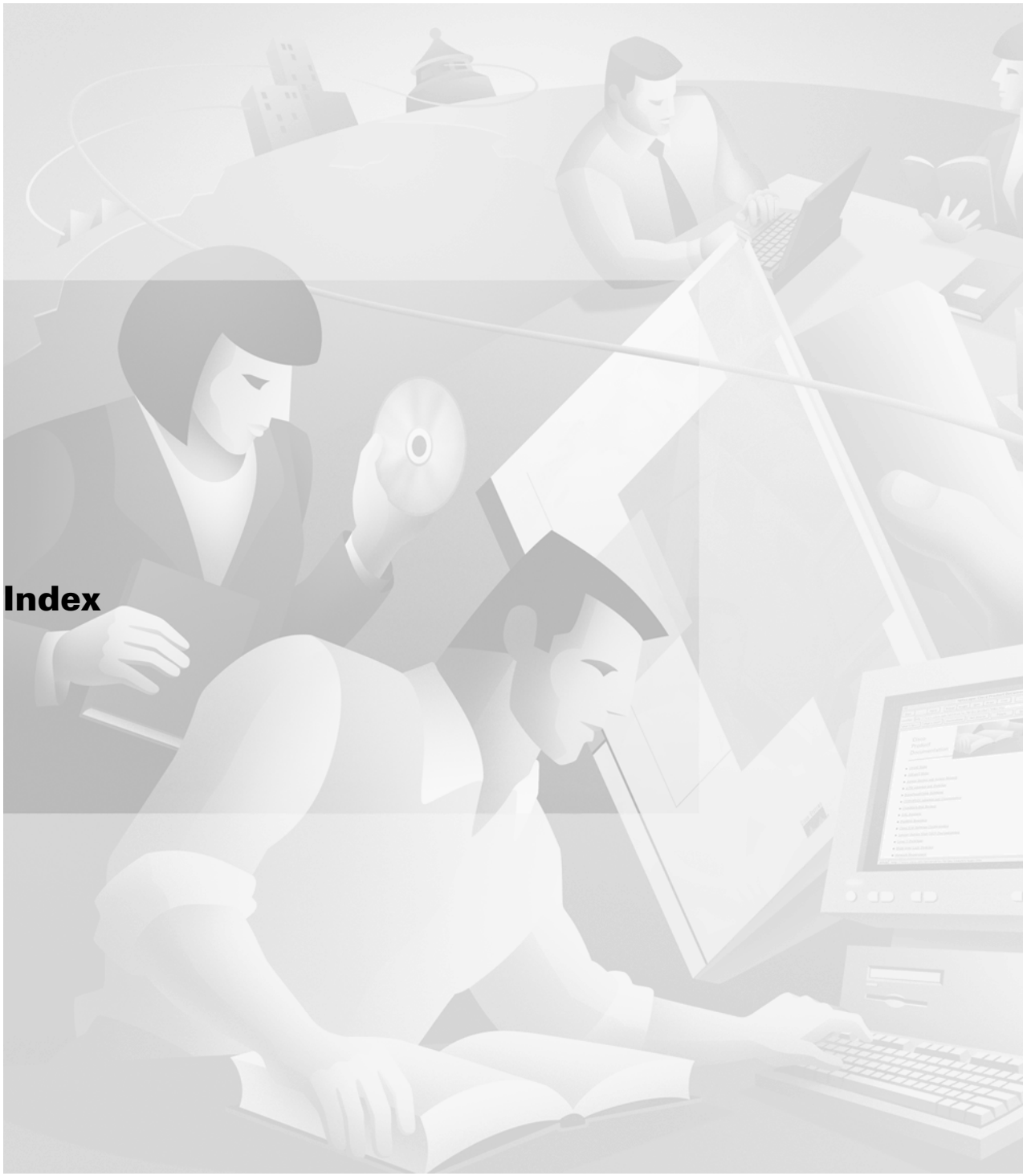
Table 54 describes the significant fields shown in the display.

Table 54 show ip mobile visitor Field Descriptions

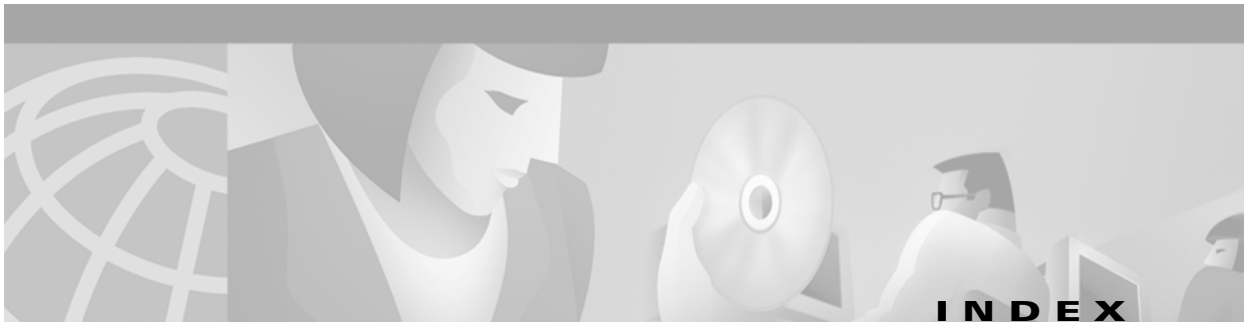
Field	Description
Total	1
20.0.0.1	Home IP address of a visitor.
Interface	Name of the interface.
MAC addr	MAC address of the visitor.
IP src	Source IP address the Registration Request of a visitor.

Table 54 show ip mobile visitor Field Descriptions (continued)

Field	Description
IP dest	Destination IP address of Registration Request of a visitor. When a foreign agent sends a reply to a visitor, the IP source address is set to this address, unless it is multicast or broadcast, in which case it is set to IP address of the output interface.
UDP src port	Source UDP port of Registration Request of the visitor.
HA addr	Home agent IP address for that visiting mobile node.
Identification	Identification used in that registration by the mobile node.
Lifetime	The lifetime granted to the mobile node for this registration.
Remaining	The number of seconds remaining until the registration is expired. It has the same initial value as in the Lifetime field, and is counted down by the foreign agent.
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 foreign agent-accepted services, based on registration flags sent by the mobile node. Possible options are: • (S) Mult-binding • (B) Broadcast • (D) Direct-to-MN • (M) MinIP • (G) GRE • (V) VJH-compress • (T) Reverse-tunnel



Index



Symbols

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W