



Cisco IOS Command Summary Volume 1 of 3

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-7811756=
Text Part Number: 78-11756-01

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

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

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

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

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

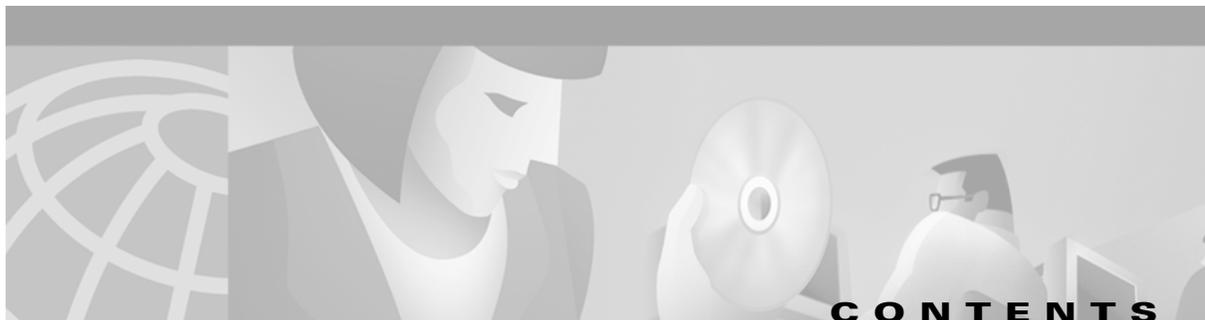
AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Unity, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, and Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, PIX, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0108R)

Cisco IOS Command Summary, Volume 1 of 3

Copyright © 2001, Cisco Systems, Inc.

All rights reserved.



About Cisco IOS Software Documentation vii

Using Cisco IOS Software xvii

Configuration Fundamentals

Basic Command-Line Interface Commands CS1-3

The Setup Command CS1-11

Terminal Operating Characteristics Commands CS1-13

Connection, Menu, and System Banner Commands CS1-33

Cisco IOS Web Browser User Interface Commands CS1-43

Cisco IOS File System Commands CS1-47

Configuration File Management Commands CS1-55

System Image and Microcode Commands CS1-63

Router Memory Commands CS1-71

Booting Commands CS1-75

Basic File Transfer Services Commands CS1-83

Basic System Management Commands CS1-93

Troubleshooting and Fault Management Commands CS1-113

SNMP Commands CS1-139

CDP Commands CS1-157

RMON Commands CS1-161

Cisco Service Assurance Agent Commands CS1-169

WCCP Commands CS1-191

Cisco 7500 Series Line Card Configuration Commands CS1-197

IP: Addressing and Services

IP Addressing Commands CS1-203

DHCP Commands CS1-227

IP Services Commands CS1-241

Server Load Balancing Commands CS1-275

Mobile IP Commands CS1-287

IP: Routing Protocols

On-Demand Routing Commands CS1-299

RIP Commands CS1-301

IGRP Commands CS1-309

OSPF Commands CS1-315

Enhanced IGRP Commands CS1-335

Integrated IS-IS Commands CS1-345

BGP Commands CS1-357

Multiprotocol BGP Extensions for IP Multicast Commands CS1-391

IP Routing Protocol-Independent Commands CS1-395

IP: Multicast

IP Multicast Routing Commands CS1-415

Multicast Source Discovery Protocol Commands CS1-447

PGM Host and Router Assist Commands CS1-457

Unidirectional Link Routing Commands CS1-463

IP Multicast Tools Commands CS1-467

AppleTalk and Novell IPX

AppleTalk Commands: access-list additional-zones Through appletalk zone CS1-477

AppleTalk Commands: clear appletalk arp Through test appletalk CS1-503

Novell IPX Commands: access-list (IPX extended) Through ipx nlsr csnp-interval CS1-515

Novell IPX Commands: ipx nlsr enable Through spf-interval CS1-551

Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS

Apollo Domain Commands CS1-591

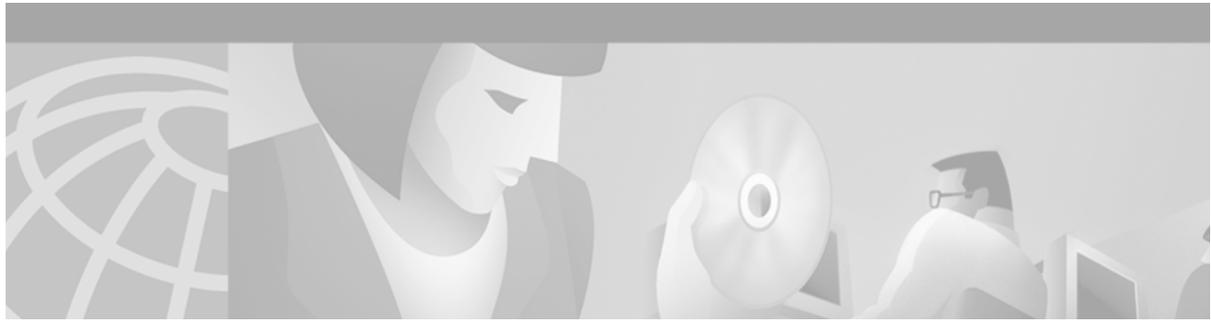
Banyan VINES Commands CS1-595

DECnet Commands CS1-613

ISO CLNS Commands CS1-633

XNS Commands CS1-673

Index



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.

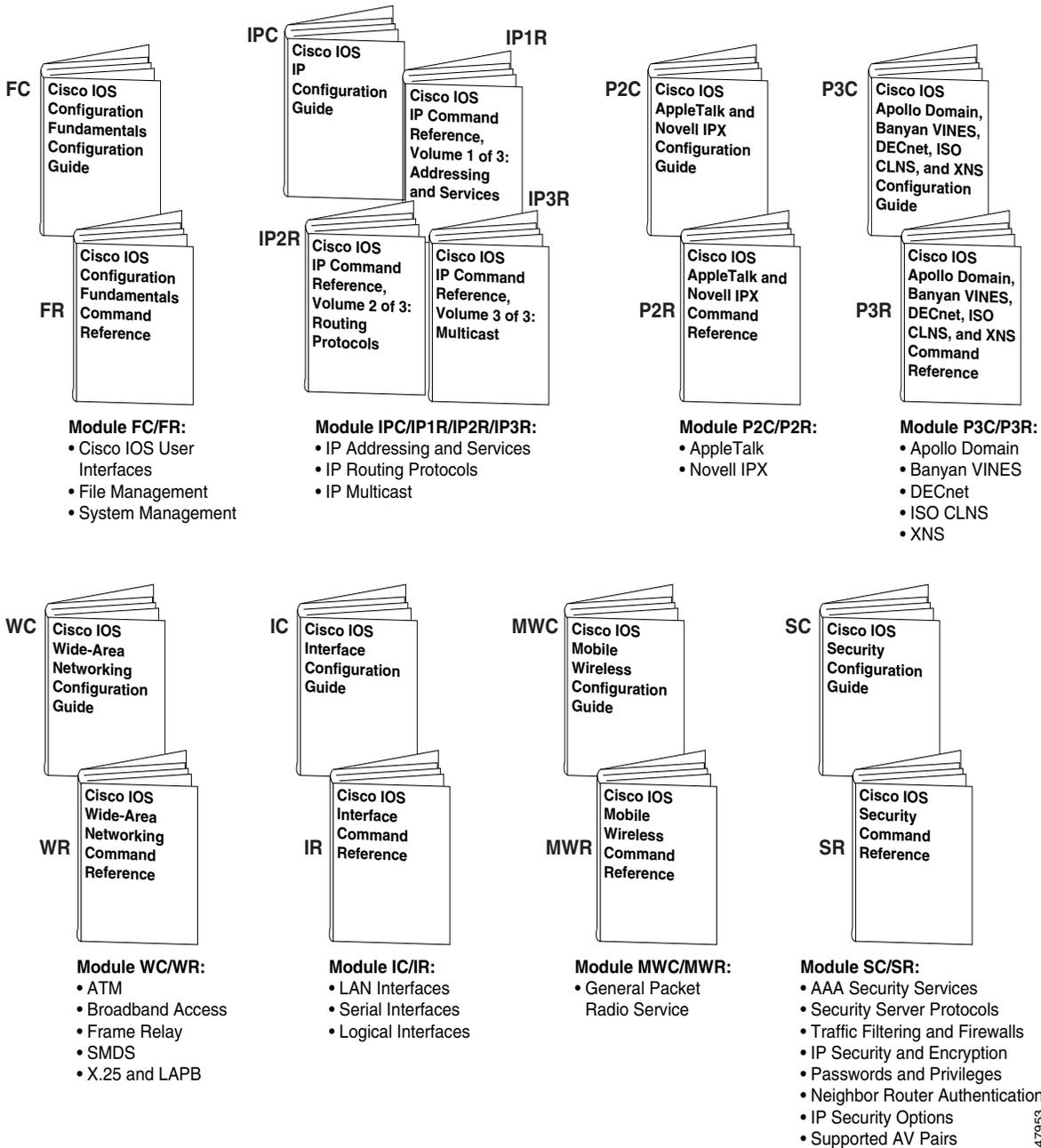
Figure 1 shows the Cisco IOS software documentation modules.



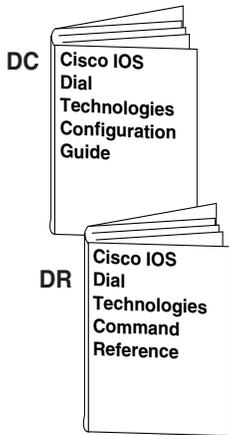
Note

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

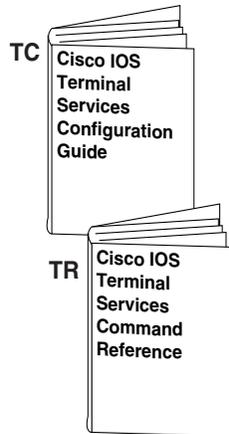


47953



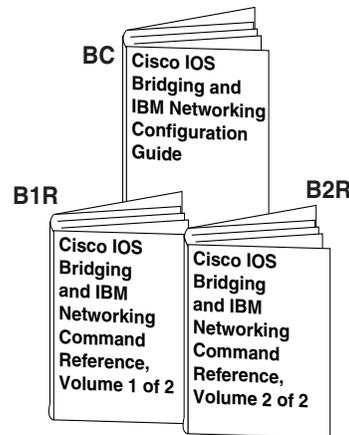
Module DC/DR:

- 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
- NAS1
- Telnet
- TN3270
- XRemote
- X.28 PAD
- Protocol Translation

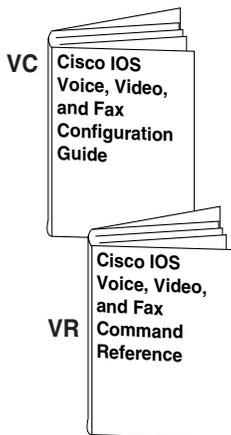


Module BC/B1R:

- 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

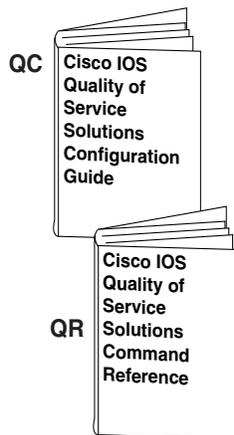
Module BC/B2R:

- 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



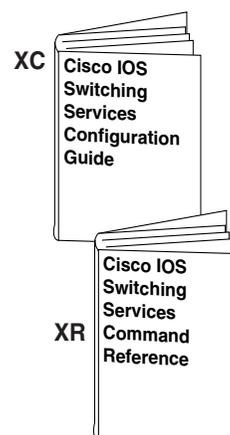
Module VC/VR:

- 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* (three 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

Since the last release, the *Cisco IOS Command Summary* has been expanded into three volumes.

Cisco IOS Command Summary, Volume 1 of 3 contains the following sections:

- Configuration Fundamentals
- IP: Addressing and Services
- IP: Routing Protocols
- IP: Multicast
- AppleTalk and Novell IPX
- Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS

Cisco IOS Command Summary, Volume 2 of 3 contains the following sections:

- Wide-Area Networking
- Security
- Interface
- Dial Technologies
- Terminal Services
- Switching Services

Cisco IOS Command Summary, Volume 3 of 3 contains the following sections:

- Bridging and IBM Networking, Volume 1 of 2
- Bridging and IBM Networking, Volume 2 of 2
- Quality of Service Solutions
- Voice, Video, and Fax
- Mobile Wireless

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.
<i>string</i>	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.
<i>italics</i>	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.
<i>abbreviated-command-entry?</i>	Provides a list of commands that begin with a particular character string. (No space between command and question mark.)
<i>abbreviated-command-entry<Tab></i>	Completes a partial command name.
?	Lists all commands available for a particular command mode.
<i>command ?</i>	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
<pre>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)#</pre>	<p>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.</p>
<pre>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</pre>	<p>Enter the command that you want to configure for the interface. This example uses the ip command.</p> <p>Enter ? to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.</p>

Table 2 How to Find Command Options (continued)

Command	Comment
<pre>Router(config-if)# ip address ? A.B.C.D IP address negotiated IP Address negotiated over PPP Router(config-if)# ip address</pre>	<p>Enter the command that you want to configure for the interface. This example uses the ip address command.</p> <p>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.</p> <p>A carriage return (<cr>) is not displayed; therefore, you must enter additional keywords or arguments to complete the command.</p>
<pre>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</pre>	<p>Enter the keyword or argument you want to use. This example uses the 172.16.0.1 IP address.</p> <p>Enter ? to display what you must enter next on the command line. In this example, you must enter an IP subnet mask.</p> <p>A <cr> is not displayed; therefore, you must enter additional keywords or arguments to complete the command.</p>
<pre>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</pre>	<p>Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask.</p> <p>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.</p> <p>A <cr> is displayed; you can press Enter to complete the command, or you can enter another keyword.</p>
<pre>Router(config-if)# ip address 172.16.0.1 255.255.255.0 Router(config-if)#</pre>	<p>In this example, Enter is pressed to complete the command.</p>

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.



Configuration Fundamentals



Basic Command-Line Interface Commands

This chapter describes the function and syntax of the basic command-line interface commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Configuration Fundamentals Command Reference*.

disable

To exit privileged EXEC mode and return to user EXEC mode, or to exit to a lower privilege level, enter the **disable** EXEC command.

disable [*privilege-level*]

Syntax Description

privilege-level (Optional) Specific privilege level (other than user EXEC mode).

editing

To reenable Cisco IOS enhanced editing features for a particular line after they have been disabled, use the **editing** line configuration command. To disable these features, use the **no** form of this command.

editing

no editing

Syntax Description

This command has no arguments or keywords.

enable

To enter privileged EXEC mode, or any other security level set by a system administrator, use the **enable** EXEC command.

```
enable [privilege-level]
```

Syntax Description	<i>privilege-level</i>	(Optional) Privilege level at which to log in.
---------------------------	------------------------	--

end

To end the current configuration session and return to privileged EXEC mode, use the **end** global configuration command.

```
end
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--

exit (EXEC)

To close an active terminal session by logging off the router, use the **exit** command in EXEC mode.

```
exit
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--

exit (global)

To exit any configuration mode to the next highest mode in the CLI mode hierarchy, use the **exit** command in any configuration mode.

```
exit
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--

full-help

To get help for the full set of user-level commands, use the **full-help** line configuration command.

full-help

Syntax Description This command has no arguments or keywords.

help

To display a brief description of the help system, enter the **help** command.

help

Syntax Description This command has no arguments or keywords.

history

To enable the command history function, use the **history** line configuration command. To disable the command history feature, use the **no** form of this command.

history

no history

Syntax Description This command has no arguments or keywords.

history size

To change the command history buffer size for a particular line, use the **history size** line configuration command. To reset the command history buffer size to ten lines, use the **no** form of this command.

history size *number-of-lines*

no history size

Syntax Description *number-of-lines* Specifies the number of command lines that the system will record in its history buffer. The range is from 0 to 256. The default is ten.

menu (EXEC)

To display a preconfigured user menu, use the **menu** command in user or privileged EXEC mode.

```
menu menu-name
```

Syntax Description	<i>menu-name</i>	The name of the menu.
--------------------	------------------	-----------------------

more begin

To search the output of any **more** command, use the **more begin** command in EXEC mode. This command begins unfiltered output of the **more** command with the first line that contains the regular expression you specify.

```
more file-url | begin regular-expression
```

Syntax Description	<i>file-url</i>	The Universal Resource Locator (url) of the file to display. More commands are advanced show commands; for details, see the command reference page in this book for the more command.
		A vertical bar (the “pipe” symbol) indicates that an output processing specification follows.
	<i>regular-expression</i>	Any regular expression found in more command output.
	/	Specifies a search at a --More-- prompt that begins unfiltered output with the first line that contains the regular expression.
	-	Specifies a filter at a --More-- prompt that only displays output lines that do not contain the regular expression.
	+	Specifies a filter at a --More-- prompt that only displays output lines that contain the regular expression.

more exclude

To filter **more** command output so that it excludes lines that contain a particular regular expression, use the **more exclude** command in EXEC mode.

```
more file-url | exclude regular-expression
```

Syntax Description	<i>file-url</i>	The Universal Resource Locator (url) of the file to display. More commands are advanced show commands; for details, see the command reference page in this book for the more command.
		A vertical bar (the “pipe” symbol) indicates that an output processing specification follows.
	<i>regular-expression</i>	Any regular expression found in more command output.
	/	Specifies a search at a --More-- prompt that begins unfiltered output with the first line that contains the regular expression.

more include

To filter **more** command output so that it displays only lines that contain a particular regular expression, use the **more include** command in EXEC mode.

```
more file-url | include regular-expression
```

Syntax Description		
	<i>file-url</i>	The Universal Resource Locator (url) of the file to display. More commands are advanced show commands; for details, see the command reference page in this book for the more command.
		A vertical bar (the “pipe” symbol) indicates that an output processing specification follows.
	<i>regular-expression</i>	Any regular expression found in more command output.
	/	Specifies a search at a --More-- prompt that begins unfiltered output with the first line that contains the regular expression.

show begin

To begin the output of any **show** command from a specified string, use the **show begin** command in EXEC mode.

```
show any-command | begin regular-expression
```

Syntax Description		
	<i>any-command</i>	Any supported show command.
		A vertical bar (the “pipe” symbol) indicates that an output processing specification follows.
	<i>regular-expression</i>	Any regular expression found in show command output. The show output will begin from the first instance of this string (output prior to this string will not be printed to the screen). The string is case-sensitive. Use parenthesis to indicate a literal use of spaces.
	/	Specifies a search at a --More-- prompt that begins unfiltered output with the first line that contains the regular expression.
	-	Specifies a filter at a --More-- prompt that only displays output lines that do not contain the regular expression.
	+	Specifies a filter at a --More-- prompt that only displays output lines that contain the regular expression.

show exclude

To filter **show** command output so that it excludes lines that contain a particular regular expression, use the **show exclude** command in EXEC mode.

```
show any-command | exclude regular-expression
```

Syntax Description	<i>any-command</i>	Any supported show command.
		A vertical bar (the “pipe” symbol) indicates that an output processing specification follows.
	<i>regular-expression</i>	Any regular expression found in show command output.
	/	Specifies a search at a --More-- prompt that begins unfiltered output with the first line that contains the regular expression.

show history

To list the commands you have entered in the current EXEC session, use the **show history** EXEC command.

show history

Syntax Description This command has no arguments or keywords.

show include

To filter **show** command output so that it only displays lines that contain a particular regular expression, use the **show include** command in EXEC mode.

show any-command | include regular-expression

Syntax Description	<i>any-command</i>	Any supported show command.
		A vertical bar (the “pipe” symbol) indicates that an output processing specification follows.
	<i>regular-expression</i>	Any regular expression found in show command output. Use parenthesis to include spaces in the expression.
	/	Specifies a search at a --More-- prompt that begins unfiltered output with the first line that contains the regular expression.

terminal editing

To reenable the enhanced editing mode for only the current terminal session, use the **terminal editing** EXEC command. To disable the enhanced editing mode on the current line, use the **no** form of this command.

terminal editing

terminal no editing

Syntax Description This command has no arguments or keywords.

terminal full-help

To get help for the full set of user-level commands, use the **terminal full-help** EXEC mode command.

terminal full-help

Syntax Description This command has no arguments or keywords.

terminal history

To enable the command history feature for the current terminal session, use the **terminal history** command in user EXEC mode or privileged EXEC mode. To disable the command history feature, use the **no** form of this command.

terminal history

terminal no history

Syntax Description This command has no arguments or keywords.

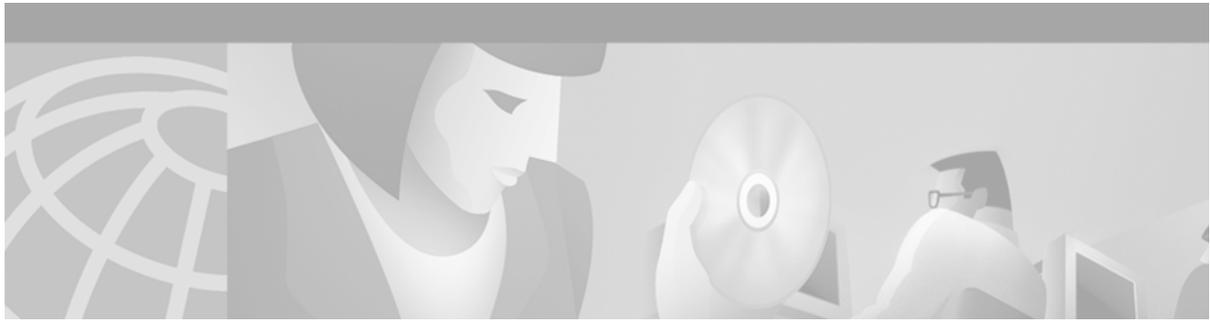
terminal history size

To change the size of the command history buffer for the current terminal session, use the **terminal history size** EXEC mode command. To reset the command history buffer to its default size of 10 lines, use the **no** form of this command.

terminal history size *number-of-lines*

terminal no history size

Syntax Description	<i>number-of-lines</i>	Number of command lines that the system will record in its history buffer. The range is from 0 to 256. The default is 10.
---------------------------	------------------------	---



The Setup Command

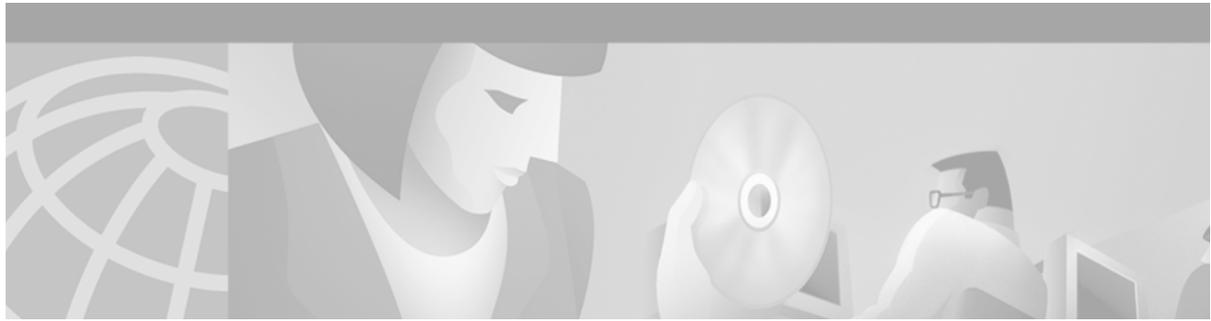
This chapter describes the function and syntax of the **setup** command. For more information about this command, refer to the corresponding chapter of the *Cisco IOS Configuration Fundamentals Command Reference*.

setup

To enter Setup mode, use the **setup** privileged EXEC command.

setup

Syntax Description This command has no arguments or keywords.



Terminal Operating Characteristics Commands

This chapter describes the function and syntax of the commands used to control terminal operating characteristics. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Configuration Fundamentals Command Reference*.

activation-character

To define the character you enter at a vacant terminal to begin a terminal session, use the **activation-character** line configuration command. To make any character activate a terminal, use the **no** form of this command.

activation-character *ascii-number*

no activation-character

Syntax Description	<i>ascii-number</i>	Decimal representation of the activation character.
---------------------------	---------------------	---

autobaud

To set the line for automatic baud detection, use the **autobaud** line configuration command. To disable automatic baud detection, use the **no** form of this command.

autobaud

no autobaud

Syntax Description	This command has no arguments or keywords.
---------------------------	--

databits

To set the number of data bits per character that are interpreted and generated by the router hardware, use the **databits** line configuration command. To restore the default value, use the **no** form of the command.

databits {5 | 6 | 7 | 8}

no databits

Syntax Description		
	5	Five data bits per character.
	6	Six data bits per character.
	7	Seven data bits per character.
	8	Eight data bits per character.

data-character-bits

To set the number of data bits per character that are interpreted and generated by the Cisco IOS software, use the **data-character-bits** line configuration command. To restore the default value, use the **no** form of this command.

data-character-bits {7 | 8}

no data-character-bits

Syntax Description		
	7	Seven data bits per character.
	8	Eight data bits per character. This is the default.

default-value exec-character-bits

To define the EXEC character width for either 7 bits or 8 bits, use the **default-value exec-character-bits** global configuration command. To restore the default value, use the **no** form of this command.

default-value exec-character-bits {7 | 8}

no default-value exec-character-bits

Syntax Description		
	7	Selects the 7-bit ASCII character set. This is the default.
	8	Selects the full 8-bit ASCII character set.

default-value special-character-bits

To configure the flow control default value from a 7-bit width to an 8-bit width, use the **default-value special-character-bits** global configuration command. To restore the default value, use the **no** form of this command.

default-value special-character-bits {7 | 8}

no default-value special-character-bits

Syntax Description		
	7	Selects the 7-bit character set. This is the default.
	8	Selects the full 8-bit character set.

disconnect-character

To define a character to disconnect a session, use the **disconnect-character** line configuration command. To remove the disconnect character, use the **no** form of this command.

disconnect-character *ascii-number*

no disconnect-character

Syntax Description		
	<i>ascii-number</i>	Decimal representation of the session disconnect character.

dispatch-character

To define a character that causes a packet to be sent, use the **dispatch-character** line configuration command. To remove the definition of the specified dispatch character, use the **no** form of this command.

dispatch-character *ascii-number1* [*ascii-number2* . . . *ascii-number*]

no dispatch-character *ascii-number1* [*ascii-number2* . . . *ascii-number*]

Syntax Description		
	<i>ascii-number1</i>	Decimal representation of the desired dispatch character.
	<i>ascii-number2</i> . . . <i>ascii-number</i>	(Optional) Additional decimal representations of characters. This syntax indicates that you can define any number of characters as dispatch characters.

dispatch-machine

To specify an identifier for a TCP packet dispatch state machine on a particular line, use the **dispatch-machine** line configuration command. To disable a state machine on a particular line, use the **no** form of this command.

dispatch-machine *name*

no dispatch-machine

Syntax Description

<i>name</i>	Name of the state machine that determines when to send packets on the asynchronous line.
-------------	--

dispatch-timeout

To set the character dispatch timer, use the **dispatch-timeout** line configuration command. To remove the timeout definition, use the **no** form of this command.

dispatch-timeout *milliseconds*

no dispatch-timeout

Syntax Description

<i>milliseconds</i>	Integer that specifies the number of milliseconds (ms) that the Cisco IOS software waits after putting the first character into a packet buffer before sending the packet. During this interval, more characters can be added to the packet, which increases the processing efficiency of the remote host.
---------------------	--

escape-character

To define a system escape character, use the **escape-character** line configuration command. To set the escape character to Break, use the **no** or **default** form of this command.

escape-character {*ascii-number* | *character* | **break** | **default** | **none**} [**soft**]

no escape-character [**soft**]

default escape-character

Syntax Description

<i>ascii-number</i>	ASCII decimal representation of a character or a control sequence (for example, Ctrl-E) to be used as the escape character.
<i>character</i>	Character to be used as the escape character (for example, !).
break	Sets the escape character to Break. Note that the Break key should not be used as an escape character on a console terminal.
default	Sets the escape key sequence to the default of Ctrl-^, X.

none	Disables escape entirely.
soft	(Optional) Sets an escape character that will wait until pending input is processed before it executes.

exec-character-bits

To configure the character widths of EXEC and configuration command characters, use the **exec-character-bits** line configuration command. To restore the default value, use the **no** form of this command.

```
exec-character-bits {7 | 8}
```

```
no exec-character-bits
```

Syntax Description	7	Selects the 7-bit character set. This is the default.
	8	Selects the full 8-bit character set for use of international and graphical characters in banner messages, prompts, and so on.

hold-character

To define the local hold character used to pause output to the terminal screen, use the **hold-character** line configuration command. To restore the default, use the **no** form of this command.

```
hold-character ascii-number
```

```
no hold-character
```

Syntax Description	<i>ascii-number</i>	ASCII decimal representation of a character or control sequence (for example, Ctrl-P).
---------------------------	---------------------	--

insecure

To configure a line as insecure, use the **insecure** line configuration command. To disable this feature, use the **no** form of this command.

```
insecure
```

```
no insecure
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--

length

To set the terminal screen length, use the **length** line configuration command. To restore the default value, use the **no** form of this command.

length *screen-length*

no length

Syntax Description

screen-length

The number of lines on the screen. A value of zero disables pausing between screens of output.

location

To provide a description of the location of a serial device, use the **location** line configuration command. To remove the description, use the **no** form of this command.

location *text*

no location

Syntax Description

text

Location description.

lockable

To enable use of the **lock** EXEC command, use the **lockable** global configuration command. To reinstate the default (the terminal session cannot be locked), use the **no** form of this command.

lockable

no lockable

Syntax Description

This command has no arguments or keywords.

logout-warning

To warn users of an impending forced timeout, use the **logout-warning** line configuration command. To restore the default, use the **no** form of this command.

logout-warning [*seconds*]

logout-warning

Syntax Description	<i>seconds</i>	(Optional) Number of seconds that are counted down before session termination. If no number is specified, the default of 20 seconds is used.
---------------------------	----------------	--

notify

To enable terminal notification about pending output from other Telnet connections, use the **notify** line configuration command. To disable notifications, use the **no** form of this command.

notify

no notify

Syntax Description	This command has no arguments or keywords.
---------------------------	--

padding

To set the padding on a specific output character, use the **padding** line configuration command. To remove padding for the specified output character, use the **no** form of this command.

padding *ascii-number count*

no padding *ascii-number*

Syntax Description	<i>ascii-number</i>	ASCII decimal representation of the character.
	<i>count</i>	Number of NULL bytes sent after the specified character, up to 255 padding characters in length.

parity

To define generation of a parity bit, use the **parity** line configuration command. To specify no parity, use the **no** form of this command.

parity { **none** | **even** | **odd** | **space** | **mark** }

no parity

Syntax Description		
	none	No parity. This is the default.
	even	Even parity.
	odd	Odd parity.
	space	Space parity.
	mark	Mark parity.

printer

To configure a printer and assign a server tty line (or lines) to it, use the **printer** global configuration command. To disable printing on a tty line, use the **no** form of this command.

```
printer printer-name {line number | rotary number} [newline-convert | formfeed]
```

```
no printer
```

Syntax Description		
	<i>printer-name</i>	Printer name.
	line number	Assigns a tty line to the printer.
	rotary number	Assigns a rotary group of tty lines to the printer.
	newline-convert	(Optional) Converts newline (linefeed) characters to a two-character sequence “carriage-return, linefeed” (CR+LF).
	formfeed	(Optional) Causes the Cisco IOS software to send a form-feed character (ASCII 0x0C) to the printer tty line immediately following each print job received from the network.

private

To save user EXEC command changes between terminal sessions, use the **private** line configuration command. To restore the default condition, use the **no** form of this command.

```
private
```

```
no private
```

Syntax Description This command has no arguments or keywords.

show whoami

To display information about the terminal line of the current user, including host name, line number, line speed, and location, use the **show whoami** EXEC command.

```
show whoami [text]
```

Syntax Description		
	<i>text</i>	(Optional) Additional data to print to the screen.

special-character-bits

To configure the number of data bits per character for special characters such as software flow control characters and escape characters, use the **special-character-bits** line configuration command. To restore the default value, use the **no** form of this command.

special-character-bits { 7 | 8 }

no special-character-bits

Syntax Description		
	7	Selects the 7-bit ASCII character set. This is the default.
	8	Selects the full 8-bit character set for special characters.

state-machine

To specify the transition criteria for the state of a particular state machine, use the **state-machine** global configuration command. To remove a particular state machine from the configuration, use the **no** form of this command.

state-machine *name state first-character last-character* [*nextstate* | **transmit**]

no state-machine *name*

Syntax Description		
	<i>name</i>	Name for the state machine (used in the dispatch-machine line configuration command). The user can specify any number of state machines, but each line can have only one state machine associated with it.
	<i>state</i>	State being modified. There are a maximum of eight states per state machine. Lines are initialized to state 0 and return to state 0 after a packet is transmitted.
	<i>first-character</i> <i>last-character</i>	Specifies a range of characters. Use ASCII numerical values. If the state machine is in the indicated state, and the next character input is within this range, the process goes to the specified next state. Full 8-bit character comparisons are done, so the maximum value is 255. Ensure that the line is configured to strip parity bits (or not generate them), or duplicate the low characters in the upper half of the space.
	<i>nextstate</i>	(Optional) State to enter if the character is in the specified range.
	transmit	(Optional) Causes the packet to be transmitted and the state machine to be reset to state 0. Recurring characters that have not been explicitly defined to have a particular action return the state machine to state 0.

stopbits

To set the number of the stop bits transmitted per byte, use the **stopbits** line configuration command. To restore the default value, use the **no** form of this command.

```
stopbits {1 | 1.5 | 2}
```

```
no stopbits
```

Syntax Description		
	1	One stop bit.
	1.5	One and one-half stop bits.
	2	Two stop bits. This is the default.

terminal databits

To change the number of data bits per character for the current terminal line for this session, use the **terminal databits** EXEC command.

```
terminal databits {5 | 6 | 7 | 8}
```

Syntax Description		
	5	Five data bits per character.
	6	Six data bits per character.
	7	Seven data bits per character.
	8	Eight data bits per character. This is the default.

terminal data-character-bits

To set the number of data bits per character that are interpreted and generated by the Cisco IOS software for the current line and session, use the **terminal data-character-bits** EXEC command.

```
terminal data-character-bits {7 | 8}
```

Syntax Description		
	7	Seven data bits per character.
	8	Eight data bits. This is the default.

terminal dispatch-character

To define a character that causes a packet to be sent for the current session, use the **terminal dispatch-character** EXEC command.

```
terminal dispatch-character ascii-number [ascii-number2 . . . ascii-number]
```

Syntax Description	<i>ascii-number</i>	The ASCII decimal representation of the character, such as Return (ASCII character 13) for line-at-a-time transmissions.
	<i>ascii-number2 . . . ascii-number</i>	(Optional) Additional decimal representations of characters. This syntax indicates that you can define any number of characters as dispatch characters.

terminal dispatch-timeout

To set the character dispatch timer for the current terminal line for the current session, use the **terminal dispatch-timeout EXEC** command.

terminal dispatch-timeout *milliseconds*

Syntax Description	<i>milliseconds</i>	Integer that specifies the number of milliseconds that the router waits after it puts the first character into a packet buffer before sending the packet. During this interval, more characters can be added to the packet, which increases the processing efficiency of the remote host.
---------------------------	---------------------	---

terminal download

To temporarily set the ability of a line to act as a transparent pipe for file transfers for the current session, use the **terminal download EXEC** command.

terminal download

Syntax Description	This command has no arguments or keywords.
---------------------------	--

terminal escape-character

To set the escape character for the current terminal line for the current session, use the **terminal escape-character EXEC** command.

terminal escape-character *ascii-number*

Syntax Description	<i>ascii-number</i>	ASCII decimal representation of the escape character or control sequence (for example, Ctrl-P).
---------------------------	---------------------	---

terminal exec-character-bits

To locally change the ASCII character set used in EXEC and configuration command characters for the current session, use the **terminal exec-character-bits** EXEC command.

```
terminal exec-character-bits {7 | 8}
```

Syntax Description		
	7	Selects the 7-bit ASCII character set. This is the default.
	8	Selects the full 8-bit character set.

terminal flowcontrol

To set flow control for the current terminal line for the current session, use the **terminal flowcontrol** EXEC command.

```
terminal flowcontrol {none | software [in | out] | hardware}
```

Syntax Description		
	none	Prevents flow control.
	software	Sets software flow control.
	in out	(Optional) Specifies the direction of flow control: in causes the router to listen to flow control from the attached device, and out causes the router to send flow control information to the attached device. If you do not specify a direction, both directions are assumed.
	hardware	Sets hardware flow control. For information about setting up the EIA/TIA-232 line, see the manual that was shipped with your product.

terminal hold-character

To define the hold character for the current session, use the **terminal hold-character** EXEC command. To return the hold character definition to the default, use the **terminal no hold-character** command.

```
terminal hold-character ascii-number
```

```
terminal no hold-character
```

Syntax Description		
	<i>ascii-number</i>	ASCII decimal representation of a character or control sequence (for example, Ctrl-P).

terminal keymap-type

To specify the current keyboard type for the current session, use the **terminal keymap-type** EXEC command.

terminal keymap-type *keymap-name*

Syntax Description

keymap-name Name defining the current keyboard type.

terminal length

To set the number of lines on the current terminal screen for the current session, use the **terminal length** EXEC command.

terminal length *screen-length*

Syntax Description

screen-length Number of lines on the screen. A value of zero disables pausing between screens of output.

terminal monitor

To display **debug** command output and system error messages for the current terminal and session, use the **terminal monitor** EXEC command.

terminal monitor

Syntax Description

This command has no arguments or keywords.

terminal notify

To enable terminal notification about pending output from other Telnet connections for the current session, use the **terminal notify** EXEC command. To disable notifications for the current session, use the **no** form of this command.

terminal notify

terminal no notify

Syntax Description

This command has no arguments or keywords.

terminal padding

To change the character padding on a specific output character for the current session, use the **terminal padding** EXEC command.

```
terminal padding ascii-number count
```

Syntax Description	<i>ascii-number</i>	ACII decimal representation of the character.
	<i>count</i>	Number of NULL bytes sent after the specified character, up to 255 padding characters in length.

terminal parity

To define the generation of the parity bit for the current terminal line and session, use the **terminal parity** EXEC command.

```
terminal parity { none | even | odd | space | mark }
```

Syntax Description	none	No parity. This is the default.
	even	Even parity.
	odd	Odd parity.
	space	Space parity.
	mark	Mark parity.

terminal-queue entry-retry-interval

To change the retry interval for a terminal port queue, use the **terminal-queue** global configuration command. To restore the default terminal port queue interval, use the **no** form of this command.

```
terminal-queue entry-retry-interval interval
```

```
no terminal-queue entry-retry-interval
```

Syntax Description	<i>interval</i>	Number of seconds between terminal port retries.
--------------------	-----------------	--

terminal rxspeed

To set the terminal receive speed (how fast information is sent to the terminal) for the current line and session, use the **terminal rxspeed** EXEC command.

```
terminal rxspeed bps
```

Syntax Description	<i>bps</i>	Baud rate in bits per second (bps).
---------------------------	------------	-------------------------------------

terminal special-character-bits

To change the ASCII character widths to accept special characters for the current terminal line and session, use the **terminal special-character-bits** EXEC command.

```
terminal special-character-bits {7 | 8}
```

Syntax Description	7	Selects the 7-bit ASCII character set. This is the default.
	8	Selects the full 8-bit ASCII character set.

terminal speed

To set the transmit and receive speeds of the current terminal line for the current session, use the **terminal speed** EXEC command.

```
terminal speed bps
```

Syntax Description	<i>bps</i>	Baud rate in bits per second (bps).
---------------------------	------------	-------------------------------------

terminal start-character

To change the flow control start character for the current session, use the **terminal start-character** EXEC command.

```
terminal start-character ascii-number
```

Syntax Description	<i>ascii-number</i>	ASCII decimal representation of the start character.
---------------------------	---------------------	--

terminal stopbits

To change the number of stop bits sent per byte by the current terminal line during an active session, use the **terminal stopbits** EXEC command.

terminal stopbits {1 | 1.5 | 2}

Syntax Description	1	One stop bit.
	1.5	One and one-half stop bits.
	2	Two stop bits. This is the default.

terminal stop-character

To change the flow control stop character for the current session, use the **terminal stop-character** EXEC command.

terminal stop-character *ascii-number*

Syntax Description	<i>ascii-number</i>	ASCII decimal representation of the stop character.

terminal telnet break-on-ip

To cause an access server to generate a hardware Break signal when an interrupt-process (ip) command is received, use the **terminal telnet break-on-ip** EXEC command.

terminal telnet break-on-ip

Syntax Description	This command has no arguments or keywords.

terminal telnet refuse-negotiations

To configure the current session to refuse to negotiate full-duplex, remote echo options on incoming connections, use the **terminal telnet refuse-negotiations** EXEC command.

terminal telnet refuse-negotiations

Syntax Description	This command has no arguments or keywords.

terminal telnet speed

To allow an access server to negotiate transmission speed for the current terminal line and session, use the **terminal telnet speed** EXEC command.

terminal telnet speed *default-speed maximum-speed*

Syntax Description	<i>default-speed</i>	Line speed, in bits per second (bps), that the access server will use if the device on the other end of the connection has not specified a speed.
	<i>maximum-speed</i>	Maximum line speed in bits per second (bps), that the device on the other end of the connection can use.

terminal telnet sync-on-break

To cause the access server to send a Telnet Synchronize signal when it receives a Telnet Break signal on the current line and session, use the **terminal telnet sync-on-break** EXEC command.

terminal telnet sync-on-break

Syntax Description	This command has no arguments or keywords.
---------------------------	--

terminal telnet transparent

To cause the current terminal line to send a Return character (CR) as a CR followed by a NULL instead of a CR followed by a Line Feed (LF) for the current session, use the **terminal telnet transparent** EXEC command.

terminal telnet transparent

Syntax Description	This command has no arguments or keywords.
---------------------------	--

terminal terminal-type

To specify the type of terminal connected to the current line for the current session, use the **terminal terminal-type** EXEC command.

terminal terminal-type *terminal-type*

Syntax Description	<i>terminal-type</i>	Defines the terminal name and type, and permits terminal negotiation by hosts that provide that type of service.
---------------------------	----------------------	--

terminal tkspeed

To set the terminal transmit speed (how fast the terminal can send information) for the current line and session, use the **terminal tkspeed** EXEC command.

terminal tkspeed *bps*

Syntax Description	<i>bps</i>	Baud rate in bits per second (bps).
---------------------------	------------	-------------------------------------

terminal-type

To specify the type of terminal connected to a line, use the **terminal-type** line configuration command. To remove any information about the type of terminal and reset the line to the default terminal emulation, use the **no** form of this command.

terminal-type {*terminal-name* | *terminal-type*}

no terminal-type

Syntax Description	<i>terminal-name</i>	Terminal name.
	<i>terminal-type</i>	Terminal type.

terminal width

To set the number of character columns on the terminal screen for the current line for a session, use the **terminal width** EXEC command.

terminal width *characters*

Syntax Description	<i>characters</i>	Number of character columns displayed on the terminal.
---------------------------	-------------------	--

where

To list the open sessions, use the **where** EXEC command.

where

Syntax Description	This command has no arguments or keywords.	
---------------------------	--	--

width

To set the terminal screen width, use the **width** line configuration command. To return to the default screen width, use the **no width** form of this command.

width *characters*

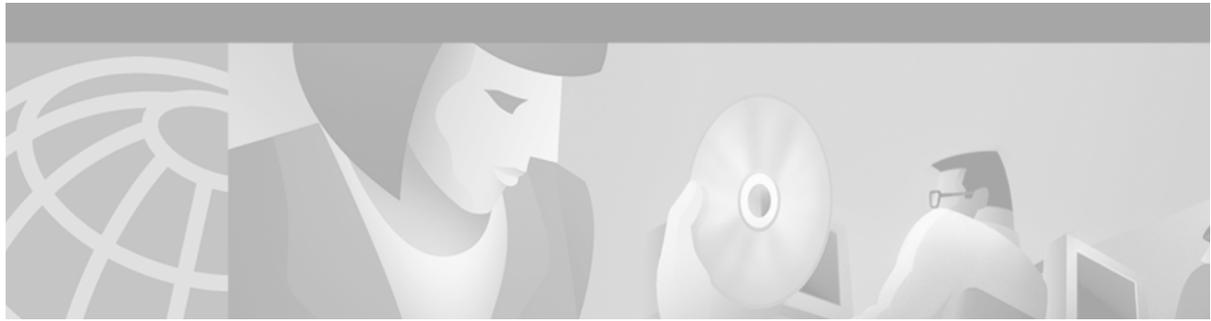
no width

Syntax Description

characters

Number of character columns displayed on the terminal.

width



Connection, Menu, and System Banner Commands

This chapter describes the function and syntax of the commands used for connection management, and the commands used to configure user menus and banners. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Configuration Fundamentals Command Reference*.

banner exec

To specify and enable a message to be displayed when an EXEC process is created (an EXEC banner), use the **banner exec** global configuration command. To delete the existing EXEC banner, use the **no** form of this command.

```
banner exec d message d
```

```
no banner exec
```

Syntax Description

<i>d</i>	Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the banner message.
<i>message</i>	Message text. You can include tokens in the form \$(token) in the message text. Tokens will be replaced with the corresponding configuration variable. Tokens are described in Table 3.

To customize the banner, use tokens in the form \$(token) in the message text. Tokens will display current Cisco IOS configuration variables, such as the router's host name and IP address. The tokens are described in Table 3.

Table 3 Tokens

Token	Information Displayed in the Banner
\$(hostname)	Displays the host name for the router.
\$(domain)	Displays the domain name for the router.
\$(line)	Displays the vty or tty (asynchronous) line number.
\$(line-desc)	Displays the description attached to the line.

banner incoming

To define and enable a banner to be displayed when there is an incoming connection to a terminal line from a host on the network, use the **banner incoming** global configuration command. To delete the incoming connection banner, use the **no** form of this command.

banner incoming *d message d*

no banner incoming

Syntax Description		
<i>d</i>		Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the banner message.
<i>message</i>		Message text. You can include tokens in the form $\$(token)$ in the message text. Tokens will be replaced with the corresponding configuration variable. Tokens are described in Table 3.

banner login

To define and enable a customized banner to be displayed before the username and password login prompts, use the **banner login** global configuration command. To disable the login banner, use **no** form of this command.

banner login *d message d*

no banner login

Syntax Description		
<i>d</i>		Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the banner message.
<i>message</i>		Message text. You can include tokens in the form $\$(token)$ in the message text. Tokens will be replaced with the corresponding configuration variable. Tokens are described in Table 3.

banner motd

To define and enable a message-of-the-day (MOTD) banner, use the **banner motd** global configuration command. To delete the MOTD banner, use the **no** form of this command.

banner motd *d message d*

no banner motd

Syntax Description		
<i>d</i>		Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the banner message.
<i>message</i>		Message text. You can include tokens in the form $\$(token)$ in the message text. Tokens will be replaced with the corresponding configuration variable.

banner slip-ppp

To customize the banner that is displayed when a SLIP or PPP connection is made, use the **banner slip-ppp** global configuration command. To restore the default SLIP or PPP banner, use the **no** form of this command.

banner slip-ppp *d message d*

no banner slip-ppp

Syntax Description	<i>d</i>	Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the banner message.
	<i>message</i>	Message text. You can include tokens in the form \$(token) in the message text. Tokens will be replaced with the corresponding configuration variable.

clear tcp

To clear a TCP connection, use the **clear tcp** privileged EXEC command.

clear tcp {**line** *line-number* | **local** *hostname port* **remote** *hostname port* | **tcb** *address*}

Syntax Description	line <i>line-number</i>	Line number of the TCP connection to clear.
	local <i>hostname port</i> remote <i>hostname port</i>	Host name of the local router and port and host name of the remote router and port of the TCP connection to clear.
	tcb <i>address</i>	Transmission Control Block (TCB) address of the TCP connection to clear. The TCB address is an internal identifier for the endpoint.

exec

To allow an EXEC process on a line, use the **exec** line configuration command. To turn off the EXEC process for the specified line, use the **no** form of this command.

exec

no exec

Syntax Description	This command has no arguments or keywords.
---------------------------	--

exec-banner

To reenable the display of EXEC and message-of-the-day (MOTD) banners on the specified line or lines, use the **exec-banner** line configuration command. To suppress the banners on the specified line or lines, use the **no** form of this command.

exec-banner

no exec-banner

Syntax Description This command has no arguments or keywords.

exec-timeout

To set the interval that the EXEC command interpreter waits until user input is detected, use the **exec-timeout** line configuration command. To remove the timeout definition, use the **no** form of this command.

exec-timeout *minutes* [*seconds*]

no exec-timeout

Syntax Description	<i>minutes</i>	Integer that specifies the number of minutes.
	<i>seconds</i>	(Optional) Additional time intervals in seconds.

lock

To configure a temporary password on a line, use the **lock** EXEC command.

lock

Syntax Description This command has no arguments or keywords.

menu clear-screen

To clear the terminal screen before displaying a menu, use the **menu clear-screen** global configuration command.

menu *menu-name* **clear-screen**

Syntax Description	<i>menu-name</i>	Name of the menu this command should be applied to.
---------------------------	------------------	---

menu command

To specify underlying commands for user menus, use the **menu command** global configuration command.

```
menu menu-name command menu-item {command | menu-exit}
```

Syntax Description		
<i>menu-name</i>	Name of the menu. You can specify a maximum of 20 characters.	
<i>menu-item</i>	Number, character, or string used as the key for the item. The key is displayed to the left of the menu item text. You can specify a maximum of 18 menu entries. When the 10th item is added to the menu, the line-mode and single-space options are activated automatically.	
<i>command</i>	Command to issue when the user selects an item.	
menu-exit	Provides a way for menu users to return to a higher-level menu or exit the menu system.	

menu default

To specify the menu item to use as the default, use the **menu default** global configuration command.

```
menu menu-name default menu-item
```

Syntax Description		
<i>menu-name</i>	Name of the menu. You can specify a maximum of 20 characters.	
<i>menu-item</i>	Number, character, or string key of the item to use as the default.	

menu line-mode

To require the user to press Enter after specifying an item, use the **menu line-mode** global configuration command.

```
menu menu-name line-mode
```

Syntax Description		
<i>menu-name</i>	Name of the menu this command should be applied to.	

menu options

To set options for items in user menus, use the **menu options** global configuration command.

```
menu menu-name options menu-item {login | pause}
```

Syntax Description	<i>menu-name</i>	The name of the menu. You can specify a maximum of 20 characters.
	<i>menu-item</i>	Number, character, or string key of the item affected by the option.
	login	Requires a login before issuing the command.
	pause	Pauses after the command is entered before redrawing the menu.

menu prompt

To specify the prompt for a user menu, use the **menu prompt** global configuration command.

```
menu menu-name prompt d prompt d
```

Syntax Description	<i>menu-name</i>	Name of the menu. You can specify a maximum of 20 characters.
	<i>d</i>	A delimiting character that marks the beginning and end of a title. Text delimiters are characters that do not ordinarily appear within the text of a title, such as slash (/), double quote ("), and tilde (~). ^C is reserved for special use and should not be used in the text of the title.
	<i>prompt</i>	Prompt string for the menu.

menu single-space

To display menu items single-spaced rather than double-spaced, use the **menu single-space** global configuration command.

```
menu menu-name single-space
```

Syntax Description	<i>menu-name</i>	Name of the menu this command should be applied to.
---------------------------	------------------	---

menu status-line

To display a line of status information about the current user at the top of a menu, use the **menu status-line** global configuration command.

```
menu menu-name status-line
```

Syntax Description	<i>menu-name</i>	Name of the menu this command should be applied to.
---------------------------	------------------	---

menu text

To specify the text of a menu item in a user menu, use the **menu text** global configuration command.

```
menu menu-name text menu-item menu-text
```

Syntax Description		
	<i>menu-name</i>	Name of the menu. You can specify a maximum of 20 characters.
	<i>menu-item</i>	Number, character, or string used as the key for the item. The key is displayed to the left of the menu item text. You can specify a maximum of 18 menu items. When the 10th item is added to the menu, the menu line-mode and menu single-space commands are activated automatically.
	<i>menu-text</i>	Text of the menu item.

menu title

To create a title (banner) for a user menu, use the **menu title** global configuration command.

```
menu menu-name title d menu-title d
```

Syntax Description		
	<i>menu-name</i>	Name of the menu. You can specify a maximum of 20 characters.
	<i>d</i>	A delimiting character that marks the beginning and end of a title. Text delimiters are characters that do not ordinarily appear within the text of a title, such as slash (/), double quote ("), and tilde (~). ^C is reserved for special use and should not be used in the text of the title.
	<i>menu-title</i>	Lines of text to appear at the top of the menu.

no menu

To delete a user menu from the configuration file, use the **no menu** global configuration command.

```
no menu menu-name
```

Syntax Description		
	<i>menu-name</i>	Name of the menu to delete from the configuration file.

motd-banner

To enable the display of message-of-the-day (MOTD) banners on the specified line or lines, use the **motd-banner** line configuration command. To suppress the MOTD banners on the specified line or lines, use the **no** form of this command.

```
motd-banner
```

```
no motd-banner
```

Syntax Description	
	This command has no arguments or keywords.

name-connection

To assign a logical name to a connection, use the **name-connection** user EXEC command.

name-connection

Syntax Description This command has no arguments or keywords.

refuse-message

To define and enable a line-in-use message, use the **refuse-message** line configuration command. To disable the message, use the **no** form of this command.

refuse-message *d message d*

no refuse-message

Syntax Description	<i>d</i>	Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the message.
	<i>message</i>	Message text.

send

To send messages to one or all terminal lines, use the **send** EXEC command.

send {*line-number* | * | **aux** *number* | **console** *number* | **tty** *number* | **vty** *number*}

Syntax Description	<i>line-number</i>	Line number to which the message will be sent.
	*	Sends a message to all lines.
	aux <i>number</i>	Sends a message to the specified AUX port.
	console <i>number</i>	Sends a message to the specified console port.
	tty <i>number</i>	Sends a message to the specified asynchronous line.
	vty <i>number</i>	Sends a message to the specified virtual asynchronous line.

service linenumbers

To configure the Cisco IOS software to display line number information after the EXEC or incoming banner, use the **service linenumbers** global configuration command. To disable this function, use the **no** form of this command.

service linenumbers

no service linenumbers

Syntax Description This command has no arguments or keywords.

vacant-message

To display an idle terminal message, use the **vacant-message** line configuration command. To remove the default vacant message or any other vacant message that may have been set, use the **no** form of this command.

vacant-message [*d message d*]

no vacant-message

Syntax Description	<i>d</i>	(Optional) Delimiting character that marks the beginning and end of the vacant-message. Text delimiters are characters that do not ordinarily appear within the text of a title, such as slash (/), double quote ("), or tilde (~). ^C is reserved for special use and should not be used in the message.
	<i>message</i>	(Optional) Vacant terminal message.

■ vacant-message



Cisco IOS Web Browser User Interface Commands

This chapter describes the function and syntax of the commands used to enable the HTTP server on your router to allow the use of the Cisco IOS Web browser user interface (UI) and ClickStart. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Configuration Fundamentals Command Reference*.

international

If you are using Telnet to access a Cisco IOS platform and you want to display 8-bit and multibyte international characters (for example, Kanji) and print the Escape character as a single character instead of as the caret and bracket symbols (^[]), use the **international** line configuration command. To display characters in 7-bit format, use the **no** form of this command.

international

no international

Syntax Description This command has no arguments or keywords.

ip http access-class

To assign an access list to the HTTP server used by the Cisco IOS ClickStart software or the Cisco Web browser UI, use the **ip http access-class** global configuration command. To remove the assigned access list, use the **no** form of this command.

ip http access-class {*access-list-number* | *access-list-name*}

no ip http access-class {*access-list-number* | *access-list-name*}

Syntax Description	<i>access-list-number</i>	Standard IP access list number in the range 0 to 99, as configured by the access-list (standard) global configuration command.
	<i>access-list-name</i>	Name of a standard IP access list, as configured by the ip access-list command.

ip http authentication

To specify a particular authentication method for HTTP server users, use the **ip http authentication** global configuration command. To disable a configured authentication method, use the **no** form of this command.

ip http authentication {aaa | enable | local | tacacs}

no ip http authentication {aaa | enable | local | tacacs}

Syntax Description		
aaa	Indicates that the AAA facility is used for authentication.	
enable	Indicates that the enable password method, which is the default method of HTTP server user authentication, is used for authentication.	
local	Indicates that the local user database as defined on the Cisco router or access server is used for authentication.	
tacacs	Indicates that the TACACS or XTACACS server is used for authentication.	

ip http port

To specify the port to be used by the Cisco IOS ClickStart software or the Cisco Web browser UI, use the **ip http port** global configuration command. To use the default port, use the **no** form of this command.

ip http port *port-number*

no ip http port

Syntax Description	<i>port-number</i>	Port number for use by the HTTP server.

ip http server

To enable the Cisco Web browser UI on a router or access server, use the **ip http server** global configuration command. To disable this feature, use the **no** form of this command.

ip http server

no ip http server

Syntax Description	This command has no arguments or keywords.

terminal international

If you are using Telnet to access a Cisco IOS platform and you want to display 8-bit and multibyte international characters (for example, Kanji) and print the Escape character as a single character instead of as the caret and bracket symbols (^[]) for a current Telnet session, use the **terminal international** EXEC command. To display characters in 7-bit format for a current Telnet session, use the **no** form of this command.

terminal international

no terminal international

Syntax Description This command has no arguments or keywords.

■ terminal international



Cisco IOS File System Commands

This chapter describes the function and syntax of the commands used to manipulate files on your routing device using the Cisco IOS File System (IFS). For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Configuration Fundamentals Command Reference*.

Commands in this chapter use URLs as part of the command syntax. URLs used in the Cisco IFS contain two parts: a file system or network prefix, and file identification suffix.

Table 4 lists some of the UTL prefixes used to indicate a device on the network.

Table 4 Network Prefixes for Cisco IFS URLs

Prefix	Description
ftp:	Specifies a File Transfer Protocol (FTP) network server.
rcp:	Specifies an remote copy protocol (rcp) network server.
tftp:	Specifies a TFTP server.

Table 5 lists the available suffix options for the URL prefixes used in Table 4.

Table 5 File ID Suffixes for Cisco IFS URLs

Prefix	Suffix Options
ftp:	[[//[username[:password]@]location]/directory]/filename For example: ftp://network-config (<i>prefix://filename</i>) ftp://jeanluc:secret@enterprise.cisco.com/ship-config
rcp:	rcp:[[//[username@]location]/directory]/filename
tftp:	tftp:[[//location]/directory]/filename

Table 6 lists some of the URL prefixes used to indicate memory locations on the system.

Table 6 File System Prefixes for Cisco IFS URLs

Prefix	Description
bootflash:	Bootflash memory.
disk0:	Rotating disk media.

Table 6 File System Prefixes for Cisco IFS URLs (continued)

Prefix	Description
flash: [<i>partition-number</i>]	Flash memory. This prefix is available on all platforms. For platforms that do not have a device named flash: , the prefix flash: is aliased to slot0: . Therefore, you can use the prefix flash: to refer to the main Flash memory storage area on all platforms
flh:	Flash load helper log files.
null:	Null destination for copies. You can copy a remote file to null to determine its size.
nvr:	NVRAM. This is the default location for the running-configuration file.
slavebootflash:	Internal Flash memory on a slave RSP card of a router configured with Dual RSPs.
slavenvram:	NVRAM on a slave RSP card.
slaveslot0:	First PCMCIA card on a slave RSP card.
slaveslot1:	Second PCMCIA card on a slave RSP card.
slot0:	First PCMCIA Flash memory card.
slot1:	Second PCMCIA Flash memory card.
xmodem:	Obtain the file from a network machine using the Xmodem protocol.
ymodem:	Obtain the file from a network machine using the Ymodem protocol.

For details about the Cisco IFS, and for IFS configuration tasks, refer to the “Configuring the Cisco IOS File System” chapter in the Release 12.2 *Cisco IOS Configuration Fundamentals Configuration Guide*.

cd

To change the default directory or file system, use the **cd EXEC** command.

```
cd [filesystem:]
```

Syntax Description

<i>filesystem:</i>	(Optional) The URL or alias of the directory or file systems followed by a colon.
--------------------	---

configure network

The **configure network** command was replaced by the **copy {rcp | tftp} running-config** command in Cisco IOS Release 11.0. The **configure network** command continues to function in Cisco IOS Release 12.2 for most systems, but support for this command may be removed in a future release.

The **copy {rcp | tftp} running-config** command was replaced by the **copy {ftp: | rcp: | tftp:}[filename] system:running-config** command in Cisco IOS Release 12.1.

The **copy {ftp: | rcp: | tftp:}[filename] system:running-config** command specifies that a configuration file should be copied from a FTP, rcp, or TFTP source to the running configuration. See the description of the **copy** command in this chapter for more information.

copy

To copy any file from a source to a destination, use the **copy** EXEC command.

```
copy [/erase] source-url destination-url
```

Syntax Description		
	/erase	(Optional) Erases the destination file system before copying.
	<i>source-url</i>	The location URL or alias of the source file or directory to be copied.
	<i>destination-url</i>	The destination URL or alias of the copied file or directory.

The exact format of the source and destination URLs varies according to the file or directory location. You may enter either an alias keyword for a particular file or an alias keyword for a file system type (not a file within a type).

delete

To delete a file on a Flash memory device, use the **delete** EXEC command.

```
delete flash-url
```

Syntax Description		
	<i>flash-url</i>	URL of the file to be deleted.

dir

To display a list of files on a file system, use the **dir** EXEC command.

```
dir [all] [filesystem:] [file-url]
```

Syntax Description		
	all	(Optional) Lists deleted files, undeleted files, and files with errors.
	<i>filesystem:</i>	(Optional) File system or directory containing the files to list, followed by a colon.
	<i>file-url</i>	(Optional) The name of the files to display on a specified device. The files can be of any type. You can use wildcards in the filename. A wildcard character (*) matches all patterns. Strings after a wildcard are ignored.

erase

To erase a file system, use the **erase EXEC** command. The **erase nvram:** command replaces the **write erase** command and the **erase startup-config** command.

erase filesystem:

Syntax Description

<i>filesystem:</i>	File system name, followed by a colon. For example, flash: or nvram:
--------------------	--

erase bootflash

The **erase bootflash:** and **erase bootflash** commands have identical functions. See the description of the **erase** command in this chapter for more information.

file prompt

To specify the level of prompting, use the **file prompt** global configuration command.

file prompt [alert | noisy | quiet]

Syntax Description

alert	(Optional) Prompts only for destructive file operations. This is the default.
noisy	(Optional) Confirms all file operation parameters.
quiet	(Optional) Seldom prompts for file operations.

format

To format a Class A or Class C Flash file system, use the **format EXEC** command.

Class C Flash File System

format filesystem1:

Class A Flash File System

format [spare spare-number] filesystem1: [[filesystem2:][monlib-filename]]



Caution

Reserve a certain number of memory sectors as spares, so that if some sectors fail, most of the Flash memory card can still be used. Otherwise, you must reformat the Flash card when some of the sectors fail.

Syntax Description	spare	(Optional) Reserves spare sectors as specified by the <i>spare-number</i> argument when formatting Flash memory.
	<i>spare-number</i>	(Optional) Number of the spare sectors to reserve on formatted Flash memory. Valid values are from 0 to 16. The default value is zero.
	<i>filesystem1:</i>	Flash memory to format, followed by a colon.
	<i>filesystem2:</i>	(Optional) File system containing the monlib file to use for formatting filesystem1 followed by a colon.
	<i>monlib-filename</i>	(Optional) Name of the ROM monitor library file (monlib file) to use for formatting the <i>filesystem1</i> argument. The default monlib file is the one bundled with the system software. When used with HSA and you do not specify the <i>monlib-filename</i> argument, the system takes ROM monitor library file from the slave image bundle. If you specify the <i>monlib-filename</i> argument, the system assumes that the files reside on the slave devices.

fsck

To check a Class C Flash file system for damage and repair any problems, use the **fsck** EXEC command.

```
fsck [/nocrc] filesystem:
```

Syntax Description	/nocrc	(Optional) Omits cyclic redundancy checks (CRCs).
	<i>filesystem:</i>	The file system to check.

mkdir

To create a new directory in a Class C Flash file system, use the **mkdir** EXEC command.

```
mkdir directory
```

Syntax Description	<i>directory</i>	The name of the directory to create.
---------------------------	------------------	--------------------------------------

more

To display a file, use the **more** EXEC command.

```
more [/ascii | /binary | /ebcdic] file-url
```

Syntax Description	/ascii	(Optional) Displays a binary file in ASCII format.
	/binary	(Optional) Displays a file in hex/text format.
	/ebcdic	(Optional) Displays a binary file in EBCDIC format.
	<i>file-url</i>	The URL of the file to display.

pwd

To show the current setting of the **cd** command, use the **pwd** EXEC command.

```
pwd
```

Syntax Description This command has no arguments or keywords.

rename

To rename a file in a Class C Flash file system, use the **rename** EXEC command.

```
rename url1 url2
```

Syntax Description	<i>url1</i>	The original path and filename.
	<i>url2</i>	The new path and filename.

rmdir

To remove an existing directory in a Class C Flash file system, use the **rmdir** EXEC command.

```
rmdir directory
```

Syntax Description	<i>directory</i>	Directory to delete.
---------------------------	------------------	----------------------

show configuration

The **show configuration** command is replaced by the **show startup-config** and **more nvram:startup-config** commands. See the description of the **show startup-config** and **more** commands for more information.

show file descriptors

To display a list of open file descriptors, use the **show file descriptors** EXEC command.

```
show file descriptors
```

Syntax Description This command has no arguments or keywords.

show file information

To display information about a file, use the **show file information** EXEC command.

```
show file information file-url
```

Syntax Description	<i>file-url</i>	The URL of the file to display.
---------------------------	-----------------	---------------------------------

show file systems

To list available file systems, use the **show file systems** EXEC command.

```
show file systems
```

Syntax Description	This command has no arguments or keywords.	
---------------------------	--	--

squeeze

To permanently delete Flash files by squeezing a Class A Flash file system, use the **squeeze** EXEC command.

```
squeeze filesystem:
```

Syntax Description	<i>filesystem:</i>	The Flash file system, followed by a colon.
---------------------------	--------------------	---

undelete

To recover a file marked “deleted” on a Class A or Class B Flash file system, use the **undelete** EXEC command.

```
undelete index [filesystem:]
```

Syntax Description	<i>index</i>	A number that indexes the file in the dir command output.
	<i>filesystem:</i>	(Optional) A file system containing the file to undelete, followed by a colon.

verify

To verify the checksum of a file on a Flash memory file system, use the **verify** EXEC command.

```
verify filesystem: [file-url]
```

Syntax Description	<i>filesystem:</i>	(Optional) File system or directory containing the files to list, followed by a colon. Standard file system keywords for this command are flash: and bootflash: .
	<i>file-url</i>	(Optional) The name of the files to display on a specified device. The files can be of any type. You can use wildcards in the filename. A wildcard character (*) matches all patterns. Strings after a wildcard are ignored.

write erase

The **write erase** command is replaced by the **erase nvram:** command. See the description of the **erase** command in this chapter for more information.

write terminal

The **write terminal** command is replaced by the **more system:running-config**. See the description of the **more** command in this chapter for more information.



Configuration File Management Commands

This chapter describes the function and syntax of the commands used to manage configuration files. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Configuration Fundamentals Command Reference*.

Flash Memory File System Types

Cisco platforms generally use one of three different Flash memory file system types. Some commands are supported on only one or two file system types. This chapter notes commands that are not supported on all file system types.

Use Table 7 to determine which Flash memory file system type your platform uses.

Table 7 Flash Memory File System Types

Type	Platforms
Class A	Cisco 7000 family, Cisco 12000 series routers, LightStream 1010 (LS1010) switch
Class B	Cisco 1003, Cisco 1004, Cisco 1005, Cisco 2500 series, Cisco 3600 series, and Cisco 4000 series routers, and Cisco AS5200 access servers
Class C	Cisco MC3810 multiservice concentrators, disk0 of Cisco SC3640 System Controllers

Replaced Commands

Some commands found in this chapter in previous releases of this book have been replaced. Older commands generally continue to provide the same functionality in the current release, but are no longer documented. Support for the older version of these commands may already be removed on your system, or may be removed in a future Cisco IOS software release.

Table 8 maps the old commands to their replacements.

Table 8 Replaced Commands

Old Command	New Command
configure network	copy ftp:[[[//[username[:password]@]location]/directory]/filename] system:running-config
configure overwrite-network	copy ftp:[[[//[username[:password]@]location]/directory]/filename] nvram:startup-config
copy rcp running-config	copy rcp:[[[//[username@]location]/directory]/filename] system:running-config
copy running-config rcp	copy system:running-config rcp:[[[//[username@]location]/directory]/filename]
copy running-config startup-config	copy system:running-config nvram:startup-config  Note The copy running-config startup-config command has been replaced by the command shown here. However, the copy running-config startup-config command will continue to be supported as a command alias for the copy system:running-config nvram:startup-config command.
copy running-config tftp	copy system:running-config tftp:[[[//location]/directory]/filename]
copy tftp running-config	copy tftp:[[[//location]/directory]/filename] system:running-config
copy tftp startup-config	copy tftp:[[[//location]/directory]/filename] nvram:startup-config
erase startup-config	erase nvram:
show configuration	more nvram:startup-config
show file	more
show running-config	more system:running-config  Note The show running-config command has been replaced by the command shown here. However, the show running-config command will continue to be supported as a command alias for the more system:running-config command.
show startup-config	more nvram:startup-config  Note The show startup-config command has been replaced by the command shown here. However, the show startup-config command will continue to be supported as a command alias for the more nvram:startup-config command.
write erase	erase nvram:

Table 8 Replaced Commands (continued)

Old Command	New Command
write memory	copy running-config startup-config or copy system:running-config nvram:startup-config
write network	copy system:running-config ftp:[[[//[username[:password]@]location]/directory]/filename]
write terminal	show running-config or more system:running-config

For more information about these command replacements, see the description of the Cisco IOS File System (IFS) in the “Using the Cisco IOS File System” chapter in the Release 12.2 *Cisco IOS Configuration Fundamentals Configuration Guide*.

boot buffersize

To modify the buffer size used to load configuration files, use the **boot buffersize** global configuration command. To return to the default setting, use the **no** form of this command.

boot buffersize *bytes*

no boot buffersize

Syntax Description	<i>bytes</i>	Specifies the size of the buffer to be used. There is no minimum or maximum size that can be specified.
--------------------	--------------	---

boot config

To specify the device and filename of the configuration file from which the router configures itself during initialization (startup), use the **boot config** global configuration command. This command is only available on Class A file system platforms. To remove the specification, use the **no** form of this command.

boot config *file-system-prefix:[directory]/filename*

no boot config

Syntax Description	<i>file-system-prefix:</i>	File system, followed by a colon (for example, nvram: , flash: , or slot0:).
	<i>directory/</i>	(Optional) File system directory the configuration file is located in, followed by a forward slash (/).
	<i>filename</i>	Name of the configuration file.

boot host

To specify the host-specific configuration file to be used at the next system startup, use the **boot host** global configuration command. To restore the host configuration filename to the default, use the **no** form of this command.

boot host *remote-url*

no boot host *remote-url*

Syntax Description	<i>remote-url</i>	Location of the configuration file. Use the following syntax: <ul style="list-style-type: none"> • ftp:[[[//[<i>username[:password]</i>@]<i>location</i>]/<i>directory</i>]/<i>filename</i>] • rnp:[[[//[<i>username</i>@]<i>location</i>]/<i>directory</i>]/<i>filename</i>] • tftp:[[[//[<i>location</i>]/<i>directory</i>]/<i>filename</i>]
---------------------------	-------------------	--

boot network

To change the default name of the network configuration file from which to load configuration commands, use the **boot network** global configuration command. To restore the network configuration filename to the default, use the **no** form of this command.

boot network *remote-url*

no boot network *remote-url*

Syntax Description	<i>remote-url</i>	Location of the configuration file. Use the following syntax: <ul style="list-style-type: none"> • ftp:[[[//[<i>username[:password]</i>@]<i>location</i>]/<i>directory</i>]/<i>filename</i>] • rnp:[[[//[<i>username</i>@]<i>location</i>]/<i>directory</i>]/<i>filename</i>] • tftp:[[[//[<i>location</i>]/<i>directory</i>]/<i>filename</i>]
---------------------------	-------------------	--

clear parser cache

To clear the parse cache entries and hit/miss statistics stored for the Parser Cache feature, use the **clear parser cache** command in privileged EXEC mode.

clear parser cache

Syntax Description	This command has no arguments or keywords.
---------------------------	--

configure

To enter global configuration mode or to configure the system from the system memory, use the **configure** privileged EXEC command. .

configure { **terminal** | **memory** }

Syntax Description	terminal	memory
	Enters global configuration mode to allow you to configure the system from the terminal.	Configures the system with the commands found in the default NVRAM configuration file.
		For the Class A Flash file system platforms, configures the system with the configuration file specified by the CONFIG_FILE environment variable.

configure overwrite-network

The **configure overwrite-network** has been replaced by the **copy** {*ftp-url* | *rcp-url* | *ftp-url*} **nvram:startup-config** command. See the description of the **copy** command in the “Cisco IOS File System Commands” chapter for more information.

parser cache

To reenble the Cisco IOS software parser cache after disabling it, use the **parser cache** global configuration command. To disable the parser cache, use the **no** form of this command.

parser cache

no parser cache

Syntax Description This command has no arguments or keywords.

service compress-config

To compress startup configuration files, use the **service compress-config** global configuration command. To disable compression, use the **no** form of this command.

service compress-config

no service compress-config

Syntax Description This command has no arguments or keywords.

service config

To enable autoloading of configuration files from a network server, use the **service config** global configuration command. To restore the default, use the **no** form of this command.

service config

no service config

Syntax Description This command has no arguments or keywords.

show configuration

The **show configuration** command has been replaced by the **show startup-config** and **more nvram:startup-config** commands. See the description of the **more** command in the “Cisco IOS File System Commands” chapter for more information.

show file

The **show file** command has been replaced by the **more** command. See the description of the **more** command in the “Cisco IOS File System Commands” chapter for more information.

show parser statistics

To displays statistics about the last configuration file parsed and the status of the Parser Cache feature, use the **show parser statistics** command in privileged EXEC mode.

show parser statistics

Syntax Description This command has no arguments or keywords.

show running-config

To display the contents of the currently running configuration file, the configuration for a specific interface, or map class information, use the **show running-config** privileged EXEC command.

show running-config [**interface** *type number* |
map-class [**dialer** [*map-class-name*] | **frame-relay** [*map-class-name*]]]

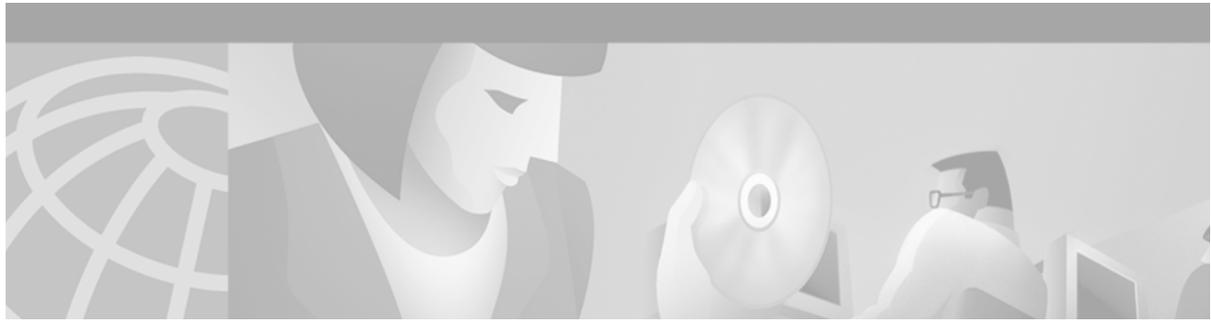
Syntax Description

interface <i>type number</i>	(Optional) Displays interface specific configuration information. If you use the interface keyword, you must specify the interface type and the interface number (for example, interface ethernet 0). Common interfaces include async, ethernet, fastEthernet, group-async, loopback, null, serial, and virtual-template. Use the show run interface ? command to determine the interfaces available on your system.
map-class	(Optional) Displays only map-class configuration information.
map-class dialer	(Optional) Displays only map-class dialer configuration information.
map-class dialer <i>map-class-name</i>	(Optional) Displays only dialer configuration information for the specified map class.
map-class frame-relay	(Optional) Displays only Frame Relay configuration information.
map-class frame-relay <i>map-class-name</i>	(Optional) Displays only Frame Relay configuration information for the specified map class.

show startup-config

The **more nvram:startup-config** command has been replaced by the **show startup-config** command. See the description of the **more** command in the “Cisco IOS File System Commands” chapter for more information.

■ show startup-config



System Image and Microcode Commands

This chapter describes the function and syntax of the commands used to load and copy system images and microcode images. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Configuration Fundamentals Command Reference*.

Flash Memory File System Types

Cisco platforms generally use one of three different Flash memory file system types. Some commands in this chapter are supported on only one or two file system types.

Use Table 9 to determine which Flash memory file system type your platform uses.

Table 9 Flash Memory File System Types

Type	Platforms
Class A	Cisco 7000 family, Cisco 12000 series routers, LightStream1010 (LS1010) switches
Class B	Cisco 1003, Cisco 1004, Cisco 1005, Cisco 2500 series, Cisco 3600 series, and Cisco 4000 series routers, and Cisco AS5200 access servers
Class C	Cisco MC3810 multiservice concentrators, disk0 of Cisco SC3640 system controllers

Replaced Commands

Some commands found in this chapter in previous releases of this book have been replaced. Older commands generally continue to provide the same functionality in the current release, but are no longer documented. Support for the older version of these commands may already be removed on your system, or may be removed in a future Cisco IOS software release.

Table 10 maps the old commands to their replacements.

Table 10 Replaced Commands

Old Command	New Command
copy erase flash	erase flash: (Class B Flash file systems only) format (Class A and C Flash file systems only)
copy verify	verify
copy verify bootflash	verify bootflash:
copy verify flash	verify flash:
copy xmodem	xmodem
copy ymodem	xmodem -y
show flh-log	more flh: logfile
verify bootflash	verify bootflash:
verify flash	verify flash:

For a description of the **copy** and **verify** commands, see the “Cisco IOS File System Commands” chapter.

copy erase flash

The **copy erase flash** command has been replaced by the **erase flash:** command. See the description of the **erase** command in the “Cisco IOS File System Commands” chapter for more information.

copy verify

The **copy verify** command has been replaced by the **verify** command. See the description of the **verify** command in the “Cisco IOS File System Commands” chapter for more information.

copy verify bootflash

The **copy verify bootflash** command has been replaced by the **verify bootflash:** command. See the description of the **verify** command in the “Cisco IOS File System Commands” chapter for more information.

copy verify flash

The **copy verify flash** command has been replaced by the **verify flash:** command. See the description of the **verify** command in the “Cisco IOS File System Commands” chapter for more information.

copy xmodem:

To copy a Cisco IOS image from a local or remote computer (such as a PC, Macintosh, or UNIX workstation) to Flash memory on a Cisco 3600 series router using the Xmodem protocol, use the **copy xmodem:** EXEC command.

copy xmodem: *flash-filesystem:*

Syntax Description

flash-filesystem:

Destination of the copied file, followed by a colon.

copy ymodem:

To copy a Cisco IOS image from a local or remote computer (such as a PC, Macintosh, or UNIX workstation) to Flash memory on a Cisco 3600 series router using the Ymodem protocol, use the **copy ymodem:** EXEC command.

copy ymodem: *flash-filesystem:*

Syntax Description

flash-filesystem:

Destination of the copied file, followed by a colon.

erase flash:

The **erase flash:** and **erase flash** commands are identical. See the description of the **erase** command in the “Cisco IOS File System Commands” chapter for more information.

microcode (7000/7500)

To specify the location of the microcode that you want to download from Flash memory into the writable control store (WCS) on Cisco 7000 series (including RSP based routers) or Cisco 7500 series routers, use the **microcode** global configuration command. To load the microcode bundled with the system image, use the **no** form of this command.

microcode *interface-type* {*flash-filesystem:filename* [*slot*] | **rom** | **system** [*slot*]}

no microcode *interface-type* {*flash-filesystem:filename* [*slot*] | **rom** | **system** [*slot*]}

Syntax Description	<i>interface-type</i>	One of the following interface processor names: aip , cip , eip , feip , fip , fsip , hip , mip , sip , sp , ssp , trip , vip , or vip2 .
	<i>flash-filesystem:</i>	Flash file system, followed by a colon. Valid file systems are bootflash , slot0 , and slot1 . Slave devices such as slaveslot0 are invalid. The slave's file system is not available during microcode reloads.
	<i>filename</i>	Name of the microcode file.
	<i>slot</i>	(Optional) Number of the slot. Range is from 0 to 15.
	rom	If ROM is specified, the router loads from the onboard ROM microcode.
	system	If the system keyword is specified, the router loads the microcode from the microcode bundled into the system image you are running for that interface type.

microcode (7200)

To configure a default override for the microcode that is downloaded to the hardware on a Cisco 7200 series router, use the **microcode** global configuration command. To revert to the default microcode for the current running version of the Cisco IOS software, use the **no** form of this command.

```
microcode {ecpa | pcpa} location
```

```
no microcode {ecpa | pcpa}
```

Syntax Description	ecpa	ESCON Channel Port Adapter (CPA) interface.
	pcpa	Parallel CPA interface.
	<i>location</i>	Location of microcode, including the device and filename.

microcode (12000)

To load a Cisco IOS software image on a line card from Flash memory or the GRP card on a Cisco 12000 series Gigabit Switch Router (GSR), use the **microcode** global configuration command. To load the microcode bundled with the GRP system image, use the **no** form of this command.

```
microcode {oc12-atm | oc12-pos | oc3-pos4} {flash file-id [slot] | system [slot]}
```

```
no microcode {oc12-atm | oc12-pos | oc3-pos4} [flash file-id [slot] | system [slot]]
```

Syntax Description	oc12-atm oc12-pos oc3-pos4	Interface name.
	flash	Loads the image from the Flash file system.

<i>file-id</i>	Specifies the device and filename of the image file to download from Flash memory. A colon (:) must separate the device and filename (for example, slot0:gsr-p-mz). Valid devices include: <ul style="list-style-type: none"> • bootflash:—Internal Flash memory. • slot0:—First PCMCIA slot. • slot1:—Second PCMCIA slot.
<i>slot</i>	(Optional) Slot number of the line card that you want to copy the software image to. Slot numbers range from 0 to 11 for the Cisco 12012 router and 0 to 7 for the Cisco 12008 router. If you do not specify a slot number, the Cisco IOS software image is downloaded on all line cards.
system	Loads the image from the software image on the GRP card.

microcode reload (7000/7500)

To reload the processor card on the Cisco 7000 series with RSP7000 or Cisco 7500 series routers, use the **microcode reload** global configuration command.

microcode reload

Syntax Description

This command has no arguments or keywords.

microcode reload (7200)

To reload the Cisco IOS microcode image on an ESCON CPA card in the Cisco 7200 series router, use the **microcode reload** command in privileged EXEC configuration mode.

microcode reload {**all** | **ecpa** [slot *slot#*] | **pcpa** [slot *slot#*]}

Syntax Description

all	Resets and reloads all hardware types that support downloadable microcode.
ecpa	Resets and reloads only those slots that contain hardware type ecpa .
pcpa	Resets and reloads only those slots that contain hardware type pcpa .
slot <i>slot#</i>	(Optional) Resets and reloads only the slot specified, and only if it contains the hardware specified.

microcode reload (12000)

To reload the Cisco IOS image from a line card on Cisco 12000 series routers, use the **microcode reload** global configuration command.

microcode reload [*slot-number*]

Syntax Description	<i>slot-number</i>	(Optional) Slot number of the line card that you want to reload the Cisco IOS software image on. Slot numbers range from 0 to 11 for the Cisco 12012 and from 0 to 7 for the Cisco 12008 router. If you do not specify a slot number, the Cisco IOS software image is reloaded on all line cards.
---------------------------	--------------------	---

more flh:logfile

To view the system console output generated during the Flash load helper operation, use the **more flh:logfile** privileged EXEC command.

more flh:logfile

Syntax Description	This command has no arguments or keywords.
---------------------------	--

show flh-log

The **show flh-log** command has been replaced by the **more flh:logfile** command. See the description of the **more flh:logfile** command in this chapter for more information.

show microcode

To display microcode image information available on line cards, use the **show microcode** EXEC command.

show microcode

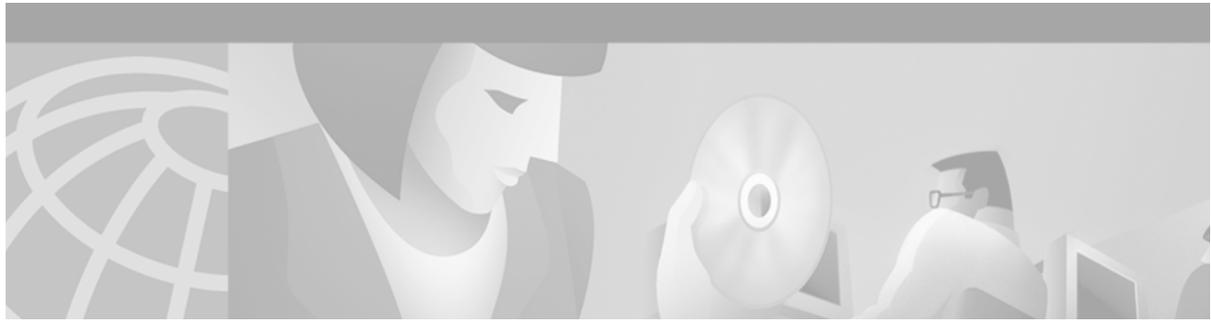
Syntax Description	This command has no arguments or keywords.
---------------------------	--

xmodem

To copy a Cisco IOS image to a router using the ROM monitor and the Xmodem or Ymodem protocol, use the **xmodem** ROM monitor command.

```
xmodem [-c] [-y] [-e] [-f] [-r] [-x] [-s data-rate] [filename]
```

Syntax Description	
-c	(Optional) CRC-16 checksumming, which is more sophisticated and thorough than standard checksumming.
-y	(Optional) Uses the Ymodem protocol for higher throughput.
-e	(Optional) Erases the first partition in Flash memory before starting the download. This option is only valid for the Cisco 1600 series.
-f	(Optional) Erases all of Flash memory before starting the download. This option is only valid for the Cisco 1600 series.
-r	(Optional) Downloads the file to DRAM. The default is Flash memory.
-x	(Optional) Do not execute Cisco IOS image on completion of the download.
-s <i>data-rate</i>	(Optional) Sets the console port's data rate during file transfer. Values are 1200 , 2400 , 4800 , 9600 , 19200 , 38400 , and 115200 bps. The default rate is specified in the configuration register. This option is only valid for the Cisco 1600 series.
<i>filename</i>	(Optional) Filename to copy. This argument is ignored when the -r keyword is specified, because only one file can be copied to DRAM. On the Cisco 1600 series routers, files are loaded to the ROM for execution.



Router Memory Commands

This chapter describes the function and syntax of the commands used to maintain router memory. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Configuration Fundamentals Command Reference*.

Flash Memory File System Types

Cisco platforms generally use one of three different Flash memory file system type. Some commands are supported on only one or two file system types.

Use Table 11 to determine which Flash memory file system type your platform uses.

Table 11 Flash Memory File System Types

Type	Platforms
Class A	Cisco 7000 family, Cisco 12000 series, LightStream 1010 (LS1010) series
Class B	Cisco 1003, Cisco 1004, Cisco 1005, Cisco 2500 series, Cisco 3600 series, Cisco 4000 series, Cisco AS5200 access servers
Class C	Cisco MC3810 multiservice concentrators; disk0 and disk1 of Cisco SC3640 system controllers

memory scan

To enable the Memory Scan feature on a Cisco 7500 series router, use the **memory scan** command. To restore the router configuration to the default, use the **no** form of this command.

memory scan

no memory scan

Syntax Description This command has no arguments or keywords.

memory-size iomem

To reallocate the percentage of DRAM to use for I/O memory and processor memory on Cisco 3600 series routers, use the **memory-size iomem** global configuration command. To revert to the default memory allocation, use the **no** form of this command.

memory-size iomem *i/o-memory-percentage*

no memory-size iomem *i/o-memory-percentage*

Syntax Description

<i>i/o-memory-percentage</i>	The percentage of DRAM allocated to I/O memory. The values permitted are 10 , 15 , 20 , 25 , 30 , 40 , and 50 . A minimum of 4 MB of memory is required for I/O memory.
------------------------------	--

partition

To separate Flash memory into partitions on Class B file system platforms, use the **partition** global configuration command. To undo partitioning and to restore Flash memory to one partition, use the **no** form of this command.

Cisco 1600 Series and Cisco 3600 Series Routers

partition *flash-filesystem:* [*number-of-partitions*][*partition-size*]

no partition *flash-filesystem:*

All Other Class B Platforms

partition flash *partitions* [*size1* *size2*]

no partition flash

Syntax Description

<i>flash-filesystem:</i>	One of the following Flash file systems, which must be followed by a colon (:). The Cisco 1600 series can only use the flash: keyword. <ul style="list-style-type: none"> flash:—Internal Flash memory slot0:—Flash memory card in PCMCIA slot 0 slot1:—Flash memory card in PCMCIA slot 1
<i>number-of-partitions</i>	(Optional) Number of partitions in Flash memory.
<i>partition-size</i>	(Optional) Size of each partition. The number of partition size entries must be equal to the number of specified partitions.
<i>partitions</i>	Number of partitions in Flash memory. Can be 1 or 2.
<i>size1</i>	(Optional) Size of the first partition (in megabytes).
<i>size2</i>	(Optional) Size of the second partition (in megabytes).

show (Flash file system)

To display the layout and contents of a Flash memory file system, use the **show** EXEC command.

Class A Flash File Systems

show flash-filesystem: [**all** | **chips** | **fileSYS**]

Class B Flash File Systems

show flash-filesystem: [**partition number**] [**all** | **chips** | **detailed** | **err** | **summary**]

Class C Flash File Systems

show flash-filesystem:

Syntax Description	
<i>flash-filesystem:</i>	Flash memory file system (bootflash: , flash: , slot0: , slot1: , slavebootflash: , slaveslot0: , or slaveslot1:), followed by a colon.
all	(Optional) On Class B Flash file systems, all keyword displays complete information about Flash memory, including information about the individual ROM devices in Flash memory and the names and sizes of all system image files stored in Flash memory, including those that are invalid. On Class A Flash file systems, the all keyword displays the following information: <ul style="list-style-type: none"> The information displayed when no keywords are used. The information displayed by the fileSYS keyword. The information displayed by the chips keyword.
chips	(Optional) Displays information per partition and per chip, including which bank the chip is in, plus its code, size, and name.
fileSYS	(Optional) Displays the Device Info Block, the Status Info, and the Usage Info.
partition number	(Optional) Displays output for the specified partition number. If you do not specify a partition in the command, the router displays output for all partitions. You can use this keyword only when Flash memory has multiple partitions.
detailed	(Optional) Displays detailed file directory information per partition, including file length, address, name, Flash memory checksum, computer checksum, bytes used, bytes available, total bytes, and bytes of system Flash memory.
err	(Optional) Displays write or erase failures in the form of number of retries.
summary	(Optional) Displays summary information per partition, including the partition size, bank size, state, and method by which files can be copied into a particular partition. You can use this keyword only when Flash memory has multiple partitions.

show memory scan

To monitor the number and type of parity (memory) errors on your system, use the **show memory scan EXEC** command.

show memory scan

Syntax Description This command has no arguments or keywords.

write memory

The **write memory** command has been replaced by the **copy system:running-config nvram:startup-config** command. See the description of the **copy** command in the “Cisco IOS File System Commands” chapter for more information.

write network

The **write network** command is replaced by the **copy system:running-config destination-url**. See the description of the **copy** command in the “Cisco IOS File System Commands” chapter for more information.



Booting Commands

This chapter describes the function and syntax of the commands used to modify the rebooting procedures of the router. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Configuration Fundamentals Command Reference*.

Flash Memory File System Types

Cisco platforms generally use one of three different Flash memory file system types. Some commands are supported on only one or two file system types. This chapter notes commands that are not supported on all file system types.

Use Table 12 to determine which Flash memory file system type your platform uses.

Table 12 Flash Memory File System Types

Type	Platforms
Class A	Cisco 7000 family, Cisco 12000 series, LightStream 1010 (LS1010)
Class B	Cisco 1003, Cisco 1004, Cisco 1005, Cisco 2500 series, Cisco 3600 series, Cisco 4000 series, Cisco AS5200 access servers
Class C	Cisco MC3810 multiservice concentrators, disk0 of Cisco SC3640 system controllers

boot

To boot the router manually, use the **boot** ROM monitor command. The syntax of this command varies according to the platform and ROM monitor version.

boot

boot *file-url*

boot *filename* [*tftp-ip-address*]

boot flash [*flash-fs:*][*partition-number:*][*filename*]

Cisco 7000 Series, 7200 Series, 7500 Series Routers

boot *flash-fs:*[*filename*]

Cisco 1600 and Cisco 3600 Series Routers

```
boot [flash-fs:][partition-number:][filename]
```

Syntax Description	
<i>file-url</i>	URL of the image to boot (for example, <code>boot tftp://172.16.15.112/routerest</code>).
<i>filename</i>	<p>When used in conjunction with the <i>ip-address</i> argument, the <i>filename</i> argument is the name of the system image file to boot from a network server. The filename is case sensitive.</p> <p>When used in conjunction with the flash keyword, the <i>filename</i> argument is the name of the system image file to boot from Flash memory.</p> <p>On all platforms except the Cisco 1600 series, Cisco 3600 series, and Cisco 7000 family routers, the system obtains the image file from internal Flash memory.</p> <p>On the Cisco 1600 series, Cisco 3600 series and Cisco 7000 family routers, the <i>flash-fs:</i> argument specifies the Flash memory device from which to obtain the system image. (See the <i>flash-fs:</i> argument later in this table for valid device values.) The filename is case sensitive. Without the <i>filename</i> argument, the first valid file in Flash memory is loaded.</p>
<i>tftp-ip-address</i>	(optional) IP address of the TFTP server on which the system image resides. If omitted, this value defaults to the IP broadcast address of 255.255.255.255.
flash	Boots the router from Flash memory. Note that this keyword is required in some boot images.
<i>flash-fs:</i>	<p>(Optional) Specifying the Flash file system is optional for all platforms except the Cisco 7500 series routers. Possible file systems are:</p> <ul style="list-style-type: none"> • flash:—Internal Flash memory on the Cisco 1600 series routers and Cisco 3600 series routers. This is the only valid Flash file system for the Cisco 1600 series routers. • bootflash:—Internal Flash memory on the Cisco 7000 family. • slot0:—Flash memory card in the first PCMCIA slot on the Cisco 7000 family and Cisco 3600 series routers. • slot1:—Flash memory card in the second PCMCIA slot on the Cisco 7000 family and Cisco 3600 series routers.
<i>partition-number:</i>	(Optional) Specifies the partition number of the file system the file should be loaded from. This argument is not available on all platforms.

boot bootldr

To specify the location of the boot image that ROM uses for booting, use the **boot bootldr** global configuration command. To remove this boot image specification, use the **no** form of this command.

boot bootldr *file-url*

no boot bootldr

Syntax Description	<i>file-url</i>	URL of the boot image on a Flash file system.
---------------------------	-----------------	---

boot bootstrap

To configure the filename that is used to boot a secondary bootstrap image, use the **boot bootstrap** global configuration command. To disable booting from a secondary bootstrap image, use the **no** form of this command.

boot bootstrap *file-url*

no boot bootstrap *file-url*

boot bootstrap flash [*filename*]

no boot bootstrap flash [*filename*]

boot bootstrap [tftp] *filename* [*ip-address*]

no boot bootstrap [tftp] *filename* [*ip-address*]

Syntax Description	<i>file-url</i>	URL of the bootstrap image.
	flash	Boots the router from Flash memory.
	<i>filename</i>	(Optional with flash) Name of the system image to boot from a network server or from Flash memory. If you omit the filename when booting from Flash memory, the router uses the first system image stored in Flash memory.
	tftp	(Optional) Boots the router from a system image stored on a TFTP server.
	<i>ip-address</i>	(Optional) IP address of the TFTP server on which the system image resides. If omitted, this value defaults to the IP broadcast address of 255.255.255.255.

boot system

To specify the system image that the router loads at startup, use one of the following **boot system** global configuration commands. To remove the startup system image specification, use the **no** form of the command.

boot system *file-url*

no boot system *file-url*

boot system flash [*flash-fs*][:*partition-number*][:*filename*]

no boot system flash [*flash-fs*][:*partition-number*][:*filename*]

boot system mop *filename* [*mac-address*] [*interface*]

no boot system mop *filename* [*mac-address*] [*interface*]

boot system rom

no boot system rom

boot system {*rcp* | *tftp* | *ftp*} *filename* [*ip-address*]

no boot system {*rcp* | *tftp* | *ftp*} *filename* [*ip-address*]

no boot system

Syntax Description

<i>file-url</i>	URL of the system image to load at system startup.
flash	<p>On all platforms except the Cisco 1600 series, Cisco 3600 series, and Cisco 7000 family routers, this keyword boots the router from internal Flash memory. If you omit all arguments that follow this keyword, the system searches internal Flash for the first bootable image.</p> <p>On the Cisco 1600 series, Cisco 3600 series, and Cisco 7000 family routers, this keyword boots the router from a Flash device, as specified by the device: argument. On the Cisco 1600 series and Cisco 3600 series routers, if you omit all optional arguments, the router searches internal Flash memory for the first bootable image. On the Cisco 7000 family routers, when you omit all arguments that follow this keyword, the system searches the PCMCIA slot 0 for the first bootable image.</p>
<i>flash-fs</i> :	<p>(Optional) Flash file system containing the system image to load at startup. The colon is required. Valid file systems are as follows:</p> <ul style="list-style-type: none"> • flash—Internal Flash memory on the Cisco 1600 series and Cisco 3600 series routers. For the Cisco 1600 series and Cisco 3600 series routers, this file system is the default if you do not specify a file system. This is the only valid file system for the Cisco 1600 series. • bootflash—Internal Flash memory in the Cisco 7000 family. • slot0—First PCMCIA slot on the Cisco 3600 series and Cisco 7000 family routers. For the Cisco 7000 family routers, this file system is the default if you do not specify a file system. • slot1—Flash memory card in the second PCMCIA slot on the Cisco 3600 series and Cisco 7000 family routers.
<i>partition-number</i> :	(Optional) Number of the Flash memory partition that contains the system image to boot, specified by the optional <i>filename</i> argument. If you do not specify a filename, the router loads the first valid file in the specified partition of Flash memory. This argument is only valid on routers that can be partitioned.

<i>filename</i>	(Optional when used with the boot system flash command) Name of the system image to load at startup. It is case sensitive. If you do not specify a filename, the router loads the first valid file in the specified Flash file system, the specified partition of Flash memory, or the default Flash file system if you also omit the <i>flash-fs:</i> argument.
mop	Boots the router from a system image stored on a Digital MOP server. Do not use this keyword with the Cisco 3600 series or Cisco 7000 family routers.
<i>mac-address</i>	(Optional) MAC address of the MOP server containing the specified system image file. If you do not include the MAC address argument, the router sends a broadcast message to all MOP boot servers. The first MOP server to indicate that it has the specified file is the server from which the router gets the boot image.
<i>interface</i>	(Optional) Interface the router uses to send out MOP requests to the MOP server. The interface options are async , dialer , ethernet , serial , and tunnel . If you do not specify the <i>interface</i> argument, the router sends a request out on all interfaces that have MOP enabled. The interface that receives the first response is the interface the router uses to load the software.
rom	Boots the router from ROM. Do not use this keyword with the Cisco 3600 series or the Cisco 7000 family routers.
rcp	Boots the router from a system image stored on a network server using rcp.
tftp	Boots the router from a system image stored on a TFTP server.
ftp	Boots the router from a system image stored on an FTP server.
<i>ip-address</i>	(Optional) IP address of the server containing the system image file. If omitted, this value defaults to the IP broadcast address of 255.255.255.255.

config-register

To change the configuration register settings, use the **config-register** global configuration command.

config-register *value*

Syntax Description	
<i>value</i>	Hexadecimal or decimal value that represents the 16-bit configuration register value that you want to use the next time the router is restarted. The value range is from 0x0 to 0xFFFF (0 to 65535 in decimal).

confreg

To change the configuration register settings while in ROM monitor mode, use the **confreg** ROM monitor command.

confreg [*value*]

Syntax Description

<i>value</i>	(Optional) Hexadecimal value that represents the 16-bit configuration register value that you want to use the next time the router is restarted. The value range is from 0x0 to 0xFFFF.
--------------	---

continue

To return to EXEC mode from ROM monitor mode, use the **continue** ROM monitor command.

continue

Syntax Description

This command has no arguments or keywords.

reload

To reload the operating system, use the **reload** EXEC command.

reload [*text* | **in** [*hh:mm*] [*text*] | **at** *hh:mm* [*month day* | *day month*] [*text*] | **cancel**]

Syntax Description

<i>text</i>	(Optional) Reason for the reload, 1 to 255 characters long.
in [<i>hh:mm</i>]	(Optional) Schedule a reload of the software to take effect in the specified minutes or hours and minutes. The reload must take place within approximately 24 days.
at <i>hh:mm</i>	(Optional) Schedule a reload of the software to take place at the specified time (using a 24-hour clock). If you specify the month and day, the reload is scheduled to take place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within approximately 24 days.
<i>month</i>	(Optional) Name of the month, any number of characters in a unique string.
<i>day</i>	(Optional) Number of the day in the range from 1 to 31.
cancel	(Optional) Cancel a scheduled reload.

show boot

The **show boot** command has been replaced by the **show bootvar** command. See the description of the **show bootvar** command in this chapter for more information.

show bootvar

To display the contents of the BOOT variable, the name of the configuration file pointed to by the CONFIG_FILE variable, the contents of the BOOTLDR variable, and the configuration register setting, use the **show bootvar** EXEC command.

```
show bootvar
```

Syntax Description This command has no arguments or keywords.

show reload

To display the reload status on the router, use the **show reload** EXEC command.

```
show reload
```

Syntax Description This command has no arguments or keywords.

show version

To display the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images, use the **show version** EXEC command.

```
show version
```

Syntax Description This command has no arguments or keywords.



Basic File Transfer Services Commands

This chapter describes the function and syntax of the commands used to configure basic file transfer services on a Cisco routing device. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Configuration Fundamentals Command Reference*.

async-bootp

To configure extended BOOTP requests for asynchronous interfaces as defined in RFC 1084, use the **async-bootp** global configuration command. To restore the default, use the **no** form of this command.

async-bootp *tag* [:*hostname*] *data*

no async-bootp

Syntax Description

<i>tag</i>	Item being requested; expressed as filename, integer, or IP dotted decimal address. See Table 13 for possible keywords.
<i>:hostname</i>	(Optional) This entry applies only to the host specified. The <i>:hostname</i> argument accepts both an IP address and a logical host name.
<i>data</i>	List of IP addresses entered in dotted decimal notation or as logical host names, a number, or a quoted string.

Table 13 *tag* Keyword Options

Keyword	Description
bootfile	Specifies use of a server boot file from which to download the boot program. Use the optional <i>:hostname</i> argument and the <i>data</i> argument to specify the filename.
subnet-mask <i>mask</i>	Dotted decimal address specifying the network and local subnetwork mask (as defined by RFC 950).
time-offset <i>offset</i>	Signed 32-bit integer specifying the time offset of the local subnetwork in seconds from Coordinated Universal Time (UTC).
gateway <i>address</i>	Dotted decimal address specifying the IP addresses of gateways for this subnetwork. A preferred gateway should be listed first.

Table 13 tag Keyword Options (continued)

Keyword	Description
time-server <i>address</i>	Dotted decimal address specifying the IP address of time servers (as defined by RFC 868).
IEN116-server <i>address</i>	Dotted decimal address specifying the IP address of name servers (as defined by IEN 116).
nbns-server <i>address</i>	Dotted decimal address specifying the IP address of Windows NT servers.
DNS-server <i>address</i>	Dotted decimal address specifying the IP address of domain name servers (as defined by RFC 1034).
log-server <i>address</i>	Dotted decimal address specifying the IP address of an MIT-LCS UDP log server.
quote-server <i>address</i>	Dotted decimal address specifying the IP address of Quote of the Day servers (as defined in RFC 865).
lpr-server <i>address</i>	Dotted decimal address specifying the IP address of Berkeley UNIX Version 4 BSD servers.
impress-server <i>address</i>	Dotted decimal address specifying the IP address of Impress network image servers.
rlp-server <i>address</i>	Dotted decimal address specifying the IP address of Resource Location Protocol (RLP) servers (as defined in RFC 887).
hostname <i>name</i>	The name of the client, which may or may not be domain qualified, depending upon the site.
bootfile-size <i>value</i>	A two-octet value specifying the number of 512-octet (byte) blocks in the default boot file.

ip ftp passive

To configure the router to use only passive File Transfer Protocol (FTP) connections, use the **ip ftp passive** global configuration command. To allow all types of FTP connections, use the **no** form of this command.

ip ftp passive

no ip ftp passive

Syntax Description This command has no arguments or keywords.

ip ftp password

To specify the password to be used for File Transfer Protocol (FTP) connections, use the **ip ftp password** global configuration command. To return the password to its default, use the **no** form of this command.

```
ip ftp password [type] password
```

```
no ip ftp password
```

Syntax Description	<i>type</i>	(Optional) Type of encryption to use on the password. A value of 0 disables encryption. A value of 7 indicates proprietary encryption.
	<i>password</i>	Password to use for FTP connections.

ip ftp source-interface

To specify the source IP address for File Transfer Protocol (FTP) connections, use the **ip ftp source-interface** global configuration command. To use the address of the interface where the connection is made, use the **no** form of this command.

```
ip ftp source-interface interface
```

```
no ip ftp source-interface
```

Syntax Description	<i>interface</i>	The interface type and number to use to obtain the source address for FTP connections.
---------------------------	------------------	--

ip ftp username

To configure the username for File Transfer Protocol (FTP) connections, use the **ip ftp username** global configuration command. To configure the router to attempt anonymous FTP, use the **no** form of this command.

```
ip ftp username username
```

```
no ip ftp username
```

Syntax Description	<i>username</i>	Username for FTP connections.
---------------------------	-----------------	-------------------------------

ip rarp-server

To enable the router to act as a Reverse Address Resolution Protocol (RARP) server, use the **ip rarp-server** interface configuration command. To restore the interface to the default of no RARP server support, use the **no** form of this command.

ip rarp-server *ip-address*

no ip rarp-server *ip-address*

Syntax Description

<i>ip-address</i>	IP address that is to be provided in the source protocol address field of the RARP response packet. Normally, this is set to whatever address you configure as the primary address for the interface.
-------------------	---

ip rcmd domain-lookup

To enable Domain Name System (DNS) security for rcp and rsh, use the **ip rcmd domain-lookup** global configuration command. To bypass DNS security for rcp and rsh, use the **no** form of this command.

ip rcmd domain-lookup

no ip rcmd domain-lookup

Syntax Description

This command has no arguments or keywords.

ip rcmd rcp-enable

To configure the Cisco IOS software to allow remote users to copy files to and from the router, use the **ip rcmd rcp-enable** global configuration command. To disable a router that is enabled for rcp, use the **no** form of this command.

ip rcmd rcp-enable

no ip rcmd rcp-enable

Syntax Description

This command has no arguments or keywords.

ip rcmd remote-host

To create an entry for the remote user in a local authentication database so that remote users can execute commands on the router using rsh or rcp, use the **ip rcmd remote-host** global configuration command. To remove an entry for a remote user from the local authentication database, use the **no** form of this command .

ip rcmd remote-host *local-username* {*ip-address* | *host*} *remote-username* [**enable** [*level*]]

no ip rcmd remote-host *local-username* {*ip-address* | *host*} *remote-username* [**enable** [*level*]]

Syntax Description		
	<i>local-username</i>	Name of the user on the local router. You can specify the router host name as the username. This name needs to be communicated to the network administrator or the user on the remote system. To be allowed to remotely execute commands on the router, the remote user must specify this value correctly.
	<i>ip-address</i>	IP address of the remote host from which the local router will accept remotely executed commands. Either the IP address or the host name is required.
	<i>host</i>	Name of the remote host from which the local router will accept remotely executed commands. Either the host name or the IP address is required.
	<i>remote-username</i>	Name of the user on the remote host from which the router will accept remotely executed commands.
	enable <i>level</i>	(Optional) Enables the remote user to execute privileged EXEC commands using rsh or to copy files to the router using rcp. The range is from 1 to 15. The default is 15. For information on the enable level, refer to the privilege level global configuration command in the Release 12.2 <i>Cisco IOS Security Command Reference</i> .

ip rcmd remote-username

To configure the remote username to be used when requesting a remote copy using rcp, use the **ip rcmd remote-username** global configuration command. To remove from the configuration the remote username, use the **no** form of this command.

ip rcmd remote-username *username*

no ip rcmd remote-username *username*

Syntax Description		
	<i>username</i>	Name of the remote user on the server. This name is used for rcp copy requests. All files and images to be copied are searched for or written relative to the directory of the remote user's account, if the server has a directory structure, for example, as do UNIX systems.

ip rcmd rsh-enable

To configure the router to allow remote users to execute commands on it using rsh, use the **ip rcmd rsh-enable** global configuration command. To disable a router that is enabled for rsh, use the **no** form of this command.

ip rcmd rsh-enable

no ip rcmd rsh-enable

Syntax Description This command has no arguments or keywords.

mop device-code

To identify the type of device sending Maintenance Operation Protocol (MOP) System Identification (sysid) messages and request program messages, use the **mop device-code** global configuration command. To set the identity to the default value, use the **no** form of this command.

mop device-code { cisco | ds200 }

no mop device-code { cisco | ds200 }

Syntax Description	cisco	Denotes a Cisco device code.
	ds200	Denotes a DECserver 200 device code.

mop retransmit-timer

To configure the length of time that the Cisco IOS software waits before resending boot requests to a Maintenance Operation Protocol (MOP) server, use the **mop retransmit-timer** global configuration command. To reinstate the default value, use the **no** form of this command.

mop retransmit-timer *seconds*

no mop retransmit-timer

Syntax Description	<i>seconds</i>	Sets the length of time (in seconds) that the software waits before resending a message. The value is a number from 1 to 20.
---------------------------	----------------	--

mop retries

To configure the number of times the Cisco IOS software will resend boot requests to a Maintenance Operation Protocol (MOP) server, use the **mop retries** global configuration command. To reinstate the default value, use the **no** form of this command.

mop retries *count*

no mop retries

Syntax Description	<i>count</i>	Indicates the number of times the software will resend a MOP boot request. The value is a number from 3 to 24.
---------------------------	--------------	--

rsh

To execute a command remotely on a remote rsh host, use the **rsh** privileged EXEC command.

rsh {*ip-address* | *host*} [**/user** *username*] *remote-command*

Syntax Description	<i>ip-address</i>	IP address of the remote host on which to execute the rsh command. Either the IP address or the host name is required.
	<i>host</i>	Name of the remote host on which to execute the command. Either the host name or the IP address is required.
	/user <i>username</i>	(Optional) Remote username.
	<i>remote-command</i>	Command to be executed remotely.

show async-bootp

To display the extended BOOTP request parameters that have been configured for asynchronous interfaces, use the **show async-bootp** privileged EXEC command.

show async-bootp

Syntax Description	This command has no arguments or keywords.
---------------------------	--

tftp-server

To configure a router or a Flash memory device on the router as a TFTP server, use one of the following **tftp-server** global configuration commands. This command replaces the **tftp-server system** command. To remove a previously defined filename, use the **no tftp-server** command with the appropriate filename.

```
tftp-server flash [partition-number:]filename1 [alias filename2] [access-list-number]
```

```
tftp-server rom alias filename1 [access-list-number]
```

```
no tftp-server { flash [partition-number:]filename1 | rom alias filename2 }
```

Cisco 1600 Series and Cisco 3600 Series Routers

```
tftp-server flash [device:][partition-number:]filename
```

```
no tftp-server flash [device:][partition-number:]filename
```

Cisco 7000 Family Routers

```
tftp-server flash device:filename
```

```
no tftp-server flash device:filename
```

Syntax Description

flash	Specifies TFTP service of a file in Flash memory.
rom	Specifies TFTP service of a file in ROM.
<i>filename1</i>	Name of a file in Flash or in ROM that the TFTP server uses in answering TFTP Read Requests.
alias	Specifies an alternate name for the file that the TFTP server uses in answering TFTP Read Requests.
<i>filename2</i>	Alternate name of the file that the TFTP server uses in answering TFTP Read Requests. A client of the TFTP server can use this alternate name in its Read Requests.
<i>access-list-number</i>	(Optional) Basic IP access list number. Valid values are from 0 to 99.
<i>partition-number:</i>	(Optional) Specifies TFTP service of a file in the specified partition of Flash memory. If the partition number is not specified, the file in the first partition is used. For the Cisco 1600 series and Cisco 3600 series routers, you must enter a colon after the partition number if a filename follows it.

<i>device:</i>	<p>(Optional) Specifies TFTP service of a file on a Flash memory device in the Cisco 1600 series, Cisco 3600 series, and Cisco 7000 family routers. The colon is required. Valid devices are as follows:</p> <ul style="list-style-type: none">• flash—Internal Flash memory on the Cisco 1600 series and Cisco 3600 series routers. This is the only valid device for the Cisco 1600 series routers.• bootflash—Internal Flash memory in the Cisco 7000 family routers.• slot0—First PCMCIA slot on the Cisco 3600 series and Cisco 7000 family routers.• slot1—Second PCMCIA slot on the Cisco 3600 series and Cisco 7000 family.• slavebootflash—Internal Flash memory on the slave RSP card of a Cisco 7507 or Cisco 7513 router configured for HSA.• slaveslot0—First PCMCIA slot of the slave RSP card on a Cisco 7507 or Cisco 7513 router configured for HSA.• slaveslot1—Second PCMCIA slot of the slave RSP card on a Cisco 7507 or Cisco 7513 router configured for HSA.
<i>filename</i>	<p>Name of the file on a Flash memory device that the TFTP server uses in answering a TFTP Read Request. Use this argument only with the Cisco 1600 series, Cisco 3600 series, Cisco 7000 series, or Cisco 7500 series routers.</p>

tftp-server system

The **tftp-server system** command has been replaced by the **tftp-server** command. See the description of the **tftp-server** command in this chapter for more information.



Basic System Management Commands

This chapter describes the function and syntax of the commands used to perform basic system management tasks, such as naming the router and setting time services. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Configuration Fundamentals Command Reference*.

absolute

To specify an absolute time when a time range is in effect, use the **absolute** time-range configuration command. To remove the time limitation, use the **no** form of this command.

absolute [*start time date*] [*end time date*]

no absolute

Syntax Description

start time date	(Optional) Absolute time and date that the permit or deny statement of the associated access list starts going into effect. The <i>time</i> is expressed in 24-hour notation, in the form of <i>hours:minutes</i> . For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m. The <i>date</i> is expressed in the format <i>day month year</i> . The minimum start is 00:00 1 January 1993. If no start time and date are specified, the permit or deny statement is in effect immediately.
end time date	(Optional) Absolute time and date that the permit or deny statement of the associated access list is no longer in effect. Same <i>time</i> and <i>date</i> format as described for the start keyword. The end time and date must be after the start time and date. The maximum end time is 23:59 31 December 2035. If no end time and date are specified, the associated permit or deny statement is in effect indefinitely.

alias

To create a command alias, use the **alias** global configuration command. To delete all aliases in a command mode or to delete a specific alias, and to revert to the original command syntax, use the **no** form of this command.

alias mode command-alias original-command

no alias mode [command-alias]

Syntax Description	<i>mode</i>	Command mode of the original and alias commands.
	<i>command-alias</i>	Command alias.
	<i>original-command</i>	Original command syntax.

buffers

To make adjustments to initial buffer pool settings and to the limits at which temporary buffers are created and destroyed, use the **buffers** global configuration command. To return the buffers to their default size, use the **no** form of this command.

buffers { **small** | **middle** | **big** | **verybig** | **large** | **huge** | *type number* } { **permanent** | **max-free** | **min-free** | **initial** } *number-of-buffers*

no buffers { **small** | **middle** | **big** | **verybig** | **large** | **huge** | *type number* } { **permanent** | **max-free** | **min-free** | **initial** } *number-of-buffers*

Syntax Description	small	Buffer size of this public buffer pool is 104 bytes.
	middle	Buffer size of this public buffer pool is 600 bytes.
	big	Buffer size of this public buffer pool is 1524 bytes.
	verybig	Buffer size of this public buffer pool is 4520 bytes.
	large	Buffer size of this public buffer pool is 5024 bytes.
	huge	Default buffer size of this public buffer pool is 18024 bytes. This value can be configured with the buffers huge size command.
	<i>type number</i>	Interface type and interface number of the interface buffer pool. The <i>type</i> value cannot be fdi .
	permanent	Number of permanent buffers that the system tries to create and keep. Permanent buffers are normally not trimmed by the system.
	max-free	Maximum number of free or unallocated buffers in a buffer pool. A maximum of 20,480 small buffers can be constructed in the pool.
	min-free	Minimum number of free or unallocated buffers in a buffer pool.
	initial	Number of additional temporary buffers that are to be allocated when the system is reloaded. This keyword can be used to ensure that the system has necessary buffers immediately after reloading in a high-traffic environment.
	<i>number-of-buffers</i>	Number of buffers to be allocated.

buffers huge size

To dynamically resize all huge buffers to the value you specify, use the **buffers huge size** global configuration command. To restore the default buffer values, use the **no** form of this command.

buffers huge size *number-of-bytes*

no buffers huge size *number-of-bytes*

Syntax Description	<i>number-of-bytes</i>	Huge buffer size (in bytes).
---------------------------	------------------------	------------------------------

calendar set

To manually set the hardware clock (calendar), use one of the formats of the **calendar set** EXEC command.

calendar set *hh:mm:ss day month year*

calendar set *hh:mm:ss month day year*

Syntax Description

hh:mm:ss Current time in hours (using 24-hour notation), minutes, and seconds.

day Current day (by date) in the month.

month Current month (by name).

year Current year (no abbreviation).

clock calendar-valid

To configure a system as an authoritative time source for a network based on its hardware clock (calendar), use the **clock calendar-valid** global configuration command. To specify that the hardware clock is not an authoritative time source, use the **no** form of this command.

clock calendar-valid

no clock calendar-valid

Syntax Description

This command has no arguments or keywords.

clock read-calendar

To manually read the hardware clock (calendar) settings into the software clock, use the **clock read-calendar** EXEC command.

clock read-calendar

Syntax Description

This command has no arguments or keywords.

clock set

To manually set the system software clock, use one of the formats of the **clock set** EXEC command.

clock set *hh:mm:ss day month year*

clock set *hh:mm:ss month day year*

Syntax Description		
	<i>hh:mm:ss</i>	Current time in hours (military format), minutes, and seconds.
	<i>day</i>	Current day (by date) in the month.
	<i>month</i>	Current month (by name).
	<i>year</i>	Current year (no abbreviation).

clock summer-time

To configure the system to automatically switch to summer time (daylight saving time), use one of the formats of the **clock summer-time** global configuration command. To configure the Cisco IOS software not to automatically switch to summer time, use the **no** form of this command.

clock summer-time *zone recurring* [*week day month hh:mm week day month hh:mm [offset]*]

clock summer-time *zone date date month year hh:mm date month year hh:mm [offset]*

clock summer-time *zone date month date year hh:mm month date year hh:mm [offset]*

no clock summer-time

Syntax Description		
	<i>zone</i>	Name of the time zone (for example, "PDT" for Pacific Daylight Time) to be displayed when summer time is in effect.
	recurring	Indicates that summer time should start and end on the corresponding specified days every year.
	date	Indicates that summer time should start on the first specific date listed in the command and end on the second specific date in the command.
	<i>week</i>	(Optional) Week of the month (1 to 5 or last).
	<i>day</i>	(Optional) Day of the week (Sunday, Monday, and so on).
	<i>date</i>	Date of the month (1 to 31).
	<i>month</i>	(Optional) Month (January, February, and so on).
	<i>year</i>	Year (1993 to 2035).
	<i>hh:mm</i>	(Optional) Time (military format) in hours and minutes.
	<i>offset</i>	(Optional) Number of minutes to add during summer time (default is 60).

clock timezone

To set the time zone for display purposes, use the **clock timezone** global configuration command. To set the time to Coordinated Universal Time (UTC), use the **no** form of this command.

clock timezone *zone hours-offset [minutes-offset]*

no clock timezone

Syntax Description		
	<i>zone</i>	Name of the time zone to be displayed when standard time is in effect.
	<i>hours-offset</i>	Hours difference from UTC.
	<i>minutes-offset</i>	(Optional) Minutes difference from UTC.

clock update-calendar

To perform a one-time update of the hardware clock (calendar) from the software clock, use the **clock update-calendar** in user or privileged EXEC mode.

clock update-calendar

Syntax Description This command has no arguments or keywords.

downward-compatible-config

To generate a configuration that is compatible with an earlier Cisco IOS release, use the **downward-compatible-config** global configuration command. To remove this feature, use the **no** form of this command.

downward-compatible-config *version*

no downward-compatible-config

Syntax Description *version* Cisco IOS release number, not earlier than Release 10.2.

hostname

To specify or modify the host name for the network server, use the **hostname** global configuration command.

hostname *name*

Syntax Description *name* New host name for the network server.

ip bootp server

To access the BOOTP service available from hosts on the network, use the **ip bootp server** global configuration command. To disable these services, use the **no** form of the command.

ip bootp server

no ip bootp server

Syntax Description This command has no arguments or keywords.

ip finger

To configure a system to accept Finger protocol requests (defined in RFC 742), use the **ip finger** global configuration command. To disable this service, use the **no** form of this command.

ip finger [*rfc-compliant*]

no ip finger

Syntax Description	<i>rfc-compliant</i>	(Optional) Configures the system to wait for “Return” or “/W” input when processing Finger requests. This keyword should not be used for those systems.
--------------------	----------------------	---

ip telnet source-interface

To allow a user to select an address of an interface as the source address for Telnet connections, use the **ip telnet source-interface** global configuration command. To reset the source address to the default for each connection, use the **no** form of this command.

ip telnet source-interface *interface*

no ip telnet source-interface

Syntax Description	<i>interface</i>	The interface whose address is to be used as the source for Telnet connections.
--------------------	------------------	---

ip tftp source-interface

To allow a user to select the interface whose address will be used as the source address for TFTP connections, use the **ip tftp source-interface** global configuration command.

ip tftp source-interface *interface*

no ip tftp source-interface

Syntax Description	<i>interface</i>	The interface whose address is to be used as the source for TFTP connections.
--------------------	------------------	---

load-interval

To change the length of time for which data is used to compute load statistics, use the **load-interval** interface configuration command. To revert to the default setting, use the **no** form of this command.

load-interval *seconds*

no load-interval *seconds*

Syntax Description	<i>seconds</i>	Length of time for which data is used to compute load statistics. A value that is a multiple of 30, from 30 to 600 (30, 60, 90, 120, and so on).
---------------------------	----------------	--

ntp access-group

To control access to the Network Time Protocol (NTP) services on the system, use the **ntp access-group** global configuration command. To remove access control to the NTP services, use the **no** form of this command.

ntp access-group { **query-only** | **serve-only** | **serve** | **peer** } *access-list-number*

no ntp access-group { **query-only** | **serve-only** | **serve** | **peer** }

Syntax Description	query-only	Allows only NTP control queries. See RFC 1305 (NTP version 3).
	serve-only	Allows only time requests.
	serve	Allows time requests and NTP control queries, but does not allow the system to synchronize to the remote system.
	peer	Allows time requests and NTP control queries and allows the system to synchronize to the remote system.
	<i>access-list-number</i>	Number (from 1 to 99) of a standard IP access list.

ntp authenticate

To enable Network Time Protocol (NTP) authentication, use the **ntp authenticate** global configuration command. To disable the feature, use the **no** form of this command.

ntp authenticate

no ntp authenticate

Syntax Description	This command has no arguments or keywords.
---------------------------	--

ntp authentication-key

To define an authentication key for Network Time Protocol (NTP), use the **ntp authentication-key** global configuration command. To remove the authentication key for NTP, use the **no** form of this command.

ntp authentication-key *number* **md5** *value*

no ntp authentication-key *number*

Syntax Description	<i>number</i>	Key number (from 1 to 4294967295).
	md5	Authentication key. Message authentication support is provided using the message digest algorithm 5 (MD5) algorithm. The key type md5 is currently the only key type supported.
	<i>value</i>	Key value (an arbitrary string of up to eight characters).

ntp broadcast

To configure the system to send Network Time Protocol (NTP) broadcast packets on a specified interface, use the **ntp broadcast** interface configuration command. To disable this capability, use the **no** form of this command.

ntp broadcast [*version number*]

no ntp broadcast

Syntax Description	<i>version number</i>	(Optional) Number from 1 to 3 indicating the NTP version.
--------------------	-----------------------	---

ntp broadcast client

To configure the system to receive Network Time Protocol (NTP) broadcast packets on a specified interface, use the **ntp broadcast client** interface configuration command. To disable this capability, use the **no** form of this command.

ntp broadcast client

no ntp broadcast client

Syntax Description	This command has no arguments or keywords.
--------------------	--

ntp broadcastdelay

To set the estimated round-trip delay between the Cisco IOS software and a Network Time Protocol (NTP) broadcast server, use the **ntp broadcastdelay** global configuration command. To revert to the default value, use the **no** form of this command.

ntp broadcastdelay *microseconds*

no ntp broadcastdelay

Syntax Description	<i>microseconds</i>	Estimated round-trip time (in microseconds) for NTP broadcasts. The range is from 1 to 999999.
---------------------------	---------------------	--

ntp clock-period



Caution

Do not enter this command; it is documented for informational purposes only. The system automatically generates this command as Network Time Protocol (NTP) determines the clock error and compensates.

As NTP compensates for the error in the software clock, it keeps track of the correction factor for this error. The system automatically saves this value into the system configuration using the **ntp clock-period** global configuration command. To revert to the default, use the **no** form of this command.

ntp clock-period *value*

no ntp clock-period

Syntax Description	<i>value</i>	Amount to add to the software clock for each clock hardware tick (this value is multiplied by 2^{-32}).
---------------------------	--------------	--

ntp disable

To prevent an interface from receiving Network Time Protocol (NTP) packets, use the **ntp disable** interface configuration command. To enable receipt of NTP packets on an interface, use the **no** form of this command.

ntp disable

no ntp disable

Syntax Description	This command has no arguments or keywords.
---------------------------	--

ntp master

To configure the Cisco IOS software as a Network Time Protocol (NTP) master clock to which peers synchronize themselves when an external NTP source is not available, use the **ntp master** global configuration command. To disable the master clock function, use the **no** form of this command.

ntp master [*stratum*]

no ntp master [*stratum*]



Caution

Use this command with caution. It is very easy to override valid time sources using this command, especially if a low stratum number is configured. Configuring multiple machines in the same network with the **ntp master** command can cause instability in keeping time if the machines do not agree on the time.

Syntax Description

<i>stratum</i>	(Optional) Number from 1 to 15. Indicates the NTP stratum number that the system will claim.
----------------	--

ntp peer

To configure the software clock to synchronize a peer or to be synchronized by a peer, use the **ntp peer** global configuration command. To disable this capability, use the **no** form of this command.

ntp peer *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**]

no ntp peer *ip-address*

Syntax Description

<i>ip-address</i>	IP address of the peer providing, or being provided, the clock synchronization.
version	(Optional) Defines the Network Time Protocol (NTP) version number.
<i>number</i>	(Optional) NTP version number (1 to 3).
key	(Optional) Defines the authentication key.
<i>keyid</i>	(Optional) Authentication key to use when sending packets to this peer.
source	(Optional) Names the interface.
<i>interface</i>	(Optional) Name of the interface from which to pick the IP source address.
prefer	(Optional) Makes this peer the preferred peer that provides synchronization.

ntp refclock

To configure an external clock source for use with Network Time Protocol (NTP) services, use the **ntp refclock** command in line configuration mode. To disable support of the external time source, use the **no** form of this command.

```
ntp refclock { trimble | telecom-solutions } pps { cts | ri | none } [inverted] [pps-offset number]
[stratum number] [timestamp-offset number]
```

```
no ntp refclock
```

Syntax Description

trimble	Enables the reference clock driver for the Trimble Palisade NTP Synchronization Kit (Cisco 7200 series routers only).
telecom-solutions	Enables the reference clock driver for a Telecom Solutions GPS device.
pps	Pulse per second (PPS) signal line. Indicate PPS pulse reference clock support. Choices are cts , ri , or none .
cts	Pulse per second on CTS.
ri	Pulse per second on RI.
none	No PPS signal available.
inverted	(Optional) PPS signal is inverted.
pps-offset <i>number</i>	(Optional) Offset of PPS pulse. The number is the offset (in milliseconds).
stratum <i>number</i>	(Optional) Number from 0 to 14. Indicates the NTP stratum number that the system will claim.
timestamp-offset <i>number</i>	(Optional) Offset of time stamp. The number is the offset (in milliseconds).

ntp server

To allow the software clock to be synchronized by a Network Time Protocol (NTP) time server, use the **ntp server** global configuration command. To disable this capability, use the **no** form of this command.

```
ntp server ip-address [version number] [key keyid] [source interface] [prefer]
```

```
no ntp server ip-address
```

Syntax Description

<i>ip-address</i>	IP address of the time server providing the clock synchronization.
version	(Optional) Defines the NTP version number.
<i>number</i>	(Optional) NTP version number (1 to 3).
key	(Optional) Defines the authentication key.
<i>keyid</i>	(Optional) Authentication key to use when sending packets to this peer.
source	(Optional) Identifies the interface from which to pick the IP source address.
<i>interface</i>	(Optional) Name of the interface from which to pick the IP source address.
prefer	(Optional) Specifies that the server referenced in this command is preferred over other configured NTP servers.

ntp source

To use a particular source address in Network Time Protocol (NTP) packets, use the **ntp source** global configuration command. To remove the specified source address, use the **no** form of this command.

ntp source *type number*

no ntp source

Syntax Description		
	<i>type</i>	Type of interface.
	<i>number</i>	Number of the interface.

ntp trusted-key

To authenticate the identity of a system to which Network Time Protocol (NTP) will synchronize, use the **ntp trusted-key** global configuration command. To disable authentication of the identity of the system, use the **no** form of this command.

ntp trusted-key *key-number*

no ntp trusted-key *key-number*

Syntax Description		
	<i>key-number</i>	Key number of authentication key to be trusted.

ntp update-calendar

To periodically update the hardware clock (calendar) from a Network Time Protocol (NTP) time source, use the **ntp update-calendar** global configuration command. To disable the periodic updates, use the **no** form of this command.

ntp update-calendar

no ntp update-calendar

Syntax Description	
	This command has no arguments or keywords.

periodic

To specify a recurring (weekly) time range for functions that support the time-range feature, use the **periodic** time-range configuration command. To remove the time limitation, use the **no** form of this command.

periodic *days-of-the-week hh:mm to [days-of-the-week] hh:mm*

no periodic *days-of-the-week hh:mm to [days-of-the-week] hh:mm*

Syntax Description

days-of-the-week The first occurrence of this argument is the starting day or day of the week that the associated time range is in effect. The second occurrence is the ending day or day of the week the associated statement is in effect.

This argument can be any single day or combinations of days: **Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday**. Other possible values are:

- **daily**—Monday through Sunday
- **weekdays**—Monday through Friday
- **weekend**—Saturday and Sunday

If the ending days of the week are the same as the starting days of the week, they can be omitted.

hh:mm The first occurrence of this argument is the starting hours:minutes that the associated time range is in effect. The second occurrence is the ending hours:minutes the associated statement is in effect.

The hours:minutes are expressed in a 24-hour clock. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.

to Entry of the **to** keyword is required to complete the range “from start-time to end-time.”

prompt

To customize the CLI prompt, use the **prompt** global configuration command. To revert to the default prompt, use the **no** form of this command.

prompt *string*

no prompt [*string*]

Syntax Description

string Text that will be displayed on screen as the CLI prompt, including any desired prompt variables.

scheduler allocate

To guarantee CPU time for processes, use the **scheduler allocate** global configuration command on the Cisco 7200 series and Cisco 7500 series routers. To restore the default, use the **no** form of this command.

scheduler allocate *interrupt-time process-time*

no scheduler allocate

Syntax Description

interrupt-time Integer (in microseconds) that limits the maximum number of microseconds to spend on fast switching within any one network interrupt context. The range is from 400 to 60000 microseconds. The default is 4000 microseconds.

process-time Integer (in microseconds) that guarantees the minimum number of microseconds to spend at the process level when network interrupts are disabled. The range is from 100 to 4000 microseconds. The default is 200 microseconds.

scheduler interval

To control the maximum amount of time that can elapse without running system processes, use the **scheduler interval** global configuration command. To restore the default, use the **no** form of this command.

scheduler interval *milliseconds*

no scheduler interval

Syntax Description

milliseconds Integer that specifies the interval (in milliseconds). The minimum interval that you can specify is 500 milliseconds; there is no maximum value.

service decimal-tty

To specify that line numbers be displayed and interpreted as decimal numbers rather than octal numbers, use the **service decimal-tty** global configuration command. To restore the default, use the **no** form of this command.

service decimal-tty

no service decimal-tty

Syntax Description

This command has no arguments or keywords.

service exec-wait

To delay the startup of the EXEC on noisy lines, use the **service exec-wait** global configuration command. To disable the delay function, use the **no** form of this command.

```
service exec-wait
```

```
no service exec-wait
```

Syntax Description This command has no arguments or keywords.

service finger

The **service finger** command has been replaced by the **ip finger** command. However, the **service finger** and **no service finger** commands continue to function to maintain backward compatibility with older versions of Cisco IOS software. Support for this command may be removed in a future release. See the description of the **ip finger** command in this chapter for more information.

service hide-telnet-address

To hide addresses while trying to establish a Telnet session, use the **service hide-telnet-address** global configuration command. To remove this service, use the **no** form of this command.

```
service hide-telnet-address
```

```
no service hide-telnet-address
```

Syntax Description This command has no arguments or keywords.

service nagle

To enable the Nagle congestion control algorithm, use the **service nagle** global configuration command. To to disable the algorithm, use the **no** form of this command.

```
service nagle
```

```
no service nagle
```

Syntax Description This command has no arguments or keywords.

service prompt config

To display the configuration prompt (config), use the **service prompt config** global configuration command. To remove the configuration prompt, use the **no** form of this command.

service prompt config

no service prompt config

Syntax Description This command has no arguments or keywords.

service tcp-small-servers

To access minor TCP/IP services available from hosts on the network, use the **service tcp-small-servers** global configuration command. To disable these services, use the **no** form of the command.

service tcp-small-servers

no service tcp-small-servers

Syntax Description This command has no arguments or keywords.

service telnet-zero-idle

To set the TCP window to zero (0) when the Telnet connection is idle, use the **service telnet-zero-idle** global configuration command. To disable this service, use the **no** form of this command.

service telnet-zero-idle

no service telnet-zero-idle

Syntax Description This command has no arguments or keywords.

service udp-small-servers

To access minor User Datagram Protocol (UDP) services available from hosts on the network, use the **service udp-small-servers** global configuration command. To disable these services, use the **no** form of this command.

```
service udp-small-servers
```

```
no service udp-small-servers
```

Syntax Description This command has no arguments or keywords.

show aliases

To display all alias commands, or the alias commands in a specified mode, use the **show aliases** EXEC command.

```
show aliases [mode]
```

Syntax Description

<i>mode</i>	(Optional) Command mode.
-------------	--------------------------

show buffers

To display statistics for the buffer pools on the network server, use the **show buffers** EXEC command.

```
show buffers [address hex-addr | [all | assigned | failures | free | old [dump | header | packet]]
| input-interface interface-type identifier | pool pool-name]
```

Syntax Description	
address	(Optional) Displays buffers at a specified address.
<i>hex-addr</i>	Address (in hexadecimal notation) of the buffer to display.
all	(Optional) Displays all buffers.
assigned	(Optional) Displays the buffers in use.
failures	(Optional) Displays buffer allocation failures.
free	(Optional) Displays the buffers available for use.
old	(Optional) Displays buffers older than one minute.
dump	(Optional) Displays the buffer header and all data in the display.
header	(Optional) Displays the buffer header only in the display.
packet	(Optional) Displays the buffer header and packet data in the display.
input-interface	(Optional) Displays interface pool information. If the specified <i>interface-type</i> argument has its own buffer pool, displays information for that pool.
<i>interface-type</i>	Value of <i>interface-type</i> can be ethernet , fastethernet , loopback , serial , or null .
<i>identifier</i>	Identifier of the interface specified in <i>interface-type</i> argument.

pool	(Optional) Displays buffers in a specified buffer pool.
<i>pool-name</i>	Specifies the name of a buffer pool to use.

show calendar

To display the current time and date setting for the hardware clock, use the **show calendar** EXEC command:

```
show calendar
```

Syntax Description This command has no arguments or keywords.

show clock

To display the time and date from the system software clock, use the **show clock** EXEC command.

```
show clock [detail]
```

Syntax Description

detail	(Optional) Indicates the clock source (NTP, VINES, hardware clock, and so on) and the current summer-time setting (if any).
---------------	---

show ntp associations

To show the status of Network Time Protocol (NTP) associations, use the **show ntp associations** EXEC command.

```
show ntp associations [detail]
```

Syntax Description

detail	(Optional) Displays detailed information about each NTP association.
---------------	--

show ntp status

To show the status of the Network Time Protocol (NTP), use the **show ntp status** EXEC command.

```
show ntp status
```

Syntax Description This command has no arguments or keywords.

show registry

To show the function registry information, use the **show registry** EXEC command.

```
show registry [registry-name [registry-num]] [brief | statistics]
```

Syntax Description	
<i>registry-name</i>	(Optional) Name of the registry to examine.
<i>registry-num</i>	(Optional) Number of the registry to examine.
brief	(Optional) Displays limited functions and services information.
statistics	(Optional) Displays function registry statistics.

show sntp

To show information about the Simple Network Time Protocol (SNTP), use the **show sntp** EXEC command on a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router.

```
show sntp
```

Syntax Description This command has no arguments or keywords.

sntp broadcast client

To use the Simple Network Time Protocol (SNTP) to accept Network Time Protocol (NTP) traffic from any broadcast server, use the **sntp broadcast client** global configuration command to configure a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 router. To prevent the router from accepting broadcast traffic, use the **no** form of this command.

```
sntp broadcast client
```

```
no sntp broadcast client
```

Syntax Description This command has no arguments or keywords.

sntp server

To configure a Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, Cisco 1750, or Cisco 800 router to use the Simple Network Time Protocol (SNTP) to request and accept Network Time Protocol (NTP) traffic from a stratum 1 time server, use the **sntp server** global configuration command. To remove a server from the list of NTP servers, use the **no** form of this command.

```
sntp server {address | hostname} [version number]
```

```
no sntp server {address | hostname}
```

Syntax Description

<i>address</i>	IP address of the time server.
<i>hostname</i>	Host name of the time server.
version number	(Optional) Version of NTP to use. The default is 1.

time-range

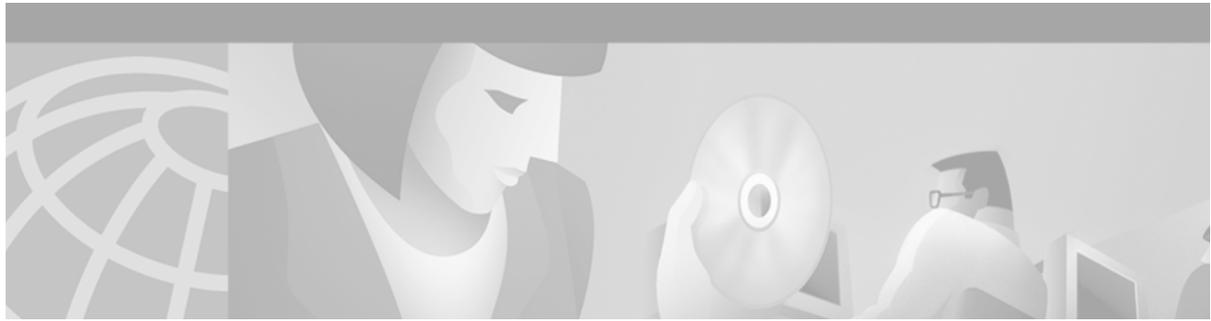
To enable time-range configuration mode and define time ranges for functions (such as extended access lists), use the **time-range** global configuration command. To remove the time limitation, use the **no** form of this command.

time-range *time-range-name*

no time-range *time-range-name*

Syntax Description

<i>time-range-name</i>	Desired name for the time range. The name cannot contain a space or quotation mark, and must begin with a letter.
------------------------	---



Troubleshooting and Fault Management Commands

This chapter describes the function and syntax of the commands used to troubleshoot a router. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Configuration Fundamentals Command Reference*.

attach

To connect to a specific line card for the purpose of executing monitoring and maintenance commands on that line card only, use the **attach** privileged EXEC command. To exit from the Cisco IOS software image on the line card and return to the Cisco IOS image on the GRP card, use the **exit** command.

attach *slot-number*

Syntax Description

<i>slot-number</i>	Slot number of the line card you want to connect to. Slot numbers range from 0 to 11 for the Cisco 12012 router and 0 to 7 for the Cisco 12008 router. If the slot number is omitted, you are prompted for the slot number.
--------------------	---

clear logging

To clear messages from the logging buffer, use the **clear logging** privileged EXEC command.

clear logging

Syntax Description

This command has no arguments or keywords.

diag

To perform field diagnostics on a line card, on the Gigabit Route Processor (GRP), on the Switch Fabric Cards (SFCs), and on the Clock Scheduler Card (CSC) in Cisco 12000 series Gigabit Switch Routers (GSRs), use the **diag** privileged EXEC command. To disable field diagnostics on a line card, use the **no** form of this command.

diag *slot-number* [**halt** | **previous** | **post** | **verbose** [**wait**] | **wait**]

no diag *slot-number*

Syntax Description

<i>slot-number</i>	Slot number of the line card you want to test. Slot numbers range from 0 to 11 for the Cisco 12012 and 0 to 7 for the Cisco 12008 router. Slot numbers for the CSC are 16 and 17, and for the FSC are 18, 19, and 20.
halt	(Optional) Stops the field diagnostic testing on the line card.
previous	(Optional) Displays previous test results (if any) for the line card.
post	(Optional) Initiates an EPROM-based extended power-on self-test (EPOST) only. The EPOST test suite is not as comprehensive as the field diagnostics, and a pass/fail message is the only message displayed on the console.
verbose [wait]	(Optional) Enables the maximum status messages to be displayed on the console. By default, only the minimum status messages are displayed on the console. If you specify the optional wait keyword, the Cisco IOS software is not automatically reloaded on the line card after the test completes.
wait	(Optional) Stops the automatic reloading of the Cisco IOS software on the line card after the completion of the field diagnostic testing. If you use this keyword, you must use the microcode reload <i>slot</i> global configuration command, or manually remove and insert the line card (to power it up) in the slot so that the GRP will recognize the line card and download the Cisco IOS software image to the line card.

exception core-file

To specify the name of the core dump file, use the **exception core-file** global configuration command. To return to the default core filename, use the **no** form of this command.

exception core-file *file-name*

no exception core-file

Syntax Description

<i>file-name</i>	Name of the core dump file saved on the server.
------------------	---

exception dump

To configure the router to dump a core file to a particular server when the router crashes, use the **exception dump** global configuration command. To disable core dumps, use the **no** form of this command.

exception dump *ip-address*

no exception dump

Syntax Description

ip-address IP address of the server that stores the core dump file.

exception linecard

To enable storing of crash information for a line card and optionally specify the type and amount of information stored, use the **exception linecard** global configuration command. To disable the storing of crash information for the line card, use the **no** form of this command.

exception linecard {**all** | **slot** *slot-number*} [**corefile** *filename* | **main-memory** *size* [**k** | **m**] | **queue-ram** *size* [**k** | **m**] | **rx-buffer** *size* [**k** | **m**] | **sqe-register-rx** | **sqe-register-tx** | **tx-buffer** *size* [**k** | **m**]]

no exception linecard

Syntax Description

all	Stores crash information for all line cards.
slot <i>slot-number</i>	Stores crash information for the line card in the specified slot. Slot numbers range from 0 to 11 for the Cisco 12012 and 0 to 7 for the Cisco 12008 router.
corefile <i>filename</i>	(Optional) Stores the crash information in the specified file in NVRAM. The default filename is <i>hostname-core-slot-number</i> (for example, c12012-core-8).
main-memory <i>size</i>	(Optional) Stores the crash information for the main memory on the line card and specifies the size of the crash information. Size of the memory to store is 0 to 268435456.
queue-ram <i>size</i>	(Optional) Stores the crash information for the queue RAM memory on the line card and specifies the size of the crash information. Size of the memory to store can be from 0 to 1048576.
rx-buffer <i>size</i> tx-buffer <i>size</i>	(Optional) Stores the crash information for the receive and transmit buffer on the line card and specifies the size of the crash information. Size of the memory to store can be from 0 to 67108864.
sqe-register-rx sqe-register-tx	(Optional) Stores crash information for the receive or transmit silicon queueing engine registers on the line card.
k m	(Optional) The k option multiplies the specified <i>size</i> by 1K (1024), and the m option multiplies the specified <i>size</i> by 1M (1024*1024).

exception memory

To cause the router to create a core dump and reboot when certain memory size parameters are violated, use the **exception memory** global configuration command. To disable the rebooting and core dump, use the **no** form of this command.

```
exception memory {fragment size | minimum size}
```

```
no exception memory {fragment | minimum}
```

Syntax Description	fragment <i>size</i>	The minimum contiguous block of memory in the free pool, in bytes.
	minimum <i>size</i>	The minimum size of the free memory pool, in bytes.

exception protocol

To configure the protocol used for core dumps, use the **exception protocol** global configuration command. To configure the router to use the default protocol, use the **no** form of this command.

```
exception protocol {ftp | rcp | tftp}
```

```
no exception protocol
```

Syntax Description	ftp	Uses File Transfer Protocol (FTP) for core dumps.
	rcp	Uses remote copy protocol (rcp) for core dumps.
	tftp	Uses TFTP for core dumps. This is the default.

exception region-size

To specify the size of the region for the exception-time memory pool, use the **exception region-size** global configuration command. To use the default region size, use the **no** form of this command.

```
exception region-size size
```

```
no exception region-size
```

Syntax Description	<i>size</i>	The size of the region for the exception-time memory pool.
--------------------	-------------	--

exception spurious-interrupt

To configure the router to create a core dump and reload after a specified number of spurious interrupts, use the **exception spurious-interrupt** command global configuration command. To disable the core dump and reload, use the **no** form of this command.

exception spurious-interrupt *[number]*

no exception spurious-interrupt

Syntax Description	<i>number</i>	(Optional) A number from 1 to 4294967295 that indicates the maximum number of spurious interrupts to include in the core dump before reloading.
---------------------------	---------------	---

execute-on

To execute commands on a line card, use the **execute-on** privileged EXEC command.

execute-on {*slot slot-number* | **all** | **master**} *command*

Syntax Description	<i>slot slot-number</i>	Executes the command on the line card in the specified slot. Slot numbers can be chosen from the following ranges: <ul style="list-style-type: none"> • Cisco 12012 router: 0 to 11 • Cisco 12008 access server: 0 to 7 • Cisco AS5800 access server: 0 to 13
	all	Executes the command on all line cards.
	master	(AS5800 only) Executes the designated command on a Dial Shelf Controller (DSC). Do not use this option; it is used for technical support troubleshooting only.
	<i>command</i>	Cisco IOS command to remotely execute on the line card.

logging

To log messages to a syslog server host, use the **logging** global configuration command. To delete the syslog server with the specified address from the list of syslogs, use the **no** form of this command.

logging *host-name*

no logging *host-name*

Syntax Description	<i>host-name</i>	Name or IP address of the host to be used as a syslog server.
---------------------------	------------------	---

logging buffered

To limit messages logged to an internal buffer based on severity, use the **logging buffered** global configuration command. To cancel the use of the buffer, use the **no** form of this command. The **default** form of this command returns the buffer size to the default size.

logging buffered [*buffer-size* | *level*]

no logging buffered

default logging buffered

Syntax Description

<i>buffer-size</i>	(Optional) Size of the buffer from 4096 to 4,294,967,295 bytes. The default size varies by platform.
<i>level</i>	(Optional) Limits the logging of messages to the buffer to a specified level. You can enter the level name or level number. See Table 14 for a list of the acceptable level name or level number keywords.

The **show logging EXEC** command displays the addresses and levels associated with the current logging setup, and any other logging statistics. See Table 14.

Table 14 Error Message Logging Priorities and Corresponding Level Names/Numbers

Level Arguments	Level	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

logging console

To limit messages logged to the console based on severity, use the **logging console** global configuration command. To disable logging to the console terminal, use the **no** form of this command.

logging console *level*

no logging console

Syntax Description

<i>level</i>	Limits the logging of messages displayed on the console terminal to a specified level. You can enter the level number or level name. See Table 14 for a list of the level arguments.
--------------	--

logging facility

To configure the syslog facility in which error messages are sent, use the **logging facility** global configuration command. To revert to the default of **local7**, use the **no** form of this command.

logging facility *facility-type*

no logging facility

Syntax Description

facility-type Syslog facility. See Table 15 for descriptions of acceptable keywords.

Table 15 describes the acceptable keywords for the *facility-type* argument.

Table 15 logging facility facility-type Argument

facility-type Keyword	Description
auth	Authorization system
cron	Cron facility
daemon	System daemon
kern	Kernel
local0–7	Reserved for locally defined messages
lpr	Line printer system
mail	Mail system
news	USENET news
sys9	System use
sys10	System use
sys11	System use
sys12	System use
sys13	System use
sys14	System use
syslog	System log
user	User process
uucp	UNIX-to-UNIX copy system

logging history

To limit syslog messages sent to the router's history table and the Simple Network Management Protocol (SNMP) network management station based on severity, use the **logging history** global configuration command. To return the logging of syslog messages to the default level, use the **no** form of this command.

logging history *severity-level*

no logging history

Syntax Description

<i>severity-level</i>	Limits the messages saved in the history table and sent to the SNMP network management station to the specified set of levels. You can enter the level number or level name. See Table 16 for a list of acceptable severity-level keywords.
-----------------------	---

Table 16 shows the *severity-level* arguments.

Table 16 Error Message Logging Priorities for History Table and SNMP Server

Severity Level Name	Severity Level Number	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

logging history size

To change the number of syslog messages stored in the router's history table, use the **logging history size** global configuration command. To return the number of messages to the default value, use the **no** form of this command.

logging history size *number*

no logging history size

Syntax Description

<i>number</i>	Number from 1 to 500 that indicates the maximum number of messages stored in the history table.
---------------	---

logging linecard

To log messages to an internal buffer on a line card, use the **logging linecard** global configuration command. To cancel the use of the internal buffer on the line cards, use the **no** form of this command.

logging linecard [*size* | *level*]

no logging linecard

Syntax Description	<i>size</i>	(Optional) Size of the buffer used for each line card. The range is from 4096 to 65,536 bytes. The default is 8 KB.
	<i>level</i>	(Optional) Limits the logging of messages displayed on the console terminal to a specified level. The message level can be one of the following: <ul style="list-style-type: none"> • alerts—Immediate action needed • critical—Critical conditions • debugging—Debugging messages • emergencies—System is unusable • errors—Error conditions • informational—Informational messages • notifications—Normal but significant conditions • warnings—Warning conditions

logging monitor

To limit messages logged to the terminal lines (monitors) based on severity, use the **logging monitor** global configuration command. This command limits the logging messages displayed on terminal lines other than the console line to messages with a level at or above the *level* argument. To disable logging to terminal lines other than the console line, use the **no** form of this command.

logging monitor *severity-level*

no logging monitor

Syntax Description	<i>severity-level</i>	Limits the logging of messages logged to the terminal lines (monitors) to a specified level. You can enter the level number or level name. See Table 17 for a list of acceptable severity-level keywords.
--------------------	-----------------------	---

Table 17 logging monitor Error Message Logging Priorities

Level Name	Level Number	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT

Table 17 logging monitor Error Message Logging Priorities (continued)

Level Name	Level Number	Description	Syslog Definition
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant conditions	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

logging on

To control logging of error messages, use the **logging on** global configuration command. This command sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages. To disable the logging process, use the **no** form of this command.

logging on

no logging on

Syntax Description This command has no arguments or keywords.

logging rate-limit

To limit the rate of messages logged per second, use the **logging rate-limit** configuration command. To disable the limit, use the **no** form of this command.

logging rate-limit { *number* | **all** | **console** } [**except** *severity*]

no logging rate-limit

Syntax Description	
<i>number</i>	Specifies rate of messages logged per second. The valid values are from 1 to 10000.
all	Sets the rate limit to all messages including the debug messages.
console	Sets the rate limit only to console messages.
except	(Optional) Excludes messages of this severity or higher.
<i>severity</i>	(Optional) Sets the logging severity level. The valid levels are from 0 to 7.

logging source-interface

To specify the source IP address of syslog packets, use the **logging source-interface** global configuration command. To remove the source designation, use the **no** form of this command.

logging source-interface *interface-type interface-number*

no logging source-interface

Syntax Description

<i>interface-type</i>	Interface type.
<i>interface-number</i>	Interface number.

logging synchronous

To synchronize unsolicited messages and debug output with solicited Cisco IOS software output and prompts for a specific console port line, auxiliary port line, or vty, use the **logging synchronous** line configuration command. To disable synchronization of unsolicited messages and debug output, use the **no** form of this command.

logging synchronous [**level** *severity-level* | **all**] [**limit** *number-of-buffers*]

no logging synchronous [**level** *severity-level* | **all**] [**limit** *number-of-buffers*]

Syntax Description

level <i>severity-level</i>	(Optional) Specifies the message severity level. Messages with a severity level equal to or higher than this value are printed asynchronously. Low numbers indicate greater severity and high numbers indicate lesser severity. The default value is 2.
all	(Optional) Specifies that all messages are printed asynchronously, regardless of the severity level.
limit <i>number-of-buffers</i>	(Optional) Specifies the number of buffers to be queued for the terminal after which new messages are dropped. The default value is 20.

logging trap

To limit messages logged to the syslog servers based on severity, use the **logging trap** global configuration command. The command limits the logging of error messages sent to syslog servers to only those messages at the specified level. To disable logging to syslog servers, use the **no** form of this command.

logging trap *level*

no logging trap

Syntax Description

<i>level</i>	Limits the logging of messages to the syslog servers to a specified level. You can enter the level number or level name. See Table 18 for a list of acceptable <i>level</i> keywords.
--------------	---

Table 18 logging trap Error Message Logging Priorities

Level Arguments	Level	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

ping (privileged)

To diagnose basic network connectivity on Apollo, AppleTalk, Connectionless Network Service (CLNS), DECnet, IP, Novell IPX, VINES, or XNS networks, use the **ping** privileged EXEC command.

ping [*protocol* | **tag**] {*host-name* | *system-address*}

Syntax Description

<i>protocol</i>	(Optional) Protocol keyword, one of apollo , appletalk , clns , decnet , ip , ipx , srb , vines , or xns .
tag	(Optional) Specifies a tag encapsulated IP ping.
<i>host-name</i>	Host name of the system to ping.
<i>system-address</i>	Address of the system to ping.

ping (user)

To diagnose basic network connectivity on AppleTalk, Connection Network Service (CLNS), IP, Novell, Apollo, VINES, DECnet, or XNS networks, use the **ping** (packet internet groper) user EXEC command.

```
ping [protocol] {host-name | system-address}
```

Syntax Description	<i>protocol</i>	(Optional) Protocol keyword, one of apollo , appletalk , clns , decnet , ip , ipx , vines , or xns .
	<i>host-name</i>	Host name of the system to ping.
	<i>system-address</i>	Address of the system to ping.

service slave-log

To allow slave Versatile Interface Processor (VIP) cards to log important error messages to the console, use the **service slave-log** global configuration command. To disable slave logging, use the **no** form of this command.

```
service slave-log
```

```
no service slave-log
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--

service tcp-keepalives-in

To generate keepalive packets on idle incoming network connections (initiated by the remote host), use the **service tcp-keepalives-in** global configuration command. To disable the keepalives, use the **no** form of this command.

```
service tcp-keepalives-in
```

```
no service tcp-keepalives-in
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--

service tcp-keepalives-out

To generate keepalive packets on idle outgoing network connections (initiated by a user), use the **service tcp-keepalives-out** global configuration command. To disable the keepalives, use the **no** form of this command.

service tcp-keepalives-out

no service tcp-keepalives-out

Syntax Description This command has no arguments or keywords.

service timestamps

To configure the system to time-stamp debugging or logging messages, use one of the **service timestamps** global configuration commands. To disable this service, use the **no** form of this command.

service timestamps *message-type* [**uptime**]

service timestamps *message-type* **datetime** [**msec**] [**localtime**] [**show-timezone**]

no service timestamps *type*

Syntax Description	<i>message-type</i>	Type of message to time stamp: debug or log .
	uptime	(Optional) Time stamp with the time since the system was rebooted.
	datetime	Time stamp with the date and time.
	msec	(Optional) Include milliseconds in the date and time stamp.
	localtime	(Optional) Time stamp relative to the local time zone.
	show-timezone	(Optional) Include the time zone name in the time stamp.

show c2600 (2600)

To display information for troubleshooting the Cisco 2600 series router, use the **show c2600** EXEC command.

show c2600

Syntax Description This command has no arguments or keywords.

show c7200 (7200)

To display information about the CPU and midplane for Cisco 7200 series routers, use the **show c7200** EXEC command.

show c7200

Syntax Description This command has no arguments or keywords.

show cls

To display the current status of all Cisco link services (CLS) sessions on the router, use the **show cls** EXEC command.

show cls [brief]

Syntax Description

brief	(Optional) Displays a brief version of the output.
--------------	--

show context (2600)

To display information stored in NVRAM when an exception occurs, use the **show context** EXEC command.

show context

Syntax Description This command has no arguments or keywords.

show context

To display information stored in NVRAM when the router crashes, use the **show context** EXEC command.

show context summary

show context {all | slot *slot-number* [*crash-index*] [all] [debug]}

Syntax Description

summary	Displays a summary of all the crashes recorded.
all	Displays all crashes for all the slots. When optionally used with the slot keyword, displays crash information for the specified slot.

slot <i>slot-number</i> <i>[crash-index]</i>	Displays information for a particular line card. Slot numbers range from 0 to 11 for the Cisco 12012 router and from 0 to 7 for the Cisco 12008. The index number allows you to look at previous crash contexts. Contexts from the last 24 line card crashes are saved on the GRP card. If the GRP reloads, the last 24 line card crash contexts are lost. For example, show context slot 3 2 shows the second most recent crash for line card in slot 3. Index numbers are displayed by the show context summary command.
debug	(Optional) Displays crash information as a hex record dump in addition to one of the options listed.

show controllers (GRP image)

To display information that is specific to the hardware, use the **show controllers** privileged EXEC command.

show controllers [**atm** *slot-number* | **clock** | **csar** [**register**] | **csc-fpga** | **dp83800** | **fab-clk** | **fia** [**register**] | **pos** [*slot-number*] [**details**] | **queues** [*slot-number*] | **sca** | **xbar**]

Syntax Description

atm <i>slot-number</i>	(Optional) Displays the ATM controllers. Number is slot-number/port-number (for example, 4/0). Slot numbers range from 0 to 11 for the Cisco 12012 router and from 0 to 7 for the Cisco 12008 router.
clock	(Optional) Displays the clock card configuration.
csar [register]	(Optional) Displays the Cisco Cell Segmentation and Reassembly (CSAR) information. CSAR is the name of the chip on the card that handles traffic between the GRP and the switch fabric interface ASICs.
csc-fpga	(Optional) Displays the clock and scheduler card register information in the field programmable gate array (FPGA).
dp83800	(Optional) Displays the Ethernet information on the GRP card.
fab-clk	(Optional) Display the switch fabric clock register information. The switch fabric clock FPGA is a chip that monitors the incoming fabric clock generated by the switch fabric. This clock is needed by each card connecting to the switch fabric to properly communicate with it. Two switch fabric clocks arrive at each card; only one can be used. The FPGA monitors both clocks and selects which one to use if only one of them is running.
fia [register]	(Optional) Displays the fabric interface ASIC information and optionally displays the register information.
pos [<i>slot-number</i>] [details]	(Optional) Displays the POS framer state and optionally displays all the details for the interface. Number is slot-number/port-number (for example, 4/0). Slot numbers range from 0 to 11 for the Cisco 12012 router and from 0 to 7 for the Cisco 12008 router.
queues [<i>slot-number</i>]	(Optional) Displays the SDRAM buffer carve information and optionally displays the information for a specific line card. The SDRAM buffer carve information displayed is suggested carve information from the GRP card to the line card. Line cards might change the shown percentages based on SDRAM available. Slot numbers range from 0 to 11 for the Cisco 12012 router and from 0 to 7 for the Cisco 12008.

sca	(Optional) Displays the SCA register information. The SCA is an ASIC that arbitrates among the line cards requests to use the switch fabric.
xbar	(Optional) Displays the crossbar register information. The XBAR is an ASIC that switches the data as it passes through the switch fabric.

show controllers (line card image)

To display information that is specific to the hardware on a line card, use the **attach** privileged EXEC command to connect to the line card and then use the **show controllers** privileged EXEC command or the **execute-on** privileged EXEC command.

show controllers atm [[*port-number*] [**all** | **sar** | **summary**]]

show controllers fia [**register**]

show controllers {**frfab** | **tofab**} {**bma** {**microcode** | **ms-inst** | **register**} | **qelem** *start-queue-element* [*end-queue-element*] | **qnum** *start-queue-number* [*end-queue-number*] | **queues** | **statistics**}

show controllers io

show controllers l3

show controllers pos {**framers** | **queues** | **registers** | **rxsram** *port-number queue-start-address* [*queue-length*] | **txsram** *port-number queue-start-address* [*queue-length*]}

Syntax Description

atm	Displays the ATM controller information.
<i>port-number</i>	(Optional) Displays request for the physical interface on the ATM card. The range of choices is from 0 to 3.
all	(Optional) Lists all details.
sar	(Optional) Lists SAR interactive command.
summary	(Optional) Lists SAR status summary.
fia	Displays the fabric interface ASIC information.
register	(Optional) Displays the register information.
frfab	(Optional) Displays the “from” (transmit) fabric information.
tofab	(Optional) Displays the “to” (receive) fabric information.
bma	For the frfab or tofab keywords, displays microcode, micro sequencer, or register information for the silicon queuing engine (SQE), also known as the buffer management ASIC (BMA).
microcode	Displays SQE information for the microcode bundled in the line card and currently running version.
ms-inst	Displays SQE information for the micro sequencer instruction.
register	Displays silicon queuing engine (SQE) information for the register.

qelem	For the frfab or tofab keywords, displays the SDRAM buffer pool queue element summary information.
<i>start-queue-element</i>	Specifies the start queue element number from 0 to 65535.
<i>end-queue-element</i>	(Optional) Specifies the end queue element number from 0 to 65535).
qnum	For the frfab or tofab keywords, displays the SDRAM buffer pool queue detail information.
<i>start-queue-number</i>	Specifies the start free queue number (from 0 to 127).
<i>end-queue-number</i>	(Optional) Specifies the end free queue number (from 0 to 127).
queues	For the frfab or tofab keywords, displays the SDRAM buffer pool information.
statistics	For the frfab or tofab keywords, displays the BMA counters.
io	Displays input/output registers.
l3	Displays Layer 3 ASIC information.
pos	Displays packet-over-sonic (POS) information for framer registers, framer queues, and ASIC registers.
framers	Displays the POS framer registers.
queues	Displays the POS framer queue information.
registers	Displays the ASIC registers.
rxsram	Displays the receive queue SRAM.
<i>port-number</i>	Specifies a port number (valid range is from 0 to 3).
<i>queue-start-address</i>	Specifies the queue SRAM logical starting address.
<i>queue-length</i>	(Optional) Specifies the queue SRAM length.
txsram	Displays the transmit queue SRAM.

show controllers logging

To display logging information about a Versatile Interface Processor (VIP) card, use the **show controllers logging** privileged EXEC command.

```
show controllers vip slot-number logging
```

Syntax Description

<i>vip slot-number</i>	VIP slot number.
------------------------	------------------

show controllers tech-support

To display general information about a Versatile Interface Processor (VIP) card when reporting a problem, use the **show controllers tech-support** privileged EXEC command.

```
show controllers vip slot-number tech-support
```

Syntax Description

<i>vip slot-number</i>	VIP slot number.
------------------------	------------------

show debugging

To display information about the types of debugging that are enabled for your router, use the **show debugging** privileged EXEC command.

show debugging

Syntax Description This command has no arguments or keywords.

show diag

To display hardware information including DRAM and static RAM (SRAM) on line cards, use the **show diag** command in privileged EXEC mode.

show diag [*slot-number*] [**details**] [**summary**]

Syntax Description	<i>slot-number</i>	(Optional) Slot number of the interface.
	details	(Optional) Displays more details than the normal show diag output.
	summary	(Optional) Displays a summary (one line per slot) of the chassis.

show environment

To display temperature, voltage, and blower information on the Cisco 7000 series, Cisco 7200 series, Cisco 7500 series routers, Cisco AS5300 series Access Servers, and Cisco 12000 series Gigabit Switch Routers (GSRs), use the **show environment** privileged EXEC command.

show environment [**alarms** | **all** | **fans** | **hardware** | **last** | **leds** | **power-supply** | **table** | **temperatures** | **voltages**]



Note

The availability of keywords will depend on your system.

Syntax Description	alarms	(Optional) Displays the alarm contact information.
	all	(Optional) Displays a detailed listing of all environmental monitor parameters (for example, the power supplies, temperature readings, voltage readings, and blower speeds). This is the default.
	fans	(Optional) Displays blower and fan information.
	hardware	(Optional) Displays hardware-specific information.
	last	(Optional) Displays information on the last measurement made.
	leds	(Optional) Displays the status of the MBus LEDs on the clock and scheduler cards and switch fabric cards.

power-supply	(Optional) Displays power supply voltage and current information. If applicable, displays the status of the Redundant Power Supply (RPS).
table	(Optional) Displays the temperature, voltage, and blower ranges and thresholds.
temperature	(Optional) Displays temperature information.
voltages	(Optional) Displays voltage information.

show gsr

To display hardware information on the Cisco 12000 series Gigabit Switch Routers (GSRs), use the **show gsr EXEC** command.

```
show gsr [chassis-info [details]]
```

Syntax Description	
chassis-info	(Optional) Displays backplane NVRAM information.
details	(Optional) In addition to the information displayed, this option includes hexadecimal output of the backplane NVRAM information.

show gt64010 (7200)

To display all GT64010 internal registers and interrupt status on the Cisco 7200 series routers, use the **show gt64010 EXEC** command.

```
show gt64010
```

Syntax Description This command has no arguments or keywords.

show logging

To display the state of logging (syslog), use the **show logging** privileged EXEC command.

```
show logging [history | slot slot-number | summary]
```

Syntax Description	
history	(Optional) Displays information in the syslog history table only.
slot <i>slot-number</i>	(Optional) Displays information in the syslog history table for a specific line card. Slot numbers range from 0 to 11 for the Cisco 12012 router and 0 to 7 for the Cisco 12008 router.
summary	(Optional) Displays counts of messages by type for each line card.

show memory

To show statistics about memory, including memory-free pool statistics, use the **show memory** EXEC command.

```
show memory [memory-type] [free] [summary]
```

Syntax Description		
	<i>memory-type</i>	(Optional) Memory type to display (processor , multibus , io , or sram). If <i>memory-type</i> is not specified, statistics for all memory types present are displayed.
	free	(Optional) Displays free memory statistics.
	summary	(Optional) Displays a summary of memory usage including the size and number of blocks allocated for each address of the system call that allocated the block.

show pci

To display information about the peripheral component interconnect (PCI) hardware registers or bridge registers for the Cisco 7200 series routers, use the **show pci** EXEC command.

```
show pci { hardware | bridge [register] }
```

Syntax Description		
	hardware	Displays PCI hardware registers.
	bridge	Displays PCI bridge registers.
	<i>register</i>	(Optional) Number of a specific bridge register in the range from 0 to 7. If not specified, this command displays information about all registers.

show pci hardware

To display information about the Host-PCI bridge, use the **show pci hardware** EXEC command.

```
show pci hardware
```

Syntax Description	
	This command has no arguments or keywords.

show processes

To display information about the active processes, use the **show processes** EXEC command.

```
show processes [cpu]
```

Syntax Description		
	cpu	(Optional) Displays detailed CPU utilization statistics.

show processes memory

To show memory used, use the **show processes memory** EXEC command.

show processes memory

Syntax Description This command has no arguments or keywords.

show protocols

To display the configured protocols, use the **show protocols** EXEC command.

This command shows the global and interface-specific status of any configured Level 3 protocol; for example, IP, DECnet, IPX, AppleTalk, and so on.

show protocols

Syntax Description This command has no arguments or keywords.

show stacks

To monitor the stack usage of processes and interrupt routines, use the **show stacks** EXEC command.

show stacks

Syntax Description This command has no arguments or keywords.

show subsys

To display the subsystem information, use the **show subsys** privileged EXEC command.

show subsys [*class class* | *name name*]

Syntax Description	class <i>class</i>	(Optional) Displays the subsystems of the specified class. Valid classes are driver , kernel , library , management , protocol , and registry .
	name <i>name</i>	(Optional) Displays the specified subsystem. Use the asterisk character (*) as a wildcard at the end of the name to list all subsystems, starting with the specified characters.

show tcp

To display the status of TCP connections, use the **show tcp** EXEC command.

```
show tcp [line-number]
```

Syntax Description	<i>line-number</i>	(Optional) Absolute line number of the line for which you want to display Telnet connection status.
---------------------------	--------------------	---

show tcp brief

To display a concise description of TCP connection endpoints, use the **show tcp brief** EXEC command.

```
show tcp brief [all]
```

Syntax Description	all	(Optional) Displays status for all endpoints. Without this keyword, endpoints in the LISTEN state are not shown.
---------------------------	------------	--

show tdm connections

To display a snapshot of the time-division multiplexing (TDM) bus connection memory in a Cisco AS5200 access server, use the **show tdm connections** EXEC command.

```
show tdm connections [motherboard | slot slot-number]
```

Syntax Description	motherboard	(Optional) Motherboard in the Cisco AS5200 access server.
	slot slot-number	(Optional) Slot number.

show tdm data

To display a snapshot of the time-division multiplexing (TDM) bus data memory in a Cisco AS5200 access server, use the **show tdm data** EXEC command.

```
show tdm data [motherboard | slot slot-number]
```

Syntax Description	motherboard	(Optional) Motherboard in the Cisco AS5200 access server.
	slot slot-number	(Optional) Slot number.

show tech-support

To display general information about the router when it reports a problem, use the **show tech-support** privileged EXEC command.

show tech-support [page] [password]

Syntax Description	
page	(Optional) Causes the output to display a page of information at a time. Use the Return key to display the next line of output or use the space bar to display the next page of information. If not used, the output scrolls (that is, does not stop for page breaks).
password	(Optional) Leaves passwords and other security information in the output. If not used, passwords and other security-sensitive information in the output are replaced with the label “<removed>” (this is the default).

test flash

To test Flash memory on MCI and envm Flash EPROM interfaces, use the **test flash** EXEC command.

test flash

Syntax Description This command has no arguments or keywords.

test interfaces

To test the system interfaces on the modular router, use the **test interfaces** EXEC command.

test interfaces

Syntax Description This command has no arguments or keywords.

test memory

To perform a test of Multibus memory (including nonvolatile memory) on the modular router, use the **test memory** EXEC command. The memory test overwrites memory.

test memory

Syntax Description This command has no arguments or keywords.

trace (privileged)

To discover the routes that packets will actually take when traveling to their destination, use the **trace** privileged EXEC command.

```
trace [protocol] [destination]
```

Syntax Description	<i>protocol</i>	(Optional) Protocols that can be used are appletalk , clns , ip and vines .
	<i>destination</i>	(Optional) Destination address or host name on the command line. The default parameters for the appropriate protocol are assumed and the tracing action begins.

trace (user)

To discover the IP routes that packets will actually take when traveling to their destination, use the **trace** EXEC command.

```
trace [protocol] [destination]
```

Syntax Description	<i>protocol</i>	(Optional) Protocols that can be used are appletalk , clns , ip and vines .
	<i>destination</i>	(Optional) Destination address or host name on the command line. The default parameters for the appropriate protocol are assumed and the tracing action begins.



SNMP Commands

This chapter describes the function and syntax of the Simple Network Management Protocol (SNMP) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Configuration Fundamentals Command Reference*.

no snmp-server

To disable Simple Network Management Protocol (SNMP) agent operation, use the **no snmp-server** global configuration command.

```
no snmp-server
```

Syntax Description This command has no arguments or keywords.

show management event

To display the Simple Network Management Protocol (SNMP) Event values that have been configured on your routing device through the use of the Event MIB, use the **show management event** command in privileged EXEC mode.

```
show management event
```

Syntax Description This command has no arguments or keywords.

show snmp

To check the status of Simple Network Management Protocol (SNMP) communications, use the **show snmp** EXEC command.

```
show snmp
```

Syntax Description This command has no arguments or keywords.

show snmp engineID

To display the identification of the local Simple Network Management Protocol (SNMP) engine and all remote engines that have been configured on the router, use the **show snmp engineID** EXEC command.

```
show snmp engineID
```

Syntax Description This command has no arguments or keywords.

show snmp group

To display the names of groups on the router and the security model, the status of the different views, and the storage type of each group, use the **show snmp group** EXEC command.

```
show snmp group
```

Syntax Description This command has no keywords or arguments.

show snmp pending

To display the current set of pending Simple Network Management Protocol (SNMP) requests, use the **show snmp pending** EXEC command.

```
show snmp pending
```

Syntax Description This command has no arguments or keywords.

show snmp sessions

To display the current Simple Network Management Protocol (SNMP) sessions, use the **show snmp sessions** EXEC command.

```
show snmp sessions [brief]
```

Syntax Description

brief	(Optional) Displays a list of sessions only. Does not display session statistics.
--------------	---

show snmp user

To display information on each Simple Network Management Protocol (SNMP) username in the group username table, use the **show snmp user** EXEC command.

```
show snmp user
```

Syntax Description This command has no arguments or keywords.

snmp-server access-policy

This command is no longer valid. The functionality provided by this command has been removed from the Cisco IOS software.

snmp-server chassis-id

To provide a message line identifying the Simple Network Management Protocol (SNMP) server serial number, use the **snmp-server chassis-id** global configuration command. To restore the default value, if any, use the **no** form of this command.

```
snmp-server chassis-id text
```

```
no snmp-server chassis-id
```

Syntax Description

<i>text</i>	Message you want to enter to identify the chassis serial number.
-------------	--

snmp-server community

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP), use the **snmp-server community** global configuration command. To remove the specified community string, use the **no** form of this command.

```
snmp-server community string [view view-name] [ro | rw] [number]
```

```
no snmp-server community string
```

Syntax Description

<i>string</i>	Community string that acts like a password and permits access to the SNMP protocol.
view <i>view-name</i>	(Optional) Name of a previously defined view. The view defines the objects available to the community.
ro	(Optional) Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.

rw	(Optional) Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.
<i>number</i>	(Optional) Integer from 1 to 99 that specifies an access list of IP addresses that are allowed to use the community string to gain access to the SNMP agent.

snmp-server contact

To set the system contact (sysContact) string, use the **snmp-server contact** global configuration command. To remove the system contact information, use the **no** form of this command.

snmp-server contact *text*

no snmp-server contact

Syntax Description

<i>text</i>	String that describes the system contact information.
-------------	---

snmp-server context

This command is no longer valid. The functionality provided by this command has been removed from the Cisco IOS software.

snmp-server enable informs

This command has no functionality. To enable the sending of Simple Network Management Protocol (SNMP) inform notifications, use one of the **snmp-server enable traps** *notification-type* global configuration commands combined with the **snmp-server host** *host-addr* **informs** global configuration command.

snmp-server enable traps

To enable all Simple Network Management Protocol (SNMP) notifications (traps or informs) available on your system, use the **snmp-server enable traps** global configuration command. To disable all available SNMP notifications, use the **no** form of this command.

snmp-server enable traps [*notification-type*]

no snmp-server enable traps [*notification-type*]

Syntax Description*notification-type*

(Optional) Type of notification (trap or inform) to enable or disable. If no type is specified, all notifications available on your device are enabled or disabled. The notification type can be one of the following keywords:

- **config**—Controls configuration notifications, as defined in the CISCO-CONFIG-MAN-MIB (enterprise 1.3.6.1.4.1.9.9.43.2). The notification type is: (1) ciscoConfigManEvent.
- **dls** [**circuit** | **tconn**]—Controls DLSw notifications, as defined in the CISCO-DLSW-MIB (enterprise 1.3.6.1.4.1.9.10.9.1.7). When the **dls** keyword is used, you can specify the specific notification types you wish to enable or disable. If no keyword is used, all DLSw notification types are enabled. The option can be one of the following keywords:
 - **circuit**—Enables DLSw circuit traps:
 - (5) ciscoDlswTrapCircuitUp
 - (6) ciscoDlswTrapCircuitDown
 - **tconn**—Enables DLSw peer transport connection traps:
 - (1) ciscoDlswTrapTConnPartnerReject
 - (2) ciscoDlswTrapTConnProtViolation
 - (3) ciscoDlswTrapTConnUp
 - (4) ciscoDlswTrapTConnDown
- **ds0-busyout**—Sends notification whenever the busyout of a DS0 interface changes state (Cisco AS5300 platform only). This is from the CISCO-POP-MGMT-MIB (enterprise 1.3.6.1.4.1.9.10.19.2) and the notification type is: (1) cpmDS0BusyoutNotification.
- **ds1-loopback**—Sends notification whenever the DS1 interface goes into loopback mode (Cisco AS5300 platform only). This notification type is defined in the CISCO-POP-MGMT-MIB (enterprise 1.3.6.1.4.1.9.10.19.2) as: (2) cpmDS1LoopbackNotification.
- **entity**—Controls Entity MIB modification notifications. This notification type is defined in the ENTITY-MIB (enterprise 1.3.6.1.2.1.47.2) as: (1) entConfigChange.
- **hsrp**—Controls Hot Standby Routing Protocol (HSRP) notifications, as defined in the CISCO-HSRP-MIB (enterprise 1.3.6.1.4.1.9.9.106.2). The notification type is: (1) cHsrpStateChange.
- **ipmulticast**—Controls IP multicast notifications.
- **modem-health**—Controls modem-health notifications.
- **rsvp**—Controls Resource Reservation Protocol (RSVP) notifications.
- **rtr**—Controls Service Assurance Agent/ Response Time Reporter (RTR) notifications.
- **syslog**—Controls error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the **logging history level** command.
- **xgcp**—Sends External Media Gateway Control Protocol (XGCP) notifications. This notification is from the XGCP-MIB-VISMI.my and the notifications are: enterprise 1.3.6.1.3.90.2 (1) xgcpUpDownNotification.

snmp-server enable traps aaa_server

To enable authentication, authorization, and accounting (AAA) server state-change Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps aaa_server** global configuration command. To disable AAA server state-change SNMP notifications, use the **no** form of this command.

```
snmp-server enable traps aaa_server
```

```
no snmp-server enable traps aaa_server
```

Syntax Description This command has no arguments or keywords.

snmp-server enable traps atm pvc

To enable the sending of ATM permanent virtual circuit (PVC) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps atm pvc** global configuration command. To disable ATM PVC-specific SNMP notifications, use the **no** form of this command.

```
snmp-server enable traps atm pvc [interval seconds] [fail-interval seconds]
```

```
no snmp-server enable traps atm pvc
```

Syntax Description	interval seconds	(Optional) Minimum period between successive traps, in the range from 1 to 3600. Generation of PVC traps is dampened by the notification interval in order to prevent trap storms. No traps are sent until the interval lapses.
	fail-interval seconds	(Optional) Minimum period for storing the failed time stamp, in the range from 0 to 3600.

snmp-server enable traps bgp

To enable Border Gateway Protocol (BGP) state-change Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps bgp** global configuration command. To disable BGP state-change SNMP notifications, use the **no** form of this command.

```
snmp-server enable traps bgp
```

```
no snmp-server enable traps bgp
```

Syntax Description This command has no arguments or keywords.

snmp-server enable traps calltracker

To enable Call Tracker CallSetup and Call Terminate Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps calltracker** global configuration command. To disable Call Tracker SNMP notifications, use the **no** form of this command.

snmp-server enable traps calltracker

no snmp-server enable traps calltracker

Syntax Description This command has no arguments or keywords.

snmp-server enable traps envmon

To enable Environmental Monitor Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps envmon** global configuration command. To disable environmental monitor SNMP notifications, use the **no** form of this command.

snmp-server enable traps envmon [shutdown] [voltage] [temperature] [fan] [supply]

no snmp-server enable traps envmon [shutdown] [voltage] [temperature] [fan] [supply]

Syntax Description	
shutdown	(Optional) Controls shutdown notifications. A ciscoEnvMonShutdownNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.1) is sent if the environmental monitor detects a testpoint reaching a critical state and is about to initiate a shutdown.
voltage	(Optional) Controls voltage notifications. A ciscoEnvMonVoltageNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.2) is sent if the voltage measured at a given testpoint is outside the normal range for the testpoint (i.e. is at the warning, critical, or shutdown stage). For access servers, this notification is defined as the caemVoltageNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.61.2.2).
temperature	(Optional) Controls temperature notifications. A ciscoEnvMonTemperatureNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.3) is sent if the temperature measured at a given testpoint is outside the normal range for the testpoint (i.e. is at the warning, critical, or shutdown stage). For access servers, this notification is defined as the caemTemperatureNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.61.2.1).
fan	(Optional) Controls fan failure notifications. A ciscoEnvMonFanNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.3.4) is sent if any one of the fans in a fan array fails.
supply	(Optional) Controls Redundant Power Supply (RPS) failure notifications. A ciscoEnvMonRedundantSupplyNotification (enterprise MIB OID 1.3.6.1.4.1.9.9.13.2.5) is sent if a redundant power supply fails.

snmp-server enable traps frame-relay

To enable Frame Relay DLCI link status Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps frame-relay** global configuration command. To disable Frame Relay link status SNMP notifications, use the **no** form of this command.

snmp-server enable traps frame-relay

no snmp-server enable traps frame-relay

Syntax Description This command has no arguments or keywords.

snmp-server enable traps isdn

To enable the sending of Integrated Services Digital Network (ISDN) specific Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps isdn** global configuration command. To disable ISDN-specific SNMP notifications, use the **no** form of this command.

snmp-server enable traps isdn [call-information] [chan-not-avail] [isdnu-interface] [layer2]

no snmp-server enable traps isdn [call-information] [chan-not-avail] [isdnu-interface] [layer2]

Syntax Description	
call-information	(Optional) Controls SNMP ISDN call information notifications, as defined in the CISCO-ISDN-MIB (enterprise 1.3.6.1.4.1.9.9.26.2). Notification types are: <ul style="list-style-type: none"> demandNbrCallInformation (1) This notification is sent to the manager whenever a successful call clears, or a failed call attempt is determined to have ultimately failed. In the event that call retry is active, then this is after all retry attempts have failed. However, only one such notification is sent in between successful call attempts; subsequent call attempts do not generate notifications of this type. demandNbrCallDetails (2) This notification is sent to the manager whenever a call connects, or clears, or a failed call attempt is determined to have ultimately failed. In the event that call retry is active, then this is after all retry attempts have failed. However, only one such notification is sent in between successful call attempts; subsequent call attempts do not generate notifications of this type.
chan-not-avail	(Optional) Controls SNMP ISDN channel-not-available notifications. ISDN PRI channel-not-available traps are generated when a requested DS0 channel is not available, or when there is no modem available to take the incoming call. These notifications are available only for ISDN PRI interfaces.
isdnu-interface	(Optional) Controls SNMP ISDN U interface notifications.
layer2	(Optional) Controls SNMP ISDN Layer 2 transition notifications.

snmp-server enable traps snmp

To enable the sending of RFC 1157 Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps snmp** global configuration command. To disable RFC 1157 SNMP notifications, use the **no** form of this command.

```
snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [warmstart]
```

```
no snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart]
[warmstart]
```

Syntax Description	
authentication	(Optional) Controls the sending of SNMP authentication failure notifications. An authenticationFailure(4) trap signifies that the sending device is the addressee of a protocol message that is not properly authenticated. The authentication method depends on the version of SNMP being used. For SNMPv1 or SNMPv2c, authentication failure occurs for packets with an incorrect community string. For SNMPv3, authentication failure occurs for packets with an incorrect SHA/MD5 authentication key or for a packet that is outside of the authoritative SNMP engine's window (for example, falls outside of configured access lists or time ranges).
linkup	(Optional) Controls the sending of SNMP linkUp notifications. A linkUp(3) trap signifies that the sending device recognizes that one of the communication links represented in the agent's configuration has come up.
linkdown	(Optional) Controls the sending of SNMP linkDown notifications. A linkDown(2) trap signifies that the sending device recognizes a failure in one of the communication links represented in the agent's configuration.
coldstart	(Optional) Controls the sending of SNMP coldStart notifications. A coldStart(0) trap signifies that the sending device is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered.
warmstart	(Optional) Controls the sending of SNMP warmStart notifications. A warmStart(1) trap signifies that the sending device is reinitializing itself such that neither the agent configuration nor the protocol entity implementation is altered.

snmp-server enable traps repeater

To enable or disable standard repeater (hub) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps repeater** global configuration command. To disable repeater notifications, use the **no** form of this command.

```
snmp-server enable traps repeater [health] [reset]
```

```
no snmp-server enable traps repeater [health] [reset]
```

Syntax Description	<p>health (Optional) The rptrHealth trap conveys information related to the operational status of the repeater. This trap is sent either when the value of rptrOperStatus changes, or upon completion of a nondisruptive test.</p> <p>The rptrOperStatus object indicates the operational state of the repeater. Status values are as follows:</p> <ul style="list-style-type: none"> • other(1)—undefined or unknown status • ok(2)—no known failures • rptrFailure(3)—repeater-related failure • groupFailure(4)—group-related failure • portFailure(5)—port-related failure • generalFailure(6)—failure, unspecified type
	<p>reset (Optional) The rptrResetEvent trap is sent on completion of a repeater reset action (triggered by the transition to a START state by a manual command). The rptrResetEvent trap is not sent when the agent restarts and sends an SNMP coldStart or warmStart trap.</p>

snmp-server enable traps voice poor-qov

To enable poor quality of voice Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps voice poor-qov** global configuration command. To disable poor quality of voice SNMP notifications, use the **no** form of this command.

```
snmp-server enable traps voice poor-qov
```

```
no snmp-server enable traps voice poor-qov
```

Syntax Description This command has no arguments or keywords.

snmp-server engineID

To configure a name for either the local or remote Simple Network Management Protocol (SNMP) engine on the router, use the **snmp-server engineID** global configuration command. To remove a specified SNMP group, use the **no** form of this command.

```
snmp-server engineID {local engineid-string | remote ip-address [udp-port port]
engineid-string }
```

```
no snmp-server engineID
```

Syntax Description	<p>local Specifies the local copy of SNMP on the router. (You must specify either local or remote.)</p>
	<p><i>engineid-string</i> The name of a copy of SNMP.</p>

remote	Specifies the remote copy of SNMP on the router. (You must specify either local or remote .)
<i>ip-address</i>	The IP address of the device that contains the remote copy of SNMP.
udp-port	(Optional) Specifies a UDP port of the host to use.
<i>port</i>	(Optional) The socket number on the remote device that contains the remote copy of SNMP.

snmp-server group

To configure a new Simple Network Management Protocol (SNMP) group, or a table that maps SNMP users to SNMP views, use the **snmp-server group** global configuration command. To remove a specified SNMP group, use the **no** form of this command.

```
snmp-server group groupname {v1 | v2c | v3 {auth | noauth | priv}} [read readview]
[write writeview] [notify notifyview] [access access-list]
```

```
no snmp-server group
```

Syntax Description

<i>groupname</i>	The name of the group.
v1	The least secure of the possible security models.
v2c	The second least secure of the possible security models. It allows for the transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.
v3	The most secure of the possible security models.
auth	Specifies authentication of a packet without encrypting it.
noauth	Specifies no authentication of a packet.
priv	Specifies authentication of a packet with encryption.
read	(Optional) The option that allows you to specify a read view.
<i>readview</i>	A string (not to exceed 64 characters) that is the name of the view that enables you only to view the contents of the agent.
write	(Optional) The option that allows you to specify a write view.
<i>writeview</i>	A string (not to exceed 64 characters) that is the name of the view that enables you to enter data and configure the contents of the agent.
notify	(Optional) The option that allows you to specify a notify view.
<i>notifyview</i>	A string (not to exceed 64 characters) that is the name of the view that enables you to specify a notify, inform, or trap.
access	(Optional) The option that enables you to specify an access list.
<i>access-list</i>	A string (not to exceed 64 characters) that is the name of the access list.

snmp-server host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** global configuration command. To remove the specified host, use the **no** form of this command.

```
snmp-server host host-addr [traps | informs] [version { 1 | 2c | 3 [auth | noauth | priv]}]
community-string [udp-port port] [notification-type]
```

```
no snmp-server host host [traps | informs]
```

Syntax Description

<i>host-addr</i>	Name or Internet address of the host (the targeted recipient).
traps	(Optional) Sends SNMP traps to this host. This is the default.
informs	(Optional) Sends SNMP informs to this host.
version	(Optional) Version of the SNMP used to send the traps. Version 3 is the most secure model, because it allows packet encryption with the priv keyword. If you use the version keyword, one of the following must be specified: <ul style="list-style-type: none"> • 1—SNMPv1. This option is not available with informs. • 2c—SNMPv2C. • 3—SNMPv3. The following three optional keywords can follow the version 3 keyword: <ul style="list-style-type: none"> – auth (Optional). Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication – noauth (Default). The noAuthNoPriv security level. This is the default if the [auth noauth priv] keyword choice is not specified. – priv (Optional). Enables Data Encryption Standard (DES) packet encryption (also called “privacy”).
<i>community-string</i>	Password-like community string sent with the notification operation. Though you can set this string using the snmp-server host command by itself, we recommend you define this string using the snmp-server community command prior to using the snmp-server host command.
udp-port <i>port</i>	(Optional) UDP port of the host to use. The default is 162.

notification-type (Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the following keywords:

- **bgp**—Sends Border Gateway Protocol (BGP) state change notifications.
 - **calltracker**—Sends Call Tracker call-start/call-end notifications.
 - **config**—Sends configuration notifications.
 - **dspu**—Sends downstream physical unit (DSPU) notifications.
 - **entity**—Sends Entity MIB modification notifications.
 - **envmon**—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded.
 - **frame-relay**—Sends Frame Relay notifications.
 - **hsrp**—Sends Hot Standby Routing Protocol (HSRP) notifications.
 - **isdn**—Sends Integrated Services Digital Network (ISDN) notifications.
 - **llc2**—Sends Logical Link Control, type 2 (LLC2) notifications.
 - **repeater**—Sends standard repeater (hub) notifications.
 - **rsrb**—Sends remote source-route bridging (RSRB) notifications.
 - **rsvp**—Sends Resource Reservation Protocol (RSVP) notifications.
 - **rtr**—Sends SA Agent (RTR) notifications.
 - **sdlc**—Sends Synchronous Data Link Control (SDLC) notifications.
 - **sdllc**—Sends SDLLC notifications.
 - **snmp**—Sends any enabled RFC 1157 SNMP linkUp, linkDown, authenticationFailure, warmStart, and coldStart notifications.
 - **stun**—Sends serial tunnel (STUN) notifications.
 - **syslog**—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the **logging history level** command.
 - **tty**—Sends Cisco enterprise-specific notifications when a Transmission Control Protocol (TCP) connection closes.
 - **voice**—Sends SNMP poor quality of voice traps, when used with the **snmp enable peer-trap poor qov** command.
 - **x25**—Sends X.25 event notifications.
-

snmp-server informs

To specify inform request options, use the **snmp-server informs** global configuration command. To return the settings to the defaults, use the **no** form of this command.

```
snmp-server informs [retries retries] [timeout seconds] [pending pending]
```

```
no snmp-server informs [retries retries] [timeout seconds] [pending pending]
```

Syntax Description	retries <i>retries</i>	(Optional) Maximum number of times to resend an inform request. The default is 3.
	timeout <i>seconds</i>	(Optional) Number of seconds to wait for an acknowledgment before resending. The default is 30 seconds.
	pending <i>pending</i>	(Optional) Maximum number of informs waiting for acknowledgments at any one time. When the maximum is reached, older pending informs are discarded. The default is 25.

snmp-server location

To set the system location string, use the **snmp-server location** global configuration command. To remove the location string, use the **no** form of this command.

snmp-server location *text*

no snmp-server location

Syntax Description	<i>text</i>	String that describes the system location information.
---------------------------	-------------	--

snmp-server manager

To start the Simple Network Management Protocol (SNMP) manager process, use the **snmp-server manager** global configuration command. To stop the SNMP manager process, use the **no** form of this command.

snmp-server manager

no snmp-server manager

Syntax Description	This command has no arguments or keywords.	
---------------------------	--	--

snmp-server manager session-timeout

To set the amount of time before a nonactive session is destroyed, use the **snmp-server manager session-timeout** global configuration command. To return the value to its default, use the **no** form of this command.

snmp-server manager session-timeout *seconds*

no snmp-server manager session-timeout

Syntax Description	<i>seconds</i>	Number of seconds before an idle session is timed out. The default is 600 seconds.
---------------------------	----------------	--

snmp-server packetsize

To establish control over the largest Simple Network Management Protocol (SNMP) packet size permitted when the SNMP server is receiving a request or generating a reply, use the **snmp-server packetsize** global configuration command. To restore the default value, use the **no** form of this command.

```
snmp-server packetsize byte-count
```

```
no snmp-server packetsize
```

Syntax Description	<i>byte-count</i>	Integer byte count from 484 to 8192. The default is 1500 bytes.
---------------------------	-------------------	---

snmp-server queue-length

To establish the message queue length for each trap host, use the **snmp-server queue-length** global configuration command.

```
snmp-server queue-length length
```

Syntax Description	<i>length</i>	Integer that specifies the number of trap events that can be held before the queue must be emptied.
---------------------------	---------------	---

snmp-server system-shutdown

To use the Simple Network Management Protocol (SNMP) message reload feature, the router configuration must include the **snmp-server system-shutdown** global configuration command. To prevent an SNMP system-shutdown request (from an SNMP manager) from resetting the Cisco agent, use the **no** form of this command.

```
snmp-server system-shutdown
```

```
no snmp-server system-shutdown
```

Syntax Description	This command has no arguments or keywords.	
---------------------------	--	--

snmp-server tftp-server-list

To limit the TFTP servers used via Simple Network Management Protocol (SNMP) controlled TFTP operations (saving and loading configuration files) to the servers specified in an access list, use the **snmp-server tftp-server-list** global configuration command. To disable this feature, use the **no** form of this command.

```
snmp-server tftp-server-list number
```

```
no snmp-server tftp-server-list
```

Syntax Description	<i>number</i>	Standard IP access list number from 1 to 99.
--------------------	---------------	--

snmp-server trap-authentication

The **snmp-server trap-authentication** command has been replaced by the **snmp-server enable traps snmp authentication** command. See the description of the **snmp-server enable traps snmp** command in this chapter for more information.

snmp-server trap link

To enable linkUp/linkDown Simple Network Management Protocol (SNMP) traps which are compliant with RFC2233, use the **snmp-server trap link** command in global configuration mode. To disable IETF compliant functionality and revert to the default Cisco implementation of linkUp/linkDown traps, use the **no** form of this command.

```
snmp-server trap link ietf
```

```
no snmp-server trap link ietf
```

Syntax Description	<i>ietf</i>	This required keyword indicates to the command parser that you would like to link functionality of SNMP linkUp/linkDown traps to the Internet Engineering Task Force (IETF) standard (as opposed to the previous Cisco implementation).
--------------------	-------------	---

snmp-server trap-source

To specify the interface (and hence the corresponding IP address) that an Simple Network Management Protocol (SNMP) trap should originate from, use the **snmp-server trap-source** global configuration command. To remove the source designation, use the **no** form of the command.

snmp-server trap-source *interface*

no snmp-server trap-source

Syntax Description	<i>interface</i>	Interface from which the SNMP trap originates. The argument includes the interface type and number in platform-specific syntax (for example, <i>type/slot/port</i>).
---------------------------	------------------	---

snmp-server trap-timeout

To define how often to try resending trap messages on the retransmission queue, use the **snmp-server trap-timeout** global configuration command.

snmp-server trap-timeout *seconds*

Syntax Description	<i>seconds</i>	Integer that sets the interval (in seconds) for resending the messages.
---------------------------	----------------	---

snmp-server user

To configure a new user to a Simple Network Management Protocol (SNMP) group, use the **snmp-server user** global configuration command. To remove a user from an SNMP group, use the **no** form of the command.

snmp-server user *username groupname* [**remote** *host* [**udp-port** *port*]]
{ **v1** | **v2c** | **v3** [**encrypted**] [**auth** { **md5** | **sha** } *auth-password*] } [**access** *access-list*]

no snmp-server user

Syntax Description	<i>username</i>	The name of the user on the host that connects to the agent.
	<i>groupname</i>	The name of the group to which the user belongs.
	remote <i>host</i>	(Optional) Specifies a remote SNMP entity to which the user belongs, and the hostname or IP address of that entity.
	udp-port <i>port</i>	(Optional) Specifies the UDP port number of the remote host. The default is UDP port 162.
	v1	Specifies that SNMPv1 should be used.
	v2c	Specifies that SNMPv2c should be used.

v3	Specifies that the SNMPv3 security model should be used. Allows the use of the encrypted or auth keyword.
encrypted	(Optional) Specifies whether the password appears in encrypted format (a series of digits, masking the true characters of the string).
auth	(Optional) Specifies which authentication level should be used.
md5	The HMAC-MD5-96 authentication level.
sha	The HMAC-SHA-96 authentication level.
<i>auth-password</i>	A string (not to exceed 64 characters) that enables the agent to receive packets from the host.
access <i>access-list</i>	(Optional) Specifies an access list to be associated with this SNMP user. The <i>access-list</i> argument represents a value from 1 to 99 that is the identifier of the standard IP access list.

snmp-server view

To create or update a view entry, use the **snmp-server view** global configuration command. To remove the specified Simple Network Management Protocol (SNMP) server view entry, use the **no** form of this command.

```
snmp-server view view-name oid-tree {included | excluded}
```

```
no snmp-server view view-name
```

Syntax Description

<i>view-name</i>	Label for the view record that you are updating or creating. The name is used to reference the record.
<i>oid-tree</i>	Object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as <i>1.3.6.2.4</i> , or a word, such as <i>system</i> . Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example, <i>1.3.*.4</i> .
included excluded	Type of view. You must specify either included or excluded .

snmp trap link-status

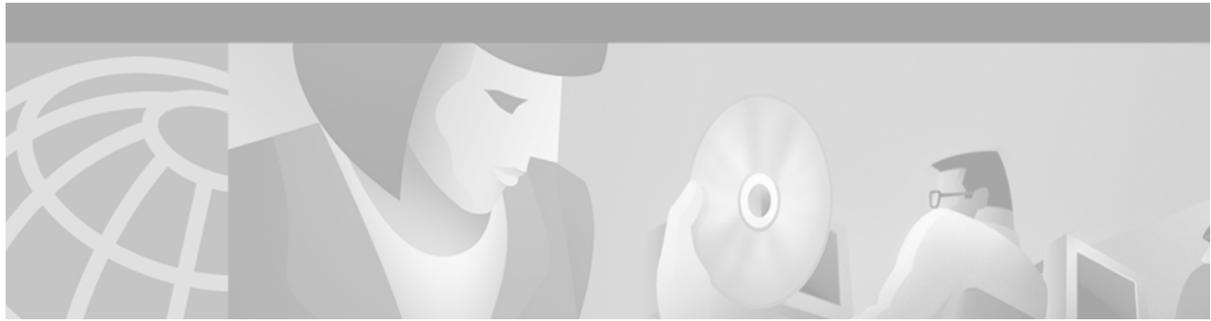
To enable Simple Network Management Protocol (SNMP) link trap generation, use the **snmp trap link-status** interface configuration command. To disable SNMP link traps, use the **no** form of this command.

```
snmp trap link-status
```

```
no snmp trap link-status
```

Syntax Description

This command has no arguments or keywords.



CDP Commands

This chapter describes the function and syntax of the Cisco Discovery Protocol (CDP) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Configuration Fundamentals Command Reference*.

cdp advertise-v2

To enable Cisco Discovery Protocol Version 2 (CDPv2) advertising functionality on a device, use the **cdp advertise-v2** global configuration command. To disable advertising CDPv2 functionality, use the **no** form of the command.

cdp advertise-v2

no cdp advertise-v2

Syntax Description This command has no arguments or keywords.

cdp enable

To enable Cisco Discovery Protocol (CDP) on an interface, use the **cdp enable** interface configuration command. To disable CDP on an interface, use the **no** form of this command.

cdp enable

no cdp enable

Syntax Description This command has no arguments or keywords.

cdp holdtime

To specify the amount of time the receiving device should hold a Cisco Discovery Protocol (CDP) packet from your router before discarding it, use the **cdp holdtime** global configuration command. To revert to the default setting, use the **no** form of this command.

cdp holdtime *seconds*

no cdp holdtime

Syntax Description*seconds*Specifies the hold time to be sent in the CDP update packets.

cdp run

To enable Cisco Discovery Protocol (CDP), use the **cdp run** global configuration command. To disable CDP, use the **no** form of this command.

cdp run

no cdp run

Syntax Description

This command has no arguments or keywords.

cdp timer

To specify how often the Cisco IOS software sends Cisco Discovery Protocol (CDP) updates, use the **cdp timer** global configuration command. To revert to the default setting, use the **no** form of this command.

cdp timer *seconds*

no cdp timer

Syntax Description*seconds*Specifies how often the Cisco IOS software sends CDP updates.

clear cdp counters

To reset Cisco Discovery Protocol (CDP) traffic counters to zero, use the **clear cdp counters** privileged EXEC command.

clear cdp counters

Syntax Description

This command has no arguments or keywords.

clear cdp table

To clear the table that contains Cisco Discovery Protocol (CDP) information about neighbors, use the **clear cdp table** privileged EXEC command.

```
clear cdp table
```

Syntax Description This command has no arguments or keywords.

show cdp

To display global Cisco Discovery Protocol (CDP) information, including timer and hold-time information, use the **show cdp** privileged EXEC command.

```
show cdp
```

Syntax Description This command has no arguments or keywords.

show cdp entry

To display information about a specific neighboring device discovered using Cisco Discovery Protocol (CDP), use the **show cdp entry** privileged EXEC command.

```
show cdp entry { * | device-name[*] [protocol | version] }
```

Syntax Description	*	Displays all of the CDP neighbors.
	<i>device-name</i>	Name of the neighbor about which you want information.
	<i>device-name</i> *	You can enter an asterisk (*) at the end of an <i>entry-name</i> as a wildcard. For example, entering show cdp entry dev* will match all entries which begin with dev .
	protocol	(Optional) Limits the display to information about the protocols enabled on a router.
	version	(Optional) Limits the display to information about the version of software running on the router.

show cdp interface

To display information about the interfaces on which Cisco Discovery Protocol (CDP) is enabled, use the **show cdp interface** privileged EXEC command.

```
show cdp interface [type number]
```

Syntax Description	<i>type</i>	(Optional) Type of interface about which you want information.
	<i>number</i>	(Optional) Number of the interface about which you want information.

show cdp neighbors

To display detailed information about neighboring devices discovered using Cisco Discovery Protocol (CDP), use the **show cdp neighbors** privileged EXEC command.

```
show cdp neighbors [type number] [detail]
```

Syntax Description	<i>type</i>	(Optional) Type of the interface connected to the neighbors about which you want information.
	<i>number</i>	(Optional) Number of the interface connected to the neighbors about which you want information.
	detail	(Optional) Displays detailed information about a neighbor (or neighbors) including network address, enabled protocols, hold time, and software version.

show cdp traffic

To display information about traffic between devices gathered using Cisco Discovery Protocol (CDP), use the **show cdp traffic** privileged EXEC command.

```
show cdp traffic
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--



RMON Commands

This chapter describes the function and syntax of the Remote Monitoring (RMON) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Configuration Fundamentals Command Reference*.

rmon

To enable Remote Monitoring (RMON) on an Ethernet interface, use the **rmon** interface configuration command. To disable RMON on the interface, use the **no rmon** form of this command.

```
rmon { native | promiscuous }
```

```
no rmon
```

Syntax Description

native	Enables RMON on the Ethernet interface. In native mode, the router processes only packets destined for this interface.
promiscuous	Enables RMON on the Ethernet interface. In promiscuous mode, the router examines every packet.

rmon alarm

To set an alarm on any MIB object, use the **rmon alarm** global configuration command. To disable the alarm, use the **no rmon alarm** form of this command.

```
rmon alarm number variable interval { delta | absolute } rising-threshold value [event-number]  
falling-threshold value [event-number] [owner string]
```

```
no rmon alarm number
```

Syntax Description

<i>number</i>	Alarm number, which is identical to the alarmIndex in the alarmTable in the Remote Monitoring (RMON) MIB.
<i>variable</i>	MIB object to monitor, which translates into the alarmVariable used in the alarmTable of the RMON MIB.

<i>interval</i>	Time in seconds the alarm monitors the MIB variable, which is identical to the alarmInterval used in the alarmTable of the RMON MIB.
delta	Tests the change between MIB variables, which affects the alarmSampleType in the alarmTable of the RMON MIB.
absolute	Tests each MIB variable directly, which affects the alarmSampleType in the alarmTable of the RMON MIB.
rising-threshold value	Value at which the alarm is triggered.
<i>event-number</i>	(Optional) Event number to trigger when the rising or falling threshold exceeds its limit. This value is identical to the alarmRisingEventIndex or the alarmFallingEventIndex in the alarmTable of the RMON MIB.
falling-threshold value	Value at which the alarm is reset.
owner string	(Optional) Specifies an owner for the alarm, which is identical to the alarmOwner in the alarmTable of the RMON MIB.

rmon capture-userdata

To disable the packet zeroing feature that initializes the user payload portion of each Remote Monitoring (RMON) MIB packet, use the **rmon capture-userdata** global configuration command. To enable packet zeroing, use the **no** form of this command.

rmon capture-userdata

no rmon capture-userdata

Syntax Description This command has no arguments or keywords.

rmon collection history

To enable Remote Monitoring (RMON) MIB history group of statistics on an interface, use the **rmon collection history** interface configuration command. To remove a specified RMON history group of statistics, use the **no** form of this command.

rmon collection history {controlEntry *integer*} [owner *ownername*] [buckets *bucket-number*] [interval *seconds*]

no rmon collection history {controlEntry *integer*} [owner *ownername*] [buckets *bucket-number*] [interval *seconds*]

Syntax Description	controlEntry	Specifies the RMON group of statistics using a value.
	<i>integer</i>	A value from 1 to 65535 that identifies the RMON group of statistics and matches the index value returned for Simple Network Management Protocol (SNMP) requests.

owner	(Optional) Specifies the name of the owner of the RMON group of statistics.
<i>ownername</i>	(Optional) Records the name of the owner of the RMON group of statistics.
buckets	(Optional) Specifies the maximum number of buckets desired for the RMON collection history group of statistics.
<i>bucket-number</i>	(Optional) A value associated with the number of buckets specified for the RMON collection history group of statistics.
interval	(Optional) Specifies the number of seconds in each polling cycle.
<i>seconds</i>	(Optional) The number of seconds in each polling cycle.

rmon collection host

To enable a Remote Monitoring (RMON) MIB host collection group of statistics on the interface, use the **rmon collection host** interface configuration command. To remove the specified RMON host collection, use the **no** form of the command.

```
rmon collection host {controlEntry integer} [owner ownername]
```

```
no rmon collection host {controlEntry integer} [owner ownername]
```

Syntax Description

controlEntry	Specifies the RMON group of statistics using a value.
<i>integer</i>	A value from 1 to 65535 that identifies the RMON group of statistics and matches the index value returned for Simple Network Management Protocol (SNMP) requests.
owner	(Optional) Specifies the name of the owner of the RMON group of statistics.
<i>ownername</i>	(Optional) Records the name of the owner of the RMON group of statistics

rmon collection matrix

To enable a Remote Monitoring (RMON) MIB matrix group of statistics on an interface, use the **rmon collection matrix** interface configuration command. To remove a specified RMON matrix group of statistics, use the **no** form of the command.

```
rmon collection matrix {controlEntry integer} [owner ownername]
```

```
no rmon collection matrix {controlEntry integer} [owner ownername]
```

Syntax Description

controlEntry	Specifies the RMON group of statistics using a value.
<i>integer</i>	A value between 1 and 65535 that identifies the RMON group of statistics and matches the index value returned for Simple Network Management Protocol (SNMP) requests.

owner	(Optional) Specifies the name of the owner of the RMON group of statistics.
<i>ownername</i>	(Optional) Records the name of the owner of the RMON group of statistics.

rmon collection rmon1

To enable all possible autoconfigurable Remote Monitoring (RMON) MIB statistic collections on the interface, use the **rmon collection rmon1** command in interface configuration mode. To disable these statistic collections on the interface, use the **no** form of the command.

rmon collection rmon1 {**controlEntry** *integer*} [**owner** *ownername*]

no rmon collection rmon1 {**controlEntry** *integer*} [**owner** *ownername*]

Syntax Description

controlEntry	Specifies the RMON group of statistics using a value.
<i>integer</i>	A value from 1 to 65535 that identifies the RMON group of statistics and matches the index value returned for Simple Network Management Protocol (SNMP) requests.
owner	(Optional) Specifies the name of the owner of the RMON group of statistics.
<i>ownername</i>	(Optional) Records the name of the owner of the RMON group of statistics.

rmon event

To add or remove an event in the RMON event table that is associated with an RMON event number, use the **rmon event** global configuration command. To disable RMON on the interface, use the **no** form of this command.

rmon event *number* [**log**] [**trap** *community*] [**description** *string*] [**owner** *string*]

no rmon event *number*

Syntax Description

<i>number</i>	Assigned event number, which is identical to the eventIndex in the eventTable in the RMON MIB.
log	(Optional) Generates an RMON log entry when the event is triggered and sets the eventType in the RMON MIB to log or log-and-trap.
trap <i>community</i>	(Optional) SNMP community string used for this trap. Configures the setting of the eventType in the RMON MIB for this row as either snmp-trap or log-and-trap. This value is identical to the eventCommunityValue in the eventTable in the RMON MIB.

description <i>string</i>	(Optional) Specifies a description of the event, which is identical to the event description in the eventTable of the RMON MIB.
owner <i>string</i>	(Optional) Owner of this event, which is identical to the eventOwner in the eventTable of the RMON MIB.

rmon queuesize

To change the size of the queue that holds packets for analysis by the Remote Monitoring (RMON) process, use the **rmon queuesize** global configuration command. To restore the default value, use the **no** form of this command.

rmon queuesize *size*

no rmon queuesize

Syntax Description	<i>size</i>	Number of packets allowed in the queue awaiting RMON analysis. Default queue size is 64 packets.
---------------------------	-------------	--

show rmon

To display the current RMON agent status on the router, use the **show rmon EXEC** command.

show rmon [**alarms** | **capture** | **events** | **filter** | **history** | **hosts** | **matrix** | **statistics** | **task** | **topn**]

Syntax Description	alarms	(Optional) Displays the RMON alarm table.
	capture	(Optional) Displays the RMON buffer capture table. Available on Cisco 2500 series and Cisco AS5200 series only.
	events	(Optional) Displays the RMON event table.
	filter	(Optional) Displays the RMON filter table. Available on Cisco 2500 series and Cisco AS5200 series only.
	history	(Optional) Displays the RMON history table. Available on Cisco 2500 series and Cisco AS5200 series only.
	hosts	(Optional) Displays the RMON hosts table. Available on Cisco 2500 series and Cisco AS5200 series only.
	matrix	(Optional) Displays the RMON matrix table. Available on Cisco 2500 series and Cisco AS5200 series only.
	statistics	(Optional) Displays the RMON statistics table. Available on Cisco 2500 series and Cisco AS5200 series only.
	task	(Optional) Displays general RMON statistics. This is the default.
	topn	(Optional) Displays the RMON top-n hosts table. Available on Cisco 2500 series and Cisco AS5200 series only.

show rmon alarms

To display the contents of the RMON alarm table of the router, use the **show rmon alarms EXEC** command.

```
show rmon alarms
```

Syntax Description This command has no arguments or keywords.

show rmon capture

To display the contents of the router's RMON capture table, use the **show rmon capture EXEC** command.

```
show rmon capture
```

Syntax Description This command has no arguments or keywords.

show rmon events

To display the contents of the router's RMON event table, use the **show rmon events EXEC** command.

```
show rmon events
```

Syntax Description This command has no arguments or keywords.

show rmon filter

To display the contents of the router's RMON filter table, use the **show rmon filter EXEC** command.

Syntax Description This command has no arguments or keywords.

show rmon history

To display the contents of the router's RMON history table, use the **show rmon history EXEC** command.

```
show rmon history
```

Syntax Description This command has no arguments or keywords.

show rmon hosts

To display the contents of the router's RMON hosts table, use the **show rmon hosts** EXEC command.

```
show rmon hosts
```

Syntax Description This command has no arguments or keywords.

show rmon matrix

To display the contents of the router's RMON matrix table, use the **show rmon matrix** EXEC command.

```
show rmon matrix
```

Syntax Description This command has no arguments or keywords.

show rmon statistics

To display the contents of the router's RMON statistics table, use the **show rmon statistics** EXEC command.

```
show rmon statistics
```

Syntax Description This command has no arguments or keywords.

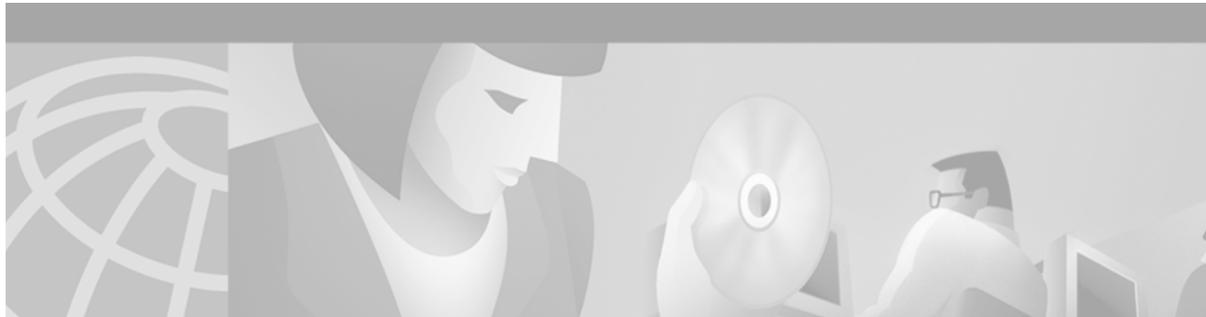
show rmon topn

To display the contents of the router's RMON Top-N host table, use the **show rmon topn** EXEC command.

```
show rmon topn
```

Syntax Description This command has no arguments or keywords.

■ show rmon topn



Cisco Service Assurance Agent Commands

This chapter describes the function and syntax of the Cisco Service Assurance Agent (SA Agent) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Configuration Fundamentals Command Reference*.

buckets-of-history-kept

To set the number of history buckets that are kept during the operation lifetime of the SA Agent, use the **buckets-of-history-kept** RTR Entry configuration command. To return to the default value, use the **no** form of this command.

buckets-of-history-kept *size*

no buckets-of-history-kept

Syntax Description	<i>size</i>	Number of history buckets kept during the lifetime of the operation. The default is 50 buckets.
---------------------------	-------------	---

data-pattern

To specify the data pattern in an SA Agent udpEcho operation to test for data corruption, use the **data pattern** RTR Entry configuration mode command. To remove the data pattern specification, use the **no** form of this command.

data-pattern *hex-pattern*

no data-pattern *hex-pattern*

Syntax Description	<i>hex-pattern</i>	Hexadecimal sting to use for monitoring the specified operation.
---------------------------	--------------------	--

distributions-of-statistics-kept

To set the number of statistic distributions kept per hop during the lifetime operation of the SA Agent, use the **distributions-of-statistics-kept** RTR Entry configuration command. To return to the default value, use the **no** form of this command.

distributions-of-statistics-kept *size*

no distributions-of-statistics-kept

Syntax Description	<i>size</i>	Number of statistic distributions kept per hop. The default is 1 distribution.
--------------------	-------------	--

filter-for-history

To define the type of information kept in the history table for an SA Agent operation, use the **filter-for-history** RTR Entry configuration command. To return to the default value, use the **no** form of this command.

filter-for-history { **none** | **all** | **overThreshold** | **failures** }

no filter-for-history { **none** | **all** | **overThreshold** | **failures** }

Syntax Description	none	No history kept. This is the default.
	all	All operation operations attempted are kept in the history table.
	overThreshold	Only packets that are over the threshold are kept in the history table.
	failures	Only packets that fail for any reason are kept in the history table.

frequency

To set the rate at which a specified SA Agent operation is sent into the network, use the **frequency** RTR Entry configuration command. To return to the default value, use the **no** form of this command.

frequency *seconds*

no frequency

Syntax Description	<i>seconds</i>	Number of seconds between the SA Agent probe operations.
--------------------	----------------	--

hops-of-statistics-kept

To set the number of hops for which statistics are maintained per path for the SA Agent operation, use the **hops-of-statistics-kept** RTR Entry configuration command. To return to the default value, use the **no** form of this command.

hops-of-statistics-kept *size*

no hops-of-statistics-kept

Syntax Description	<i>size</i>	Number of hops for which statistics are maintained per path. The default is 16 hops for type pathEcho and 1 hop for type echo .
---------------------------	-------------	---

http-raw-request

To explicitly specify the options for a GET request for an SA Agent HTTP operation, use the **http-raw-request** command in RTR Entry configuration mode.

http-raw-request

Syntax Description	This command has no arguments or keywords.
---------------------------	--

hours-of-statistics-kept

To set the number of hours for which statistics are maintained for the SA Agent operation, use the **hours-of-statistics-kept** RTR Entry configuration command. To return to the default value, use the **no** form of this command.

hours-of-statistics-kept *hours*

no hours-of-statistics-kept

Syntax Description	<i>hours</i>	Number of hours that the router maintains statistics. The default is 2 hours.
---------------------------	--------------	---

lives-of-history-kept

To set the number of lives maintained in the history table for the SA Agent operation, use the **lives-of-history-kept** RTR Entry configuration command. To return to the default value, use the **no** form of this command.

lives-of-history-kept *lives*

no lives-of-history-kept

Syntax Description

<i>lives</i>	Number of lives maintained in the history table for the operation. If you specify 0 lives, history is not collected for the operation.
--------------	---

lsr-path

To define a loose source routing (LSR) path for a Cisco SA Agent IP echo operation, use the **lsr-path** RTR Entry configuration command. To remove the definition, use the **no** form of this command.

lsr-path {*hostname* | *ip-address*} [{*hostname* | *ip-address*} ...]

no lsr-path

Syntax Description

{ <i>hostname</i> <i>ip-address</i> }	Hostname or IP address of the first hop in the LSR path.
[{ <i>hostname</i> <i>ip-address</i> } ...]	(Optional) Indicates that you can continue specifying host destinations until you specify the final host target. Each hostname or ip-address specified indicates another hop on the path. The maximum number of hops you can specify is eight. Do not enter the dots (...).

owner

To configure the Simple Network Management Protocol (SNMP) owner of an SA Agent operation, use the **owner** RTR Entry configuration command. To return to the default value, use the **no** form of this command.

owner *text*

no owner

Syntax Description

<i>text</i>	Name of the SNMP owner from 0 to 255 ASCII characters. The default is none.
-------------	---

paths-of-statistics-kept

To set the number of paths for which statistics are maintained per hour for the SA Agent operation, use the **paths-of-statistics-kept** RTR Entry configuration command. To return to the default value, use the **no** form of this command.

paths-of-statistics-kept *size*

no paths-of-statistics-kept

Syntax Description*size*

Number of paths for which statistics are maintained per hour. The default is 5 paths for **type pathEcho** and 1 path for **type echo**.

request-data-size

To set the protocol data size in the payload of the SA Agent operation's request packet, use the **request-data-size** RTR Entry configuration command. To return to the default value, use the **no** form of this command.

request-data-size *byte*

no request-data-size

Syntax Description*byte*

Size of the protocol data in the payload of the request packet of the operation. Range is 0 to the maximum of the protocol. The default is 1 byte.

response-data-size

To set the protocol data size in the payload of an SA Agent operation's response packet, use the **response-data-size** RTR Entry configuration command. To return to the default value, use the **no** form of this command.

response-data-size *byte*

no response-data-size

Syntax Description*byte*

Size of the protocol data in the payload in the operation's response packet. For "appl" protocols, the default is 0 bytes. For all others, the default is the same value as the **request-data-size**.

rtr

To begin configuring an SA Agent operation by entering RTR Entry configuration mode, use the **rtr** command in global configuration mode. To remove all configuration information for an operation, including the schedule of the operation, reaction configuration, and reaction triggers, use the **no** form of this command.

rtr *op-number*

no rtr *op-number*

Syntax Description	<i>op-number</i>	Operation number used for the identification of the SA Agent operation you wish to configure.
---------------------------	------------------	---

rtr key-chain

To enable SA Agent control message authentication and specify an MD5 key chain, use the **rtr key-chain** global configuration command. To remove control message authentication, use the **no** form of this command.

rtr key-chain *name*

no rtr key-chain

Syntax Description	<i>name</i>	Name of MD5 key chain.
---------------------------	-------------	------------------------

rtr low-memory

To specify how much unused memory must be available to allow SA Agent configuration, use the **rtr low-memory** global configuration command. To remove the type configuration for the operation, use the **no** form of this command.

rtr low-memory *value*

no rtr low-memory

Syntax Description	<i>value</i>	Specifies amount of memory, in bytes, that must be available to configure SA Agent (RTR). The range is from 0 to the maximum amount of free memory bytes available.
---------------------------	--------------	---

rtr reaction-configuration

To configure certain actions to occur based on events under the control of the SA Agent, use the **rtr reaction-configuration** global configuration command. To return to the default values of the operation, use the **no** form of this command.

```
rtr reaction-configuration operation-number [verify-error-enable] [connection-loss-enable]
[timeout-enable] [threshold-falling milliseconds] [threshold-type option] [action-type
option]
```

```
no rtr reaction-configuration operation-number
```

Syntax Description

<i>operation-number</i>	Number of the SA Agent operation to configure.
verify-error-enable	(Optional) Enables error verification. The default is disabled.
connection-loss-enable	(Optional) Enables checking for connection loss in connection-oriented protocols. Disabled by default.
timeout-enable	(Optional) Enables checking for response time reporting operation timeouts based on the timeout value configured for the operation with the timeout RTR Entry configuration command. The default is disabled.
threshold-falling <i>milliseconds</i>	(Optional) Sets the falling threshold (standard RMON-type hysteresis mechanism) in milliseconds. When the falling threshold is met, generate a resolution reaction event. The rising of the operation over threshold is set with the threshold RTR Entry configuration command. The default value is 3000 ms.
threshold-type <i>option</i>	(Optional) Specify the algorithm used by the SA Agent to calculate over and falling threshold violations. The value for <i>option</i> can be one of the following keywords: <ul style="list-style-type: none"> never—Do not calculate threshold violations (the default). immediate—When the response time exceeds the rising over threshold or drops below the falling threshold, immediately perform the action defined by action-type. consecutive [<i>occurrences</i>]—When the response time exceeds the rising threshold consecutively five times or drops below the falling threshold consecutively five times, perform the action defined by action-type. Optionally specify the number of consecutive occurrences. The default is 5. xofy [<i>x-value y-value</i>]—When the response time exceeds the rising threshold five out of the last five times or drops below the falling threshold five out of the last five times, perform the action defined by action-type. Optionally specify the number of violations that must occur and the number that must occur within a specified number. The default is 5 for both x-value and y-value.

- **average** [*attempts*]—When the average of the last five response times exceeds the rising threshold or when the average of the last five response times drops below the falling threshold, perform the action defined by **action-type**. Optionally specify the number of operations to average. The default is the average of the last five response time operations. For example: if the threshold of the operation is 5000 ms and the last three attempts results of the operation are 6000, 6000, and 5000 ms, the average would be $6000 + 6000 + 5000 = 17000/3 > 5000$, thus violating the 5000-ms threshold.

action-type option

(Optional) Specify what action or combination of actions the operation performs when you configure **connection-loss-enable** or **timeout-enable**, or threshold events occur. For the **action-type** to occur for threshold events, the **threshold-type** must be defined to anything other than **never**. Option can be one of the following keywords:

- **none**—No action is taken.
- **trapOnly**—Send an SNMP trap on both over and falling threshold violations.
- **nmvtOnly**—Send an SNA NMVT Alert on over threshold violation and an SNA NMVT Resolution on falling threshold violations.
- **triggerOnly**—Have one or more target operation's operational state make the transition from "pending" to "active" on over (and falling) threshold violations. The target operations are defined with the **rtr reaction-trigger** command. A target operation will continue until its life expires as specified by the target operation's life value configured with the **rtr schedule** global configuration command. A triggered target operation must finish its life before it can be triggered again.
- **trapAndNmvt**—Send a combination of **trapOnly** and **nmvtOnly**.
- **trapAndTrigger**—Send a combination of **trapOnly** and **triggerOnly**.
- **nmvtAndTrigger**—Send a combination of **nmvtOnly** and **triggerOnly**.
- **trapNmvtAndTrigger**—Send a combination of **trapOnly**, **nmvtOnly**, and **triggerOnly**.

rtr reaction-trigger

To define a second SA Agent operation to make the transition from a pending state to an active state when one of the trigger action-type options are defined with the **rtr reaction-configuration** global configuration command, use the **rtr reaction-trigger** global configuration command. To remove the trigger combination, use the **no** form of this command.

rtr reaction-trigger *operation-number target-operation*

no rtr reaction-trigger *operation-number*

Syntax Description	<i>operation-number</i>	Number of the operation in the active state that has the action-type set with the rtr reaction-configuration global configuration command.
	<i>target-operation</i>	Number of the operation in the pending state that is waiting to be triggered with the rtr global configuration command.

rtr reset

To perform a shutdown and restart of the SA Agent, use the **rtr reset** global configuration command.

```
rtr reset
```

Syntax Description This command has no arguments or keywords.

rtr responder

To enable the SA Agent Responder feature, use the **rtr responder** global configuration command. To disable the SA Agent Responder, use the **no** form of this command.

```
rtr responder [type {udpEcho | tcpConnect} [ipaddress ipaddr] port port]
```

```
no rtr responder [type {udpEcho | tcpConnect} [ipaddress ipaddr] port port]
```

Syntax Description	type udpEcho	(Optional) Specifies that the responder will accept and return udpEcho operation packets.
		
	Note	You should use type udpEcho keyword combination for Jitter (UDP Echo +) operations as well.
	type tcpConnect	(Optional) Specifies that the responder will accept and return tcpConnect operation packets.
	ipaddress ipaddr	(Optional) Specifies the IP address that the operation will be received at.
	port port	(Optional) Specifies the port number that the operation will be received on.

rtr restart

To restart an SA Agent operation, use the **rtr restart** global configuration command.

```
rtr restart operation-number
```

Syntax Description	<i>operation-number</i>	Number of the SA Agent operation to restart. SA Agent allows a maximum of 500 operations.
---------------------------	-------------------------	---

rtr schedule

To configure the time parameters for an SA Agent operation, use the **rtr schedule** global configuration command. To stop the operation and place it in the default state (**pending**), use the **no** form of this command.

```
rtr schedule operation-number [life {forever | seconds}] [start-time
  {hh:mm[:ss] [month day | day month] | pending | now | after hh:mm[:ss]}] [ageout seconds]
```

```
no rtr schedule operation-number
```

Syntax Description

<i>operation-number</i>	(Required) Number of the SA Agent operation to schedule.
life <i>seconds</i>	(Optional) Number of seconds the operation actively collects information. The default is 3600 seconds (one hour).
life forever	(Optional) Schedules the operation to run indefinitely.
start-time	(Optional) Time when the operation starts collecting information. If the start-time is not specified, no information is collected until the start-time is configured or a trigger occurs that performs a start-time now .
start-time <i>hh:mm[:ss]</i>	(Optional) Specifies an absolute start time using hour, minute, and (optionally) second. Use the 24-hour clock notation. For example, start-time 01:02 means “start at 1:02 a.m.,” and start-time 13:01:30 means “start at 1:01 p.m. and 30 seconds.” The current day is implied unless you specify a <i>month</i> and <i>day</i> .
<i>month</i>	(Optional) Name of the month to start the operation in. If <i>month</i> is not specified, the current month is used. Use of this argument requires that a day be specified as well. You can specify the month with the full English name, or using the first three letters of the month.
<i>day</i>	(Optional) Number of the day (in the range 1 to 31) to start the operation on. If a day is not specified, the current day is used. Use of this argument requires that a month be specified as well.
start-time pending	(Optional) No information is collected. This is the default value.
start-time now	(Optional) Indicates that the operation should start immediately.
start-time after <i>hh:mm:ss</i>	(Optional) Indicates that the operation should start <i>hh</i> hours, <i>mm</i> minutes, and <i>ss</i> seconds after this command was entered.
ageout <i>seconds</i>	(Optional) Number of seconds to keep the operation in memory when it is not actively collecting information. The default is 0 seconds (never ages out).

samples-of-history-kept

To set the number of entries kept in the history table per bucket for the SA Agent operation, use the **samples-of-history-kept** RTR Entry configuration command. To return to the default value, use the **no** form of this command.

samples-of-history-kept *samples*

no samples-of-history-kept

Syntax Description	<i>samples</i>	Number of entries kept in the history table per bucket. The default is 16 entries for type pathEcho and 1 entry for type echo .
---------------------------	----------------	---

show rtr application

To display global information about the SA Agent feature, use the **show rtr application** EXEC command.

show rtr application [**tabular** | **full**]

Syntax Description	tabular	(Optional) Displays information in a column format reducing the number of screens required to display the information.
	full	(Optional) Displays all information using identifiers next to each displayed value. This is the default.

show rtr authentication

To display SA Agent RTR authentication information, use the **show rtr authentication** EXEC command.

show rtr authentication

Syntax Description	This command has no arguments or keywords.
---------------------------	--

show rtr collection-statistics

To display statistical errors for all SA Agent operations or a specified operation, use the **show rtr collection-statistics** EXEC command.

show rtr collection-statistics [*operation-number*] [**tabular** | **full**]

Syntax Description	<i>operation-number</i>	(Optional) Number of the SA Agent operation to display.
	tabular	(Optional) Display information in a column format reducing the number of screens required to display the information.
	full	(Optional) Display all information using identifiers next to each displayed value. This is the default.

show rtr configuration

To display configuration values including all defaults for all SA Agent operations or the specified operation, use the **show rtr configuration** EXEC command.

```
show rtr configuration [operation] [tabular | full]
```

Syntax Description	<i>operation</i>	(Optional) Number of the SA Agent operation to display.
	tabular	(Optional) Display information in a column format reducing the number of screens required to display the information.
	full	(Optional) Display all information using identifiers next to each displayed value. This is the default.

show rtr distributions-statistics

To display statistic distribution information (captured response times) for all SA Agent operations or the specified operation, use the **show rtr distributions-statistics** EXEC command.

```
show rtr distributions-statistics [operation] [tabular | full]
```

Syntax Description	<i>operation</i>	(Optional) Number of the SA Agent operation to display.
	tabular	(Optional) Displays information in a column format reducing the number of screens required to display the information. This is the default.
	full	(Optional) Displays all information using identifiers next to each displayed value.

show rtr history

To display history collected for all SA Agent operations or for a specified operation, use the **show rtr history** EXEC command.

```
show rtr history [operation-number] [tabular | full]
```

Syntax Description	<i>operation-number</i>	(Optional) Displays history for only the specified operation.
	tabular	(Optional) Displays information in a column format reducing the number of screens required to display the information. This is the default.
	full	(Optional) Displays all information using identifiers next to each displayed value.

show rtr operational-state

To display the operational state of all SA Agent operations or the specified operation, use the **show rtr operational-state EXEC** command.

```
show rtr operational-state [operation-number] [tabular | full]
```

Syntax Description	<i>operation-number</i>	(Optional) Number of the SA Agent operation to display.
	tabular	(Optional) Displays information in a column format reducing the number of screens required to display the information.
	full	(Optional) Displays all information using identifiers next to each displayed value. This is the default.

show rtr reaction-trigger

To display the reaction trigger information for all SA Agent operations or the specified operation, use the **show rtr reaction-trigger EXEC** command.

```
show rtr reaction-trigger [operation-number] [tabular | full]
```

Syntax Description	<i>operation-number</i>	(Optional) Number of the SA Agent operation to display.
	tabular	(Optional) Display information in a column format reducing the number of screens required to display the information.
	full	(Optional) Display all information using identifiers next to each displayed value. This is the default.

show rtr responder

To display SA Agent RTR Responder information, use the **show rtr responder EXEC** command.

```
show rtr responder
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--

show rtr totals-statistics

To display the total statistical values (accumulation of error counts and completions) for all SA Agent operations or the specified operation, use the **show rtr totals-statistics EXEC** command.

show rtr totals-statistics [*number*] [**tabular** | **full**]

Syntax Description		
	<i>number</i>	(Optional) Number of the SA Agent operation to display.
	tabular	(Optional) Display information in a column format reducing the number of screens required to display the information.
	full	(Optional) Display all information using identifiers next to each displayed value. This is the default.

statistics-distribution-interval

To set the time interval for each statistics distribution kept for the SA Agent, use the **statistics-distribution-interval RTR** Entry configuration command. To return to the default value, use the **no** form of this command.

statistics-distribution-interval *milliseconds*

no statistics-distribution-interval

Syntax Description		
	<i>milliseconds</i>	Number of milliseconds (ms) used for each statistics distribution kept. The default is 20 ms.

tag

To create a user-specified identifier for an SA Agent operation, use the **tag RTR** Entry configuration command. To remove a tag from a operation, use the **no** form of this command.

tag *text*

no tag

Syntax Description		
	<i>text</i>	Name of a group that this operation belongs to. From 0 to 16 ASCII characters.

threshold

To set the rising threshold (hysteresis) that generates a reaction event and stores history information for the SA Agent operation, use the **threshold** RTR Entry configuration command. To return to the default value, use the **no** form of this command.

threshold *milliseconds*

no threshold

Syntax Description

milliseconds

Number of milliseconds required for a rising threshold to be declared. The default value is 5000 ms.

timeout

To set the amount of time the SA Agent operation waits for a response from its request packet, use the **timeout** RTR Entry configuration command. To return to the default value, use the **no** form of this command.

timeout *milliseconds*

no timeout

Syntax Description

milliseconds

Number of milliseconds (ms) the operation waits to receive a response from its request packet. The default is 5000 ms.

tos

To define a type of service (ToS) byte in the IP header of SA Agent operations, use the **tos** RTR Entry configuration command. To return to the default value, use the **no** form of this command.

tos *number*

no tos

Syntax Description

number

Service type byte in the IP header. The range is 0 to 255. The default is 0.

type dhcp

To configure a Dynamic Host Configuration Protocol SA Agent operation, use the **type dhcp** RTR Entry configuration command. To disable a DHCP SA Agent operation, use the **no** form of this command.

```
type dhcp [source-ipaddr source-ipaddr] [dest-ipaddr dest-ipaddr] [option decimal-option
  [circuit-id circuit-id] [remote-id remote-id] [subnet-mask subnet-mask]]
```

```
no type dhcp
```

Syntax Description

source-ipaddr <i>source-ipaddr</i>	(Optional) Source name or IP address.
dest-ipaddr <i>dest-ipaddr</i>	(Optional) Destination name or IP address.
option <i>decimal-option</i>	(Optional) Option number. The only currently valid value is 82. DHCP option 82 allows you to specify the circuit ID, remote ID, or the subnet mask for the destination DHCP server.
circuit-id <i>circuit-id</i>	(Optional) Circuit ID in hexadecimal.
remote-id <i>remote-id</i>	(Optional) Remote ID in hexadecimal.
subnet-mask <i>subnet-mask</i>	(Optional) Subnet mask IP address. The default value is 255.255.255.0.

type dlsw

To configure a data-link switching (DLSw) SA Agent operation, use the **type dlsw** RTR Entry configuration command. To remove the type configuration for the operation, use the **no** form of this command.

```
type dlsw peer-ipaddr ipaddr
```

```
no type dlsw peer-ipaddr ipaddr
```

Syntax Description

peer-ipaddr	Peer destination.
<i>ipaddr</i>	IP address.

type dns

To configure a Domain Name System (DNS) SA Agent operation, use the **type dns** RTR Entry configuration command. To remove the type configuration for the operation, use the **no** form of this command.

```
type dns target-addr {ip-address | hostname} name-server ip-address
```

```
no type dns target-addr {ip-address | hostname} name-server ip-address
```

Syntax Description

target-addr { <i>ip-address</i> <i>hostname</i> }	Target (destination) IP address or hostname.
name-server <i>ip-address</i>	IP address of the Domain Name Server.

type echo

To configure an SA Agent end-to-end echo response time probe operation, use the **type echo** RTR Entry configuration command. To remove the operation from the configuration, use the **no** form of this command.

```
type echo protocol protocol-type target [source-ipaddr ip-address]
```

```
no type echo protocol protocol-type target [source-ipaddr ip-address]
```

Syntax Description

protocol <i>protocol-type</i> <i>target</i>	<p>Protocol used by the operation. The <i>protocol-type target</i> argument combination must take one of the following forms:</p> <ul style="list-style-type: none"> • ipIcmpEcho { <i>ip-address</i> <i>hostname</i> }—IP/ICMP Echo. Requires a destination IP address or IP host name. • snaRUEcho <i>sna-hostname</i>—SNA's SSCP Native Echo. Requires the host name defined for the SNA's PU connection to VTAM. • snaLU0EchoAppl <i>sna-hostname</i> [<i>sna-application</i>] [<i>sna-mode</i>]—SNA LU type 0 connection to Cisco's NSPECHO host application that requires the host name defined for the SNA's PU connection to VTAM. Optionally, specify the host application name (the default is NSPECHO) and SNA mode to access the application. • snaLU2EchoAppl <i>sna-hostname</i> [<i>sna-application</i>] [<i>sna-mode</i>]—SNA LU type 2 connection to Cisco's NSPECHO host application that requires the host name defined for the SNA's PU connection to VTAM. Optionally, specify the host application name (the default is NSPECHO) and SNA mode to access the application.
source-ipaddr <i>ip-address</i>	(Optional) Specifies an IP address as the source for the operation.

type ftp

To configure an FTP operation, use the **type ftp** RTR Entry configuration command. To remove the type configuration for the operation, use the **no** form of this command.

```
type ftp operation get url url [source-ipaddr source-ipaddr] [mode { passive | active }]
```

```
no type ftp operation get url url [source-ipaddr source-ipaddr] [mode { passive | active }]
```

Syntax Description		
operation get		Specifies an FTP GET operation. (Support for other FTP operation types may be added in future releases.)
url <i>url</i>		Location information for the file to retrieve.
source-ipaddr <i>source-ipaddr</i>		(Optional) Source address of the operation.
mode		(Optional) Specifies mode, either active or passive.
passive		FTP passive transfer mode. This mode is the default.
active		FTP active transfer mode.

type http

To configure a Hypertext Transfer Protocol (HTTP) SA Agent operation, use the **type http** RTR Entry configuration command. To remove the type configuration for the operation, use the **no** form of this command.

```
type http operation {get | raw} url url [name-server ipaddress] [version version number]
[source-ipaddr {name | ipaddr}] [source-port port number] [cache {enable | disable}]
[proxy proxy-url]
```

```
no type http operation {get | raw} url url [name-server ipaddress] [version version number]
[source-ipaddr {name | ipaddr}] [source-port port number] [cache {enable | disable}]
[proxy proxy-url]
```

Syntax Description		
operation get		Specifies an HTTP GET operation.
operation raw		Specifies an HTTP RAW operation.
url <i>url</i>		Specifies the URL of destination HTTP server.
name-server		(Optional) Specifies name of destination Domain Name Server.
<i>ipaddress</i>		(Optional) IP address of Domain Name Server.
version		(Optional) Specifies version number.
<i>version number</i>		(Optional) Version number.
source-ipaddr		(Optional) Specifies source name or IP address.
<i>name</i>		Source name.
<i>ipaddr</i>		Source IP address.
source-port		(Optional) Specifies source port.
<i>port number</i>		(Optional) Source port number.
cache		(Optional) Enables or disables download of cached HTTP page.
enable		Enables downloads of cached HTTP page.
disable		Disables download of cached HTTP page.
proxy		(Optional) Proxy information.
<i>proxy-url</i>		(Optional) Proxy information or URL.

type jitter

To configure a jitter SA Agent operation, use the **type jitter** RTR Entry configuration command. To disable a jitter operation, use the **no** form of this command.

```
type jitter dest-ipaddr {name | ipaddr} dest-port port-number [source-ipaddr {name | ipaddr}]
  [source-port port-number] [control {enable | disable}] [num-packets number-of-packets]
  [interval inter-packet-interval]
```

```
no type jitter dest-ipaddr {name | ipaddr} dest-port port-number [source-ipaddr {name |
  ipaddr}] [source-port port-number] [control {enable | disable}] [num-packets
  number-of-packets] [interval inter-packet-interval]
```

Syntax Description	
dest-ipaddr	Destination for the operation.
<i>name</i>	Destination IP host name.
<i>ipaddr</i>	Destination IP address.
dest-port	Destination port.
<i>port-number</i>	Port number of the destination port.
source-ipaddr	(Optional) Source IP address.
<i>name</i>	IP host name.
<i>ipaddr</i>	IP address.
source-port	(Optional) Source port.
<i>port-number</i>	Port number of the source.
control	(Optional) Combined with the enable or disable keyword, enables or disables sending a control message to the destination port.
enable	Enables the SA Agent to send a control message to the destination port prior to sending a probe packet. This is the default value.
disable	Disables sending of control messages to the responder prior to sending a probe packet.
num-packets	(Optional) Number of packets, as specified by the number argument.
<i>number-of-packets</i>	The default value is 10.
interval	(Optional) Interpacket interval in milliseconds. The default value of the
<i>inter-packet-interval</i>	<i>inter-packet-interval</i> argument is 20 ms.

type pathEcho

To configure an IP/ICMP Path Echo SA Agent operation, use the **type pathEcho** RTR Entry configuration command. To remove the operation from the configuration, use the **no** form of this command.

```
type pathEcho protocol ipIcmpEcho {ip-address | ip-hostname}
```

```
no type pathEcho protocol ipIcmpEcho {ip-address | ip-hostname}
```

Syntax Description		
protocol ipIcmpEcho		Specifies an IP/ICMP Echo operation. This is currently the only protocol type supported for the SA Agent Path Echo operation.
<i>ip-address</i>		Specifies the IP address of the target device.
<i>ip-hostname</i>		Specifies the designated IP name of the target device.

type tcpConnect

To define a tcpConnect probe, use the **type tcpConnect** RTR Entry configuration command. To remove the type configuration for the probe, use the **no** form of this command.

```
type tcpConnect dest-ipaddr {name | ipaddr} dest-port port-number [source-ipaddr {name | ipaddr} source-port port-number] [control {enable | disable}]
```

```
no type tcpConnect dest-ipaddr {name | ipaddr} dest-port port-number
```

Syntax Description		
dest-ipaddr <i>name</i> <i>ipaddr</i>		Destination of tcpConnect probe. <i>name</i> indicates IP host name. <i>ipaddr</i> indicates IP address.
dest-port <i>port-number</i>		Destination port number.
source-ipaddr <i>name</i> <i>ipaddr</i>		(Optional) Source IP host name or IP address.
source-port <i>port-number</i>		(Optional) Port number of the source. When a port number is not specified, SA Agent picks the best IP address (nearest to the target) and available UDP port.
control		(Optional) Specifies that the SA Agent control protocol should be used when running this probe. The control protocol is required when the probe's target is a Cisco router that does not natively provide the service (TCP service in this case). Combined with the enable or disable keyword, enables or disables sending a control message to the destination port. The default is that the control protocol is enabled. When enabled, the SA Agent sends a control message to the SA Agent Responder (if available) to enable the destination port prior to sending a probe packet.
enable		Enables the SA Agent collector to send a control message to the destination port prior to sending a probe packet.
disable		Disables the SA Agent from sending a control message to the target prior to sending a probe packet.

type udpEcho

To define a udpEcho probe, use the **type udpEcho** RTR Entry configuration command. To remove the type configuration for the probe, use the **no** form of this command.

```
type udpEcho dest-ipaddr {name | ipaddr} dest-port port-number [source-ipaddr {name | ipaddr} source-port port-number] [control {enable | disable}]
```

```
no type udpEcho dest-ipaddr {name | ipaddr} dest-port port-number
```

Syntax Description	dest-ipaddr <i>name ipaddr</i>	Destination of the udpEcho probe. Use an IP host name or IP address.
	dest-port <i>port-number</i>	Destination port number. The range of port numbers is from 1 to 65,535.
	source-ipaddr <i>name ipaddr</i>	(Optional) Source IP host name or IP address.
	source-port <i>port-number</i>	(Optional) Port number of the source. When a port number is not specified, SA Agent picks the best IP address (nearest to the target) and available UDP port
	control	(Optional) Specifies that the SA Agent RTR control protocol should be used when running this probe. The control protocol is required when the probe's target is a Cisco router that does not natively provide the service (UDP service in this case). Combined with the enable or disable keyword, enables or disables sending of a control message to the destination port. The default is that the control protocol is enabled.
	enable	Enable the SA Agent collector to send a control message to the destination port prior to sending a probe packet.
	disable	Disable the SA Agent from sending a control message to the responder prior to sending a probe packet.

verify-data

To cause the SA Agent operation to check each response for corruption, use the **verify-data** RTR Entry configuration command. To return to the default value, use the **no** form of this command.

verify-data

no verify-data

Syntax Description This command has no arguments or keywords.



WCCP Commands

This chapter describes the function and syntax of the commands used to configure Web Cache Communication Protocol Version 1 (WCCPv1) and Version 2 (WCCPv2) on a routing device. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Configuration Fundamentals Command Reference*.

Table 19 lists those commands that have been replaced since Cisco IOS Release 12.0.

Table 19 Replaced WCCP Commands

Command in Cisco IOS Release 12.0:	Replaced by or Integrated into:
<code>ip wccp enable</code>	<code>ip wccp</code>
<code>ip wccp redirect-list</code>	<code>ip wccp</code>
<code>ip web-cache redirect</code>	<code>ip wccp web-cache redirect out</code> (see the <code>ip wccp <service> redirect</code> command)
<code>show ip wccp web-caches</code>	<code>show ip wccp web-cache detail</code> (see the <code>show ip wccp</code> command)



Note

Cisco IOS Release 12.2 allows you to enable either WCCPv1 functionality or WCCPv2 functionality on your router using the `ip wccp version` command. However, you must use the commands introduced with WCCPv2 to configure WCCPv1. The original WCCPv1 configuration commands that have been replaced (see Table 19) will no longer function.

clear ip wccp

To remove Web Cache Communication Protocol (WCCP) statistics (counts) maintained on the router for a particular service, use the `clear ip wccp EXEC` command.

```
clear ip wccp { web-cache | service-number }
```

Syntax Description

<code>web-cache</code>	Directs the router to remove statistics for the web cache service.
<code>service-number</code>	Directs the router to remove statistics for a specified cache service. The number can be from 0 to 99.

ip wccp

To direct a router to enable or disable the support for a cache engine service group, use the **ip wccp** global configuration command. To remove the ability of a router to control support for a service group, use the **no** form of this command.

```
ip wccp { web-cache | service-number } [group-address multicast-address] [redirect-list
access-list] [group-list access-list] [password password]
```

```
no ip wccp { web-cache | service-number } [group-address multicast-address] [redirect-list
access-list] [group-list access-list] [password password]
```

Syntax Description

web-cache	Enables the web cache service.
<i>service-number</i>	Enables the specified Web Cache Communication Protocol (WCCP) service. Services are identified using a number from 0 to 99. If Cisco Cache Engines are being used in your service group, the reverse-proxy service is indicated by a value of 99.
group-address <i>multicast-address</i>	(Optional) Directs the router to use a specified multicast IP address for communication with the WCCP service group. The <i>multicast-address</i> argument requires a multicast address, which is used by the router to determine which cache engine should receive redirected messages.
redirect-list <i>access-list</i>	(Optional) Directs the router to use an access list to control traffic redirected to this service group. The <i>access-list</i> argument should consist of a string of no more than 64 characters (name or number) that specifies the access list.
group-list <i>access-list</i>	(Optional) Directs the router to use an access list to determine which cache engines are allowed to participate in the service group. The <i>access-list</i> argument should consist of a string of no more than 64 characters (name or number) that specifies the access list.
password <i>password</i>	(Optional) Directs the router to apply Message Digest 5 (MD5) authentication to messages received from the service group. Messages that are not accepted by the authentication are discarded. The password can be up to seven characters in length.

ip wccp enable

The **ip wccp enable** has been replaced by the **ip wccp** command. See the description of the **ip wccp** command in this chapter for more information.

ip wccp group-listen

To configure an interface on a router to enable or disable the reception of IP multicast packets for the Web Cache Communication Protocol (WCCP) feature, use the **ip wccp group-listen** interface configuration command. To remove control of the reception of IP multicast packets for the WCCP feature, use the **no** form of this command.

```
ip wccp {web-cache | service-number} group-listen
```

```
no ip wccp {web-cache | service-number} group-listen
```

Syntax	Description
web-cache	Directs the router to send packets to the web cache service.
<i>service-number</i>	The identification number of the cache engine service group being controlled by a router. The number can be from 0 to 99.

ip wccp redirect exclude in

To configure an interface to exclude packets received on an interface from being checked for redirection, use the **ip wccp redirect exclude in** interface configuration command. To disable the ability of a router to exclude packets from redirection checks, use the **no** form of this command.

```
ip wccp redirect exclude in
```

```
no ip wccp redirect exclude in
```

Syntax	Description
	This command has no arguments or keywords.

ip wccp redirect-list

This command is now documented as part of the **ip wccp {web-cache | service-number}** command. See the description of the **ip wccp** command in this chapter for more information.

ip wccp <service> redirect

To enable packet redirection on an outbound or inbound interface using Web Cache Communication Protocol (WCCP), use the **ip wccp service redirect** interface configuration command. To disable WCCP redirection, use the **no** form of this command.

```
ip wccp service redirect {out | in}
```

```
no ip wccp service redirect {out | in}
```

Syntax Description	<i>service</i>	Specifies the service group. You can specify the web-cache keyword, or you can specify the identification number(from 0 to 99) of the service.
	redirect	Enables packet redirection checking on an outbound or inbound interface.
	out	Specifies packet redirection on an outbound interface.
	in	Specifies packet redirection on an inbound interface.

ip wccp version

To specify which version of Web Cache Communication Protocol (WCCP) you want to configure on your router, use the **ip wccp version** global configuration command.

```
ip wccp version {1 | 2}
```

Syntax Description	1	Web Cache Communication Protocol Version 1 (WCCPv1).
	2	Web Cache Communication Protocol Version 2 (WCCPv2).

ip web-cache redirect

The **ip web-cache redirect** interface configuration command has been replaced by the **ip wccp <service> redirect** interface configuration command. The **ip web-cache redirect** command is no longer supported. See the description of the **ip wccp <service> redirect** command in this chapter for more information.

show ip wccp

To display global statistics related to the Web Cache Communication Protocol (WCCP) feature, use the **show ip wccp EXEC** command.

```
show ip wccp {web-cache | service-number} [view | detail]
```

Syntax Description	web-cache	Directs the router to display statistics for the web cache service.
	<i>service-number</i>	The identification number of the cache engine service group being controlled by a router. The number can be from 0 to 99. For cache engine clusters using Cisco Cache Engines, the reverse proxy service is indicated by a value of 99 .
	view	(Optional) Displays which other members of a particular service group have or have not been detected.
	detail	(Optional) Displays information for the router and all cache engines in the currently configured cluster.

show ip wccp web-caches

The **show ip wccp web-caches** command has been replaced by the **show ip wccp web-cache detail** command. See the description of the **show ip wccp** command in this chapter for more information.

■ show ip wccp web-caches



Cisco 7500 Series Line Card Configuration Commands

This chapter describes the function and syntax of the Cisco IOS software commands used to configure characteristics for Cisco 7500 series line cards. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Configuration Fundamentals Command Reference*.

service single-slot-reload-enable

To enable single line card reloading for all line cards in a Cisco 7500 series router, use the **service single-slot-reload-enable** global configuration command. To disable single line card reloading for the line cards, use the **no** form of this command.

service single-slot-reload-enable

no service single-slot-reload-enable

Syntax Description This command has no arguments or keywords.

slave auto-sync config

To turn on automatic synchronization of configuration files for a Cisco 7507 or Cisco 7513 router that is configured for High System Availability (HSA) using Dual RSP Cards, use the **slave auto-sync config** global configuration command. To turn off automatic synchronization, use the **no** form of the command.

slave auto-sync config

no slave auto-sync config

Syntax Description This command has no arguments or keywords.

slave default-slot

To specify the default slave Route Switch Processor (RSP) card on a Cisco 7507 or Cisco 7513 router, use the **slave default-slot** global configuration command.

```
slave default-slot processor-slot-number
```

Syntax Description	<i>processor-slot-number</i>	Number of a processor slot that contains the default slave RSP. On the Cisco 7507 router, valid values are 2 or 3. On the Cisco 7513 router, valid values are 6 or 7. The default is the higher number processor slot.

slave image

To specify the image that the slave Route Switch Processor (RSP) runs on a Cisco 7507 or Cisco 7513 router, use the **slave image** global configuration command.

```
slave image {system | file-url}
```

Syntax Description	system	Loads the slave image that is bundled with the master system image. This is the default.
	<i>file-url</i>	Loads the slave image from the specified file in a Flash file system. If you do not specify a filename, the first file on the specified Flash file system is the default file.

slave reload

To force a reload of the image that the slave Route Switch Processor (RSP) card is running on a Cisco 7507 or Cisco 7513 router, use the **slave reload** global configuration command.

```
slave reload
```

Syntax Description	This command has no arguments or keywords.

slave sync config

To manually synchronize configuration files on the master and slave Route Switch Processor (RSP) cards of a Cisco 7507 or Cisco 7513 router, use the **slave sync config** privileged EXEC command.

```
slave sync config
```

Syntax Description	This command has no arguments or keywords.

slave terminal

To enable access to the slave Route Switch Processor (RSP) console, use the **slave terminal** global configuration command. To disable access to the slave RSP console, use the **no** form of this command.

slave terminal

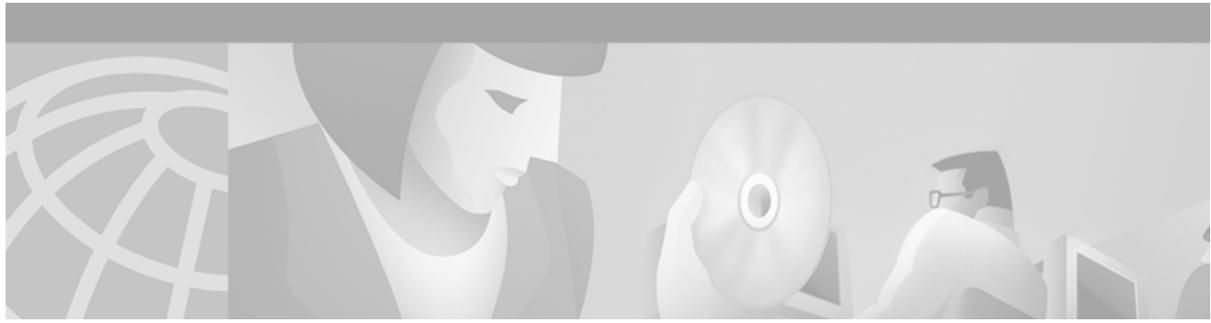
no slave terminal

Syntax Description This command has no arguments or keywords.

■ slave terminal



IP: Addressing and Services



IP Addressing Commands

This chapter describes the function and syntax of the IP addressing commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*.

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		
	<i>ip-address</i>	IP address in four-part dotted decimal format corresponding to the local data-link address.
	<i>hardware-address</i>	Local data-link address (a 48-bit address).
	<i>type</i>	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.

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.

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

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.

clear host

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

clear host {*name* | *}

Syntax Description	<i>name</i>	Particular host entry to remove.
	*	Removes all entries.

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 { * | [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.
inside	(Optional) Clears the inside translations containing the specified <i>global-ip</i> and <i>local-ip</i> addresses.
<i>global-ip</i>	(Optional) When used without the arguments <i>protocol</i> , <i>global-port</i> , and <i>local-port arguments</i> , clears a simple translation that also contains the specified <i>local-ip</i> address. When used with the <i>protocol</i> , <i>global-port</i> , and <i>local-port arguments</i> , clears an extended translation.
<i>local-ip</i>	(Optional) Clears an entry that contains this local IP address and the specified <i>global-ip</i> address.
outside	(Optional) Clears the outside translations containing the specified <i>global-ip</i> and <i>local-ip</i> addresses.
<i>protocol</i>	Clears an entry that contains this protocol and the specified <i>global-ip</i> address, <i>local-ip</i> address, <i>global-port value</i> , and <i>local-port value</i> .
<i>global-port</i>	Clears an entry that contains this <i>global-port value</i> and the specified <i>protocol value</i> , <i>global-ip</i> address, <i>local-ip</i> address, and <i>local-port value</i> .
<i>local-port</i>	Clears an entry that contains this <i>local-port value</i> and the specified <i>protocol value</i> , <i>global-ip</i> address, <i>local-ip</i> address, and <i>global-port value</i> .

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.

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

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		
	<i>ip-address</i>	IP address.
	<i>mask</i>	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.

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		
	<i>ip-address</i>	(Optional) IP broadcast address for a network.

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 <i>seconds</i>	(Optional) Length of time (in 30-second increments) during which the average <i>trigger-threshold</i> and <i>teardown-threshold</i> 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 <i>seconds</i>	(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.	

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.

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.

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*]

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

Syntax Description *access-list-number* (Optional) Number of the access list. If specified, a broadcast must pass the access list to be forwarded.

ip domain-list

To define a list of default domain names to complete unqualified host names, use the **ip domain-list** global configuration command. 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.

ip domain-lookup

To enable the IP Domain Naming System (DNS)-based host name-to-address translation, use the **ip domain-lookup** global configuration command. 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.

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** global configuration command. 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.

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.
<i>port</i>	(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.

ip forward-protocol any-local-broadcast

To forward any broadcasts including local subnet broadcasts, use the **ip forward-protocol any-local-broadcast** global configuration command. To disable this type of forwarding, use the **no** form of this command.

```
ip forward-protocol any-local-broadcast
```

```
no ip forward-protocol any-local-broadcast
```

Syntax Description

This command has no arguments or keywords.

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
```

```
no ip forward-protocol spanning-tree
```

Syntax Description

This command has no arguments or keywords.

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.

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

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 address1*

Syntax Description	<i>name</i>	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.
	<i>tcp-port-number</i>	(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).
	<i>address1</i>	Associated IP address.
	<i>address2...address8</i>	(Optional) Additional associated IP addresses. You can bind up to eight addresses to a host name.

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

<i>host-name</i>	Name of the host.
<i>ip-address</i>	IP address of the host.

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 <i>seconds</i>	(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 <i>seconds</i>	(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 <i>seconds</i>	(Optional) Minimum interval in seconds between advertisements. The range is from 1 to 1800. The default is 450 seconds.
preference <i>number</i>	(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 <i>address [number]</i>	(Optional) IP address (<i>address</i>) to proxy advertise, and optionally, its preference value (<i>number</i>).

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.
<i>keepalive</i>	(Optional) Frequency, in seconds, 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 300 seconds (5 minutes).
<i>hold-time</i>	(Optional) Hold time, in seconds. 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 900 seconds (15 minutes).
access-group	(Optional) Indicates that you are applying an access list. This access list applies only to local-area mobility.
<i>access-list-number</i>	(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.
<i>name</i>	(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.

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

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 }
```

```
no ip nat { inside | outside }
```

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.

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

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 | name } pool name [overload] | static local-ip global-ip }
```

```
no ip nat inside source { list { access-list-number | name } pool name [overload] | static local-ip global-ip }
```

Syntax Description

list <i>access-list-number</i>	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 <i>name</i>	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 <i>name</i>	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 <i>local-ip</i>	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.
<i>global-ip</i>	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.

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 | name} pool name | static global-ip local-ip}
```

```
no ip nat outside source {list {access-list-number | name} pool name | static global-ip local-ip}
```

Syntax Description

list <i>access-list-number</i>	Standard IP access list number. Packets with source addresses that pass the access list are translated using global addresses from the named pool.
list <i>name</i>	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 <i>name</i>	Name of the pool from which global IP addresses are allocated.
static <i>global-ip</i>	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.
<i>local-ip</i>	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, <i>Address Allocation for Private Internets</i>).

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

<i>name</i>	Name of the pool.
<i>start-ip</i>	Starting IP address that defines the range of addresses in the address pool.
<i>end-ip</i>	Ending IP address that defines the range of addresses in the address pool.
netmask <i>netmask</i>	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 <i>prefix-length</i>	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.

ip nat service skinny tcp port

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

```
ip nat service skinny tcp port number
```

```
no ip nat service skinny tcp port number
```

Syntax Description

<i>number</i>	Port number on which the Cisco CallManager is listening for skinny messages.
---------------	--

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] {timeout | udp-timeout | dns-timeout | tcp-timeout | finrst-timeout | icmp-timeout | syn-timeout | port-timeout} seconds
```

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

Syntax Description		
	<i>max-entries</i>	(Optional) Specifies the maximum number of NAT entries.
	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.
	syn-timeout	Specifies the timeout value for TCP flows immediately after a synchronous transmission (SYN) message which consists of digital signals that are sent with precise clocking. The default is 60 seconds.
	port-timeout	Specifies that the timeout value applies to the TCP/UDP port.
	<i>seconds</i>	Number of seconds after which the specified port translation times out. The default is 0.

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 { bitcount | decimal | hexadecimal }
```

```
no ip netmask-format [ bitcount | decimal | hexadecimal ]
```

Syntax Description		
	bitcount	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, 0FFFFFFF00).

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.

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.

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.

ip nhrp map

To statically configure the IP-to-NonBroadcast MultiAccess (NBMA) address mapping of IP destinations connected to an NBMA 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		
	<i>ip-address</i>	IP address of the destinations reachable through the NBMA network. This address is mapped to the NBMA address.
	<i>nbma-address</i>	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.

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

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

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

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

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.
---------------------------	--

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

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.

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		
<i>trigger-threshold</i>		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.
<i>teardown-threshold</i>		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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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

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*]

Syntax Description	<i>type</i>	(Optional) Interface type.
	<i>number</i>	(Optional) Interface number.

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.

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	<i>address</i>	Network address for which a mask is required.
---------------------------	----------------	---

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.

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.
---------------------------	----------------	---

show ip nhrp

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

```
show ip nhrp [dynamic | static] [type number]
```

Syntax Description	dynamic	(Optional) Displays only the dynamic (learned) IP-to-nonbroadcast multiaccess (NBMA) address cache entries.
	static	(Optional) Displays only the static IP-to-NBMA address entries in the cache (configured through the ip nhrp map command).
	type	(Optional) Interface type about which to display the NHRP cache (for example, atm or tunnel).
	number	(Optional) Interface number about which to display the NHRP cache.

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.

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.

tunnel mode

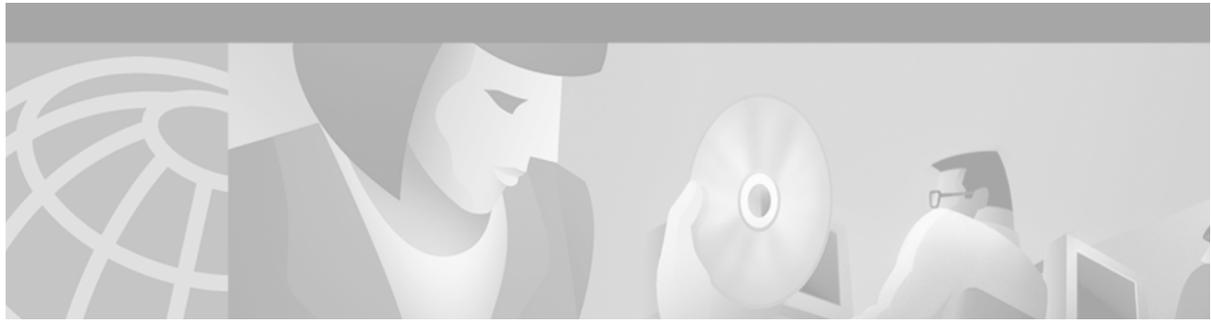
To set the encapsulation mode for the tunnel interface, use the **tunnel mode** interface configuration command. To set to the default, use the **no** form of this command.

tunnel mode { **aurp** | **cayman** | **dvmrp** | **eon** | **gre ip** [**multipoint**] | **ipip** | **nos** }

no tunnel mode

Syntax Description

aurp	AppleTalk Update-Based Routing Protocol (AURP).
cayman	Cayman Tunnel Talk AppleTalk encapsulation.
dvmrp	Distance Vector Multicast Routing Protocol.
eon	EON compatible Connectionless Network Service (CLNS) tunnel.
gre ip	Generic routing encapsulation (GRE) protocol over IP.
multipoint	(Optional) Enables a GRE tunnel to be used in a multipoint fashion. Can be used with the gre ip keyword only, and requires the use of the tunnel key command.
ipip	IP over IP encapsulation.
nos	KA9Q/network operating system (NOS) compatible IP over IP.



DHCP Commands

This chapter describes the function and syntax of the Dynamic Host Configuration Protocol (DHCP) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*.

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	<i>filename</i>	Specifies the name of the file that is used as a boot image.
---------------------------	-----------------	--

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	<i>address</i>	The address of the binding you want to clear.
	*	Clears all automatic bindings.

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

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.

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

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	<i>name</i>	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.
---------------------------	-------------	---

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

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	<i>address</i>	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.
	<i>address2...address8</i>	(Optional) Specifies up to eight addresses in the command line.

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

<i>domain</i>	Specifies the domain name string of the client.
---------------	---

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

<i>hardware-address</i>	Specifies the MAC address of the hardware platform of the client.
<i>type</i>	Indicates the protocol of the hardware platform. Strings and values are acceptable. The string options are: <ul style="list-style-type: none"> • ethernet • ieee802 The value options are: <ul style="list-style-type: none"> • 1 10Mb Ethernet • 6 IEEE 802 If no type is specified, the default protocol is Ethernet.

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		
	<i>address</i>	Specifies the IP address of the client.
	<i>mask</i>	(Optional) Specifies the network mask of the client.
	<i>prefix-length</i>	(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 (/).

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.

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*]

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

Syntax Description		
	<i>client-id</i>	(Optional) Specifies the client identifier. Used to override the MAC address normally created for the client-id string.
	<i>interface-name</i>	(Optional) The interface name from which the MAC address is taken.

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.

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	<i>url</i>	Specifies the remote file used to store the automatic bindings. Following are the acceptable URL file formats: <ul style="list-style-type: none"> • tftp://host/filename • ftp://user:password@host/filename • rcp://user@host/filename
	timeout <i>seconds</i>	(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 <i>seconds</i>	(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.

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

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

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

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

<i>milliseconds</i>	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.
---------------------	---

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

<i>name</i>	Can either be a symbolic string (such as engineering) or an integer (such as 0).
-------------	--

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.

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.

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.

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.

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	<i>days</i>	Specifies the duration of the lease in numbers of days.
	<i>hours</i>	(Optional) Specifies the number of hours in the lease. A <i>days</i> value must be supplied before you can configure an <i>hours</i> value.
	<i>minutes</i>	(Optional) Specifies the number of minutes in the lease. A <i>days</i> value and an <i>hours</i> value must be supplied before you can configure a <i>minutes</i> value.
	infinite	Specifies that the duration of the lease is unlimited.

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	<i>address</i>	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.
	<i>address2...address8</i>	(Optional) Specifies up to eight addresses in the command line.

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	<i>type</i>	Specifies the NetBIOS node type. Valid types are: <ul style="list-style-type: none"> • b-node—Broadcast • p-node—Peer-to-peer • m-node—Mixed • h-node—Hybrid (recommended)
---------------------------	-------------	--

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	<i>network-number</i>	The IP address of the DHCP address pool.
	<i>mask</i>	(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.
	<i>prefix-length</i>	(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 (/).

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

<i>address</i>	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.
<i>address2...address8</i>	(Optional) Specifies up to eight addresses in the command line.

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

<i>code</i>	Specifies the DHCP option code.
<i>instance number</i>	(Optional) Specifies a number from 0 to 255.
<i>ascii string</i>	Specifies an NVT ASCII character string. ASCII character strings that contain white space must be delimited by quotation marks.
<i>hex string</i>	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.
<i>ip address</i>	Specifies an IP address.

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.

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	<i>ip-address</i>	(Optional) Specifies the IP address of the DHCP client for which bindings will be displayed.
---------------------------	-------------------	--

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	<i>ip-address</i>	(Optional) Specifies the IP address of the conflict found.
---------------------------	-------------------	--

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	<i>url</i>	(Optional) Specifies the remote file used to store automatic DHCP bindings. Following are the acceptable URL file formats: <ul style="list-style-type: none"> • tftp://host/filename • ftp://user:password@host/filename • rcp://user@host/filename
---------------------------	------------	--

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.
---------------------------	--

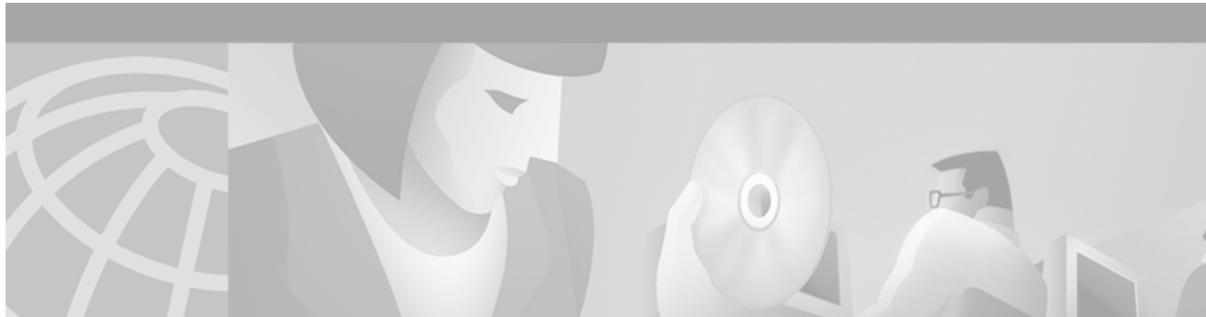
show ip dhcp server statistics

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.

■ show ip dhcp server statistics



IP Services Commands

This chapter describes the function and syntax of the IP services commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*.

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** line configuration command. To remove access restrictions, use the **no** form of this command.

```
access-class access-list-number {in | out}
```

```
no access-class access-list-number {in | out}
```

Syntax Description	
<i>access-list-number</i>	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.
out	Restricts outgoing connections between a particular Cisco device and the addresses in the access list.

access-list (IP extended)

To define an extended IP access list, use the extended version of the **access-list** global configuration command. To remove the access lists, 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]
```

```
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]
```

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]
```

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]
```

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]
```

Syntax Description

<i>access-list-number</i>	Number of an access list. This is a decimal number from 100 to 199 or from 2000 to 2699.
dynamic <i>dynamic-name</i>	(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 <i>Cisco IOS Security Configuration Guide</i> .
timeout <i>minutes</i>	(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 <i>Cisco IOS Security Configuration Guide</i> .
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.

<i>protocol</i>	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 below.
<i>source</i>	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the any keyword as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host source as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>source-wildcard</i>	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: <ul style="list-style-type: none"> • 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 <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host source as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0. <p>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.</p>
<i>destination</i>	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the any keyword as an abbreviation for the <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host destination as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.
<i>destination-wildcard</i>	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: <ul style="list-style-type: none"> • 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 <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host destination as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.
precedence <i>precedence</i>	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7, or by name.

tos <i>tos</i>	(Optional) Packets can be filtered by type of service level, as specified by a number from 0 to 15, or by name.
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.
log-input	(Optional) Includes the input interface and source MAC address or VC in the logging output.
time-range <i>time-range-name</i>	(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.
<i>icmp-type</i>	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
<i>icmp-code</i>	(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.
<i>icmp-message</i>	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name.
<i>igmp-type</i>	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15.
<i>operator</i>	(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 <i>source</i> and <i>source-wildcard</i> , it must match the source port. If the operator is positioned after the <i>destination</i> and <i>destination-wildcard</i> , it must match the destination port. The range operator requires two port numbers. All other operators require one port number.
<i>port</i>	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. 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 bits set. The nonmatching case is that of the initial TCP datagram to form a connection.

access-list (IP standard)

To define a standard IP access list, use the standard version of the **access-list** global configuration command. To remove a standard access lists, 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

<i>access-list-number</i>	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.
<i>source</i>	Number of the network or host from which the packet is being sent. There are two alternative ways to specify the source: <ul style="list-style-type: none"> Use a 32-bit quantity in four-part, dotted-decimal format. Use the any keyword as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.
<i>source-wildcard</i>	(Optional) Wildcard bits to be applied to the source. There are two alternative ways to specify the source wildcard: <ul style="list-style-type: none"> 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 <i>source</i> and <i>source-wildcard</i> 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.

access-list compiled

To enable the Turbo Access Control Lists (Turbo ACL) feature, use the **access-list compiled** global configuration command. 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.

access-list remark

To write a helpful comment (remark) for an entry in a numbered IP access list, use the **access-list remark** global configuration command. 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	<i>access-list-number</i>	Number of an IP access list.
	<i>remark</i>	Comment that describes the access list entry, up to 100 characters long.

clear access-list counters

To clear the counters of an access list, use the **clear access-list counters** EXEC command.

clear access-list counters {*access-list-number* | *access-list-name*}

Syntax Description	<i>access-list-number</i>	Access list number of the access list for which to clear the counters.
	<i>access-list-name</i>	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.

clear ip accounting

To clear the active or checkpointed database when IP accounting is enabled, use the **clear ip accounting** EXEC command.

clear ip accounting [**checkpoint**]

Syntax Description	checkpoint	(Optional) Clears the checkpointed database.
---------------------------	-------------------	--

clear ip drp

To clear all statistics being collected on Director Response Protocol (DRP) requests and replies, use the **clear ip drp** EXEC command.

```
clear ip drp
```

Syntax Description This command has no arguments or keywords.

clear tcp statistics

To clear TCP statistics, use the **clear tcp statistics** privileged EXEC command.

```
clear tcp statistics
```

Syntax Description This command has no arguments or keywords.

deny (IP)

To set conditions for a named IP access list, use the **deny** access-list configuration command. 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]
```

```
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]
```

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]
```

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]
```

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]
```

Syntax Description

<i>source</i>	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the any keyword as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host <i>source</i> as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>source-wildcard</i>	Wildcard bits to be applied to the source. There are three alternative ways to specify the source wildcard: <ul style="list-style-type: none"> • 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 <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host <i>source</i> as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>protocol</i>	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.
<i>destination</i>	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the any keyword as an abbreviation for the <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host <i>destination</i> as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.

<i>destination-wildcard</i>	<p>Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard:</p> <ul style="list-style-type: none"> • 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 <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host <i>destination</i> as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.
precedence <i>precedence</i>	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7 or by name.
tos <i>tos</i>	(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15, or by name.
log	<p>(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.)</p> <p>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.</p>
time-range <i>time-range-name</i>	(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.
<i>icmp-type</i>	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
<i>icmp-code</i>	(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.
<i>icmp-message</i>	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name.
<i>igmp-type</i>	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15.
<i>operator</i>	<p>(Optional) Compares source or destination ports. Possible operands include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).</p> <p>If the operator is positioned after the <i>source</i> and <i>source-wildcard</i>, it must match the source port.</p> <p>If the operator is positioned after the <i>destination</i> and <i>destination-wildcard</i>, it must match the destination port.</p> <p>The range operator requires two port numbers. All other operators require one port number.</p>

<i>port</i>	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. 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.

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]
```

```
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]
```

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]
```

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]
```

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]
```



Caution

Named IP access lists will not be recognized by any software release prior to Cisco IOS Release 11.2.

Syntax Description

<i>dynamic-name</i>	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 <i>Cisco IOS Security Configuration Guide</i> .
timeout <i>minutes</i>	(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 <i>Cisco IOS Security Configuration Guide</i> .
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
<i>protocol</i>	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.
<i>source</i>	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part, dotted decimal format. • Use the any keyword as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host source as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>source-wildcard</i>	Wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard: <ul style="list-style-type: none"> • 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 <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host source as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>destination</i>	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part, dotted decimal format. • Use the any keyword as an abbreviation for the <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host destination as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.

<i>destination-wildcard</i>	<p>Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard:</p> <ul style="list-style-type: none"> • 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 <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host <i>destination</i> as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.
precedence <i>precedence</i>	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7, or by name.
tos <i>tos</i>	(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15, or by name.
log	<p>(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.)</p> <p>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.</p>
<i>icmp-type</i>	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
<i>icmp-code</i>	(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.
<i>icmp-message</i>	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name.
<i>igmp-type</i>	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15.
<i>operator</i>	<p>(Optional) Compares source or destination ports. Possible operands include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).</p> <p>If the operator is positioned after the <i>source</i> and <i>source-wildcard</i>, it must match the source port.</p> <p>If the operator is positioned after the <i>destination</i> and <i>destination-wildcard</i>, it must match the destination port.</p> <p>The range operator requires two port numbers. All other operators require one port number.</p>
<i>port</i>	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. 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.

forwarding-agent

To specify the port on which the Forwarding Agent will listen for wildcard and fixed affinities, use the **forwarding-agent** CASA-port configuration command. To disable listening on that port, use the **no** form of the command.

forwarding-agent *port-number* [*password* [*timeout*]]

no forwarding-agent

Syntax Description		
	<i>port-number</i>	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.
	<i>password</i>	(Optional) Text password used for generating the MD5 digest.
	<i>timeout</i>	(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.

ip access-group

To control access to an interface, use the **ip access-group** interface configuration command. 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		
	<i>access-list-number</i>	Number of an access list. This is a decimal number from 1 to 199 or from 1300 to 2699.
	<i>access-list-name</i>	Name of an IP access list as specified by an ip access-list command.
	in	Filters on inbound packets.
	out	Filters on outbound packets.

ip access-list

To define an IP access list by name, use the **ip access-list** global configuration command. 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.
	<i>access-list-name</i>	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.

ip accounting

To enable IP accounting on an interface, use the **ip accounting** interface configuration command. To disable IP accounting, use the **no** form of this command.

ip accounting [**access-violations**]

no ip accounting [**access-violations**]

Syntax Description	access-violations	(Optional) Enables IP accounting with the ability to identify IP traffic that fails IP access lists.
---------------------------	--------------------------	--

ip accounting-list

To define filters to control the hosts for which IP accounting information is kept, use the **ip accounting-list** global configuration command. 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	<i>ip-address</i>	IP address in dotted decimal format.
	<i>wildcard</i>	Wildcard bits to be applied to the <i>ip-address</i> argument.

ip accounting-threshold

To set the maximum number of accounting entries to be created, use the **ip accounting-threshold** global configuration command. 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	<i>threshold</i>	Maximum number of entries (source and destination address pairs) that the Cisco IOS software accumulates.
---------------------------	------------------	---

ip accounting-transits

To control the number of transit records that are stored in the IP accounting database, use the **ip accounting-transits** global configuration command. 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

<i>count</i>	Number of transit records to store in the IP accounting database.
--------------	---

ip casa

To configure the router to function as a forwarding agent, use the **ip casa** global configuration command. To disable the forwarding agent, use the **no** form of this command.

ip casa *control-address igmp-address*

no ip casa

Syntax Description

<i>control-address</i>	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.
<i>igmp-address</i>	IGMP address 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** global configuration command. 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

<i>access-list-number</i>	Number of a standard IP access list in the range from 1 to 99 or from 1300 to 1999.
---------------------------	---

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** global configuration command. 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	<i>name-of-chain</i>	Name of the key chain containing one or more authentication keys.
---------------------------	----------------------	---

ip drp server

To enable the Director Response Protocol (DRP) Server Agent that works with DistributedDirector, use the **ip drp server** global configuration command. 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.
---------------------------	--

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** global configuration command. 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.
	<i>milliseconds</i>	Time limit (in milliseconds) in which one ICMP destination unreachable message is sent. The range is 1 millisecond to 4294967295 milliseconds.

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** interface configuration command. 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.

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.

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.

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.

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	<i>characters</i>	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.
---------------------------	-------------------	--

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	<i>number</i>	Number of TCP header compression connections the cache supports, in the range from 3 to 1000. The default is 32 connections (16 calls).
---------------------------	---------------	---

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.
---------------------------	----------------	--

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 <i>minutes</i>	(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.

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	<i>packets</i>	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.
---------------------------	----------------	--

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.

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.

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.

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	<i>bytes</i>	Window size (in bytes). The maximum is 65,535 bytes. The default value is 2144 bytes.
---------------------------	--------------	---

ip unreachable

To enable the generation of Internet Control Message Protocol (ICMP) unreachable messages, use the **ip unreachable** interface configuration command. To disable this function, use the **no** form of this command.

ip unreachable

no ip unreachable

Syntax Description	This command has no arguments or keywords.
---------------------------	--

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*]

no permit *protocol source source-wildcard destination destination-wildcard*
[**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*]

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*]

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]
```

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]
```

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]
```

Syntax Description

<i>source</i>	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part, dotted decimal format. • Use the any keyword as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host <i>source</i> as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>source-wildcard</i>	Wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard: <ul style="list-style-type: none"> • 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 <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host <i>source</i> as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>protocol</i>	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.

<i>destination</i>	<p>Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination:</p> <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the any keyword as an abbreviation for the <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host <i>destination</i> as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.
<i>destination-wildcard</i>	<p>Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard:</p> <ul style="list-style-type: none"> • 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 <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host <i>destination</i> as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.
precedence <i>precedence</i>	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7 or by name.
tos <i>tos</i>	(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15, or by name.
log	<p>(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.)</p> <p>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.</p>
time-range <i>time-range-name</i>	(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.
<i>icmp-type</i>	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
<i>icmp-code</i>	(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.
<i>icmp-message</i>	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name.
<i>igmp-type</i>	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15.

<i>operator</i>	<p>(Optional) Compares source or destination ports. Possible operands include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).</p> <p>If the operator is positioned after the <i>source</i> and <i>source-wildcard</i>, it must match the source port.</p> <p>If the operator is positioned after the <i>destination</i> and <i>destination-wildcard</i>, it must match the destination port.</p> <p>The range operator requires two port numbers. All other operators require one port number.</p>
<i>port</i>	<p>(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535.</p> <p>TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.</p>
established	<p>(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.</p>

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	<i>remark</i>	Comment that describes the access list entry, up to 100 characters long.
---------------------------	---------------	--

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	<i>access-list-number</i>	(Optional) Number of the access list to display. The system displays all access lists by default.
	<i>access-list-name</i>	(Optional) Name of the IP access list to display.

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.

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	<i>access-list-number</i>	(Optional) Number of the IP access list to display.
	<i>access-list-name</i>	(Optional) Name of the IP access list to display.

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.

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 <i>ip-address</i>	(Optional) Displays the source address of a given TCP connection.
	detail	(Optional) Displays the detailed statistics.
	daddr <i>ip-address</i>	(Optional) Displays the destination address of a given TCP connection.
	sport <i>source-port</i>	(Optional) Displays the source port of a given TCP connection.
	dport <i>destination-port</i>	(Optional) Displays the destination port of a given TCP connection.
	protocol <i>protocol</i>	(Optional) Displays the protocol of a given TCP connection.

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.

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.

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.

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.

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.

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.

show ip traffic

To display statistics about IP traffic, use the **show ip traffic** EXEC command.

```
show ip traffic
```

Syntax Description This command has no arguments or keywords.

show standby

To display Hot Standby Router Protocol (HSRP) information, use the **show standby** privileged EXEC command.

```
show standby [type number [group]] [active | init | listen | standby] [brief]
```

Syntax Description

<i>type number</i>	(Optional) Interface type and number for which output is displayed.
<i>group</i>	(Optional) Group number on the interface for which output is displayed.
active	(Optional) Displays HSRP groups in the active state.
init	(Optional) Displays HSRP groups in the initial state.
listen	(Optional) Displays HSRP groups in the listen or learn state.
standby	(Optional) Displays HSRP groups in the standby or speak state.
brief	(Optional) A single line of output summarizes each standby group.

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.

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 string
```

```
no standby [group-number] authentication string
```

Syntax Description

<i>group-number</i>	(Optional) Group number on the interface to which this authentication string applies.
<i>string</i>	Authentication string. It can be up to eight characters long. The default string is cisco .

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		
	<i>group-number</i>	(Optional) Group number on the interface for which HSRP is being activated. The default is 0.
	<i>ip-address</i>	(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.

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.ACxy), use the **no** form of this command.

```
standby [group-number] mac-address mac-address
```

```
no standby [group-number] mac-address
```

Syntax Description		
	<i>group-number</i>	(Optional) Group number on the interface for which HSRP is being activated. The default is 0.
	<i>mac-address</i>	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		
	<i>seconds</i>	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.

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	
<i>group-name</i>	Specifies the name of the standby group.

standby preempt

To configure Hot Standby Router Protocol (HSRP) preemption and preemption delay, use the **standby preempt** interface configuration command. To restore the default values, use the **no** form of this command.

standby [*group-number*] **priority** *priority* [**preempt** [**delay** [**minimum** | **sync**] *delay*]]

standby [*group-number*] [**priority** *priority*] **preempt** [**delay** [**minimum** | **sync**] *delay*]

no standby [*group-number*] **priority** *priority* [**preempt** [**delay** [**minimum** | **sync**] *delay*]]

no standby [*group-number*] [**priority** *priority*] **preempt** [**delay** [**minimum** | **sync**] *delay*]

Syntax Description	
<i>group-number</i>	(Optional) Group number on the interface to which the other arguments in this command apply.
priority <i>priority</i>	(Optional) 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.
preempt	(Optional) 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 the preempt keyword is not configured, the local router assumes control as the active router only if it receives information indicating that there is no router currently in the active state (acting as the designated router).
delay minimum <i>delay</i>	(Optional) Time (in seconds). The <i>delay</i> argument causes the local router to postpone taking over the active role for <i>delay</i> (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).
delay sync <i>delay</i>	(Optional) Specifies the maximum synchronization period in <i>delay</i> seconds.

standby priority

To configure Hot Standby Router Protocol (HSRP) priority, use the **standby priority** interface configuration commands. To restore the default values, use the **no** form of this command.

```
standby [group-number] priority priority [preempt [delay [minimum | sync] delay]]
```

```
standby [group-number] [priority priority] preempt [delay [minimum | sync] delay]
```

```
no standby [group-number] priority priority [preempt [delay [minimum | sync] delay]]
```

```
no standby [group-number] [priority priority] preempt [delay [minimum | sync] delay]
```

Syntax Description		
<i>group-number</i>	(Optional) Group number on the interface to which the other arguments in this command apply.	
priority <i>priority</i>	(Optional) 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.	
preempt	(Optional) 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 the preempt keyword is not configured, the local router assumes control as the active router only if it receives information indicating that there is no router currently in the active state (acting as the designated router).	
delay minimum <i>delay</i>	(Optional) Time (in seconds). The <i>delay</i> argument causes the local router to postpone taking over the active role for <i>delay</i> (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).	
delay sync <i>delay</i>	(Optional) Specifies the maximum synchronization period in <i>delay</i> seconds.	

standby redirects

To enable Internet Control Message Protocol (ICMP) redirect messages to be sent when the Hot Standby Router Protocol (HSRP) is configured on an interface, use the **standby redirects** interface configuration command. To disable the HSRP ICMP redirection filter, use the **no** form of this command.

```
standby redirects [enable | disable]
```

```
no standby redirects
```

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.	

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 hellotime holdtime
```

```
no standby [group-number] timers hellotime holdtime
```

Syntax Description		
	<i>group-number</i>	(Optional) Group number on the interface to which the timers apply. The default is 0.
	<i>hellotime</i>	Hello interval (in seconds). This is an integer from 1 to 255. The default is 3 seconds.
	<i>holdtime</i>	Time (in seconds) before the active or standby router is declared to be down. This is an integer from 1 to 255. The default is 10 seconds.

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		
	<i>group-number</i>	(Optional) Group number on the interface to which the tracking applies.
	<i>interface-type</i>	Interface type (combined with interface number) that will be tracked.
	<i>interface-number</i>	Interface number (combined with interface type) that will be tracked.
	<i>interface-priority</i>	(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.

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.
---------------------------	------------------------	---

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	<i>port-number</i>	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.
	<i>password</i>	(Optional) Text password used for generating the MD5 digest.
	<i>timeout</i>	(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.

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	<i>type</i>	Transmit interface type to be linked with the (current) receive-only interface.
	<i>number</i>	Transmit interface number to be linked with the (current) receive-only interface.



Server Load Balancing Commands

This chapter describes the function and syntax of the server load balancing commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*.

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.

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

<i>ip-address</i>	Agent IP address.
<i>port</i>	Agent port number.
<i>timeout</i>	(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.

<i>retry-count</i>	(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.
<i>retry-interval</i>	(Optional) Interval (in seconds) between retries. The default is 180 seconds.

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

<i>bind-id</i>	(Optional) Bind ID number. The default bind ID is 0.
----------------	--

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.
<i>farm-name</i>	(Optional) Character string used to identify the server farm.
vserver	(Optional) Clears the connection database for the virtual server named.
<i>server-name</i>	(Optional) Character string used to identify the virtual server.
counters	Clears the IP IOS SLB counters.

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

<i>ip-address</i>	Client IP address. The default is 0.0.0.0 (all clients).
<i>network-mask</i>	Client IP network mask. The default is 0.0.0.0 (all subnetworks).

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	<i>duration</i>	Delay timer duration in seconds. The valid range is from 1 to 600 seconds. The default value is 10 seconds.
---------------------------	-----------------	---

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.
	<i>number-conns</i>	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.
	<i>number-clients</i>	(Optional) Client connection reassignment threshold value in the range from 1 to 8. The default is 2 client connection failures.

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	<i>duration</i>	Idle connection timer duration (in seconds). Valid values range from 10 to 65535. The default is 3600 seconds (1 hour).
---------------------------	-----------------	---

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.

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.
	<i>group-name</i>	(Optional) Specifies the HSRP group name with which the IOS SLB virtual server is associated.

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.
	<i>password</i>	(Optional) Password value for MD5 authentication. This password must match the password configured on the host agent.
	<i>timeout</i>	(Optional) Delay period (in seconds) during which both the old password and the new password are accepted. The default value is 180 seconds.

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	<i>serverfarm-name</i>	Character string used to identify the server farm. The character string is limited to 15 characters.
---------------------------	------------------------	--

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	<i>virtserver-name</i>	Character string used to identify the virtual server. The character string is limited to 15 characters.
---------------------------	------------------------	---

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	<i>maximum-number</i>	Maximum number of simultaneous active connections on the real server. Valid values range from 1 to 4294967295. The default is 4294967295.
---------------------------	-----------------------	---

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.
--------------------	--------	---

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.

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.
--------------------	------------	-------------------------

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	<p><i>threshold</i></p> <p>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.</p> <p>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.</p> <p>Valid threshold values range from 1 to 4 SYNs. The default value is 3.</p>
---------------------------	---

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	<p><i>retry-value</i></p> <p>Time, in seconds, to wait after the detection of a server failure before a new connection to the server is attempted.</p> <p>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 OUTOFERVICE by the network administrator.</p> <p>Valid values range from 1 to 3600. The default value is 60 seconds.</p> <p>A value of 0 means do not attempt a new connection to the server when it fails.</p>
---------------------------	---

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	<i>serverfarm-name</i>	Name of a server farm that has already been defined using the ip slb serverfarm command.
---------------------------	------------------------	---

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.
	<i>virtserver-name</i>	(Optional) Name of the virtual server to be monitored.
	client	(Optional) Displays only those connections associated with a particular client IP address.
	<i>ip-address</i>	(Optional) IP address of the client to be monitored.
	detail	(Optional) Displays detailed connection information.

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.
	<i>ip-address</i>	(Optional) Agent IP address.
	<i>port-number</i>	(Optional) Agent port number.
	detail	(Optional) Displays all data available.
	weights	(Optional) Displays information about weights assigned to real servers for load balancing.

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.
<i>virtserver-name</i>	(Optional)	Name of the virtual server.
detail	(Optional)	Displays detailed information.

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.
<i>serverfarm-name</i>	(Optional)	Name of the server farm.
detail	(Optional)	Displays detailed server farm information.

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.

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.
<i>ip-address</i>	(Optional)	IP address of the client.

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.
<i>virtserver-name</i>	(Optional) Name of the virtual server.
detail	(Optional) Displays detailed virtual server information.

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

<i>duration</i>	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.
<i>group-id</i>	(Optional) Number identifying the sticky group to which the virtual server belongs. Valid values range from 0 to 255.

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

<i>syn-count</i>	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.
<i>interval</i>	(Optional) Interval (in milliseconds) for SYN threshold monitoring. Valid values range from 50 to 5000. The default is 100 ms.

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	
<i>ip-address</i>	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.
<i>port-number</i>	<p>(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 <i>port-number</i> argument are as follows:</p> <ul style="list-style-type: none"> • 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 <p>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).</p>
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.
<i>service-name</i>	(Optional) Type of connection coupling. Currently, the only choice is ftp . Couple FTP data connections with the control session that created them.

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.



Mobile IP Commands

This chapter describes the function and syntax of the Mobile IP commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*.

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 {tacacs+ | radius}
```

```
no aaa authorization ipmobile {tacacs+ | radius}
```

Syntax Description

tacacs+	Specifies TACACS+.
radius	Specifies RADIUS.

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.
<i>standby-group-name</i>	(Optional) Name of the standby group.
<i>ip-address</i>	(Optional) IP address of a mobile node.

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.
	<i>lower</i>	IP address of mobile node. Can be used alone, or as lower end of a range of addresses.
	<i>upper</i>	(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.

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.
--------------------	------	---

clear ip mobile visitor

To remove visitor information, use the **clear ip mobile visitor** EXEC command.

```
clear ip mobile visitor [ip-address]
```

Syntax Description	<i>ip-address</i>	(Optional) IP address. If not specified, visitor information will be removed for all addresses.
--------------------	-------------------	---

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 <i>interface</i>	(Optional) IP address of the interface. Sets the care-of address on the foreign agent. Multiple care-of addresses can be configured.	
reg-wait <i>seconds</i>	(Optional) Pending registration expires after the specified number of seconds if no reply is received. Range is from 5 to 600. Default is 15.	

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 <i>acl</i>	(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.	
limit <i>number</i>	(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.	
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.	

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 [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		
broadcast	(Optional) Enables broadcast datagram routing. By default, broadcasting is disabled.	
care-of-access <i>acl</i>	(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 <i>number</i>	(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 <i>seconds</i>	(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 <i>acl</i>	(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.

ip mobile home-agent address

To define a global home agent address on a different subnet for virtual networks, use the **ip mobile home-agent address** global configuration command. To remove the address, use the **no** form of this command.

ip mobile home-agent address *address*

no ip mobile home-agent address *address*

Syntax Description

<i>address</i>	Home agent address.
----------------	---------------------

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

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

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

<i>lower</i> [<i>upper</i>]	Range of mobile host or mobile node group IP addresses.
interface <i>name</i>	Mobile node that belongs to the specified interface.
virtual-network <i>net mask</i>	The wireless mobile node resides in the virtual network created using the ip mobile virtual-network command.
aaa	(Optional) Retrieves security associations from a AAA (TACACS+ or RADIUS) server.
load-sa	(Optional) Stores security associations in memory after retrieval.
care-of-access <i>acl</i>	(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 <i>number</i>	(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.

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.

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

<i>seconds</i>	Lifetime in seconds. Range is from 3 to 65535 (infinity).
----------------	---

ip mobile secure

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

```
ip mobile secure { host | visitor | home-agent | foreign-agent } address { inbound-spi spi-in
outbound-spi spi-out | spi spi } key hex string [replay timestamp [number] algorithm md5
mode prefix-suffix]
```

```
no ip mobile secure { host | visitor | home-agent | foreign-agent } address { inbound-spi spi-in
outbound-spi spi-out | spi spi } key hex string [replay timestamp [num] algorithm md5
mode prefix-suffix]
```

Syntax Description

host	Security association of the mobile host on the home agent.
visitor	Security association of the mobile host on the foreign agent.
home-agent	Security association of the remote home agent on the foreign agent.
foreign-agent	Security association of the remote foreign agent on the home agent.
<i>address</i>	IP address of host, visitor or mobility agent.
inbound-spi <i>spi-in</i>	Security parameter index used for authenticating inbound registration packets. Range is from 0x100 to 0xffffffff.
outbound-spi <i>spi-out</i>	Security parameter index used for calculating the authenticator in outbound registration packets. Range is from 0x100 to 0xffffffff.
spi <i>spi</i>	Bidirectional SPI. Range is from 0x100 to 0xffffffff.
key <i>hex string</i>	ASCII string of hexadecimal values. No spaces are allowed.
replay	(Optional) Replay protection used on registration packets.
timestamp	(Optional) Used to validate incoming packets to ensure that they are not being “replayed” by a spoofer using timestamp method.
<i>number</i>	(Optional) Number of seconds. Registration is valid if received within the specified time. This means the sender and receiver are in time synchronization (NTP can be used).
algorithm	(Optional) Algorithm used to authenticate messages during registration.
md5	(Optional) Message Digest 5.
mode	(Optional) Mode used to authenticate during registration.
prefix-suffix	(Optional) The key is used to wrap the registration information for authentication (for example, key registration information key) to calculate the message digest.

ip mobile tunnel

To specify the settings of tunnels created by Mobile IP, use the **ip mobile tunnel** interface configuration command.

```
ip mobile tunnel { route-cache | path-mtu-discovery [age-timer { minutes | infinite } ] }
```

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 <i>minutes</i>		(Optional) Time interval in minutes after which the tunnel reestimates the path MTU.
infinite		(Optional) Turns off the age timer.

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 [address address]
```

Syntax Description		
<i>net</i>		Network associated with the IP address of the virtual network.
<i>mask</i>		Mask associated with the IP address of the virtual network.
address <i>address</i>		(Optional) IP address of a home agent on a virtual network.

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.

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 <i>address</i>		(Optional) IP address of mobile node.
summary		(Optional) Total number of bindings in the table.

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.

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	<i>address</i>	(Optional) IP address of specific mobile node. If not specified, information for all mobile nodes is displayed.
	interface <i>interface</i>	(Optional) All mobile nodes whose home network is on this interface.
	network <i>address</i>	(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.

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	<i>interface</i>	(Optional) IP address of mobile node. If not specified, all interfaces are shown.
---------------------------	------------------	---

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.
<i>address</i>	IP address.

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.

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.

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.

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.

■ show ip mobile visitor



IP: Routing Protocols



On-Demand Routing Commands

This chapter describes the function and syntax of the On-Demand Routing (ODR) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*.

router odr

To configure a router to accept On-Demand Routing (ODR) routes from a stub routers, use the **router odr** global configuration command. To disable ODR, use the **no** form of this command.

router odr

no router odr

Syntax Description This command has no arguments or keywords.

timers basic (ODR)

To adjust ODR network timers, use the **timers basic** router configuration command. To restore the default timers, use the **no** form of this command.

timers basic *update invalid holddown flush [sleeptime]*

no timers basic

Syntax Description	<i>update</i>	Rate (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol.
	<i>invalid</i>	Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the <i>update</i> argument. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters holddown. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets.

<i>holddown</i>	Interval (in seconds) during which routing information regarding better paths is suppressed. It should be at least three times the value of the <i>update</i> argument. A route enters into a <i>holddown</i> state when an update packet is received that indicates the route is unreachable. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. When <i>holddown</i> expires, routes advertised by other sources are accepted and the route is no longer inaccessible.
<i>flush</i>	Amount of time (in seconds) that must pass before the route is removed from the routing table; the interval specified must be at least the sum of the <i>invalid</i> and <i>holddown</i> arguments. If it is less than this sum, the proper holddown interval cannot elapse, which results in a new route being accepted before the holddown interval expires.
<i>sleeptime</i>	(Optional) Interval (in milliseconds) for postponing routing updates in the event of a flash update. The <i>sleeptime</i> value should be less than the <i>update</i> time. If the <i>sleeptime</i> is greater than the <i>update</i> time, routing tables will become unsynchronized.



RIP Commands

This chapter describes the function and syntax of the Routing Information Protocol (RIP) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*.

auto-summary (RIP)

To restore the default behavior of automatic summarization of subnet routes into network-level routes, use the **auto-summary** router configuration command. To disable this function and send subprefix routing information across classful network boundaries, use the **no** form of this command.

auto-summary

no auto-summary

Syntax Description This command has no arguments or keywords.

default-information originate

To generate a default route into Routing Information Protocol (RIP), use the **default-information originate** router configuration command. To disable this feature, use the **no** form of this command.

default-information originate [**route-map** *map-name*]

no default-information originate

Syntax Description **route-map** *map-name* (Optional) Routing process will generate the default route if the route map is satisfied.

default-metric (RIP)

To set default metric values for Routing Information Protocol (RIP), use the **default-metric** router configuration command. To return to the default state, use the **no** form of this command.

default-metric *number-value*

no default-metric [*number-value*]

Syntax Description	<i>number-value</i>	Default metric value.
--------------------	---------------------	-----------------------

input-queue

To adjust the depth of the Routing Information Protocol (RIP) input queue, use the **input-queue** router configuration command. To remove the configured depth and restore the default depth, use the **no** form of this command.

input-queue *depth*

no input-queue [*depth*]

Syntax Description	<i>depth</i>	Numerical value associated with the depth of the RIP input queue. The larger the numerical value, the larger the depth of the queue. The range is from 0 to 1024.
--------------------	--------------	---

ip rip authentication key-chain

To enable authentication for Routing Information Protocol (RIP) Version 2 packets and to specify the set of keys that can be used on an interface, use the **ip rip authentication key-chain** interface configuration command. To prevent authentication, use the **no** form of this command.

ip rip authentication key-chain *name-of-chain*

no ip rip authentication key-chain [*name-of-chain*]

Syntax Description	<i>name-of-chain</i>	Enables authentication and specifies the group of keys that are valid.
--------------------	----------------------	--

ip rip authentication mode

To specify the type of authentication used in Routing Information Protocol (RIP) Version 2 packets, use the **ip rip authentication mode** interface configuration command. To restore clear text authentication, use the **no** form of this command.

```
ip rip authentication mode {text | md5}
```

```
no ip rip authentication mode
```

Syntax Description

text	Clear text authentication.
md5	Keyed Message Digest 5 (MD5) authentication.

ip rip receive version

To specify a Routing Information Protocol (RIP) version to receive on an interface basis, use the **ip rip receive version** interface configuration command. To follow the global version rules, use the **no** form of this command.

```
ip rip receive version [1] [2]
```

```
no ip rip receive version
```

Syntax Description

1	(Optional) Accepts only RIP Version 1 packets on the interface.
2	(Optional) Accepts only RIP Version 2 packets on the interface.

ip rip send version

To specify a Routing Information Protocol (RIP) version to send on an interface basis, use the **ip rip send version** interface configuration command. To follow the global version rules, use the **no** form of this command.

```
ip rip send version [1] [2]
```

```
no ip rip send version
```

Syntax Description

1	(Optional) Sends only RIP Version 1 packets out the interface.
2	(Optional) Sends only RIP Version 2 packets out the interface.

ip rip triggered

To enable triggered extensions to Routing Information Protocol (RIP), use the **ip rip triggered** interface configuration command. To disable triggered extensions to RIP, use the **no** form of this command.

ip rip triggered

no ip rip triggered

Syntax Description This command has no arguments or keywords.

ip split-horizon (RIP)

To enable the split horizon mechanism, use the **ip split-horizon** interface configuration command. To disable the split horizon mechanism, use the **no** form of this command.

ip split-horizon

no ip split-horizon

Syntax Description This command has no arguments or keywords.

ip summary-address rip

To configure a Cisco router running Routing Information Protocol (RIP) to advertise a summarized local IP address pool on a network access server so that the address pool can be provided to dialup clients and specify the IP address and network mask that identify the routes to be summarized, use the **ip summary-address rip** router configuration command. To disable the split horizon mechanism, use the **no** form of this command.

ip summary-address rip *ip-address ip-network-mask*

no ip summary-address rip *ip-address ip-network-mask*

Syntax Description	<i>ip-address</i>	IP address to be summarized.
	<i>ip-network-mask</i>	IP network mask that drives route summarization for the specified IP address.

neighbor (RIP)

To define a neighboring router with which to exchange routing information, use the **neighbor** router configuration command. To remove an entry, use the **no** form of this command.

neighbor *ip-address*

no neighbor *ip-address*

Syntax Description	<i>ip-address</i>	IP address of a peer router with which routing information will be exchanged.
---------------------------	-------------------	---

network (RIP)

To specify a list of networks for the Routing Information Protocol (RIP) routing process, use the **network** router configuration command. To remove an entry, use the **no** form of this command.

network *ip-address*

no network *ip-address*

Syntax Description	<i>ip-address</i>	IP address of the network of directly connected networks.
---------------------------	-------------------	---

offset-list

To add an offset to incoming and outgoing metrics to routes learned via Routing Information Protocol (RIP), use the **offset-list** router configuration command. To remove an offset list, use the **no** form of this command.

offset-list {*access-list-number* | *access-list-name*} {**in** | **out**} *offset* [*interface-type* *interface-number*]

no offset-list {*access-list-number* | *access-list-name*} {**in** | **out**} *offset* [*interface-type* *interface-number*]

Syntax Description	<i>access-list-number</i>	Standard access list number to be applied. Access list number 0 indicates all access lists. If <i>offset</i> is 0, no action is taken. For IGRP, the offset is added to the delay component only.
	<i>access-list-name</i>	Standard access list name to be applied.
	in	Applies the access list to incoming metrics.
	out	Applies the access list to outgoing metrics.
	<i>offset</i>	Positive offset to be applied to metrics for networks matching the access list. If the offset is 0, no action is taken.
	<i>interface-type</i>	(Optional) Interface type to which the offset list is applied.
	<i>interface-number</i>	(Optional) Interface number to which the offset list is applied.

output-delay

To change the interpacket delay for Routing Information Protocol (RIP) updates sent, use the **output-delay** router configuration command. To remove the delay, use the **no** form of this command.

output-delay *delay*

no output-delay [*delay*]

Syntax Description

<i>delay</i>	Delay (in milliseconds) between packets in a multiple-packet RIP update. The range is from 8 to 50 milliseconds. The default is no delay.
--------------	---

router rip

To configure the Routing Information Protocol (RIP) routing process, use the **router rip** global configuration command. To turn off the RIP routing process, use the **no** form of this command.

router rip

no router rip

Syntax Description

This command has no arguments or keywords.

show ip rip database

To display summary address entries in the Routing Information Protocol (RIP) routing database entries if relevant are routes being summarized based upon a summary address, use the **show ip rip database EXEC** command.

show ip rip database

Syntax Description

This command has no arguments or keywords.

timers basic

To adjust Routing Information Protocol (RIP) network timers, use the **timers basic** router configuration command. To restore the default timers, use the **no** form of this command.

timers basic *update invalid holddown flush*

no timers basic

Syntax Description

<i>update</i>	Rate (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol. The default is 30 seconds.
<i>invalid</i>	Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the <i>update</i> argument. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters into a <i>holddown</i> state. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. The default is 180 seconds.
<i>holddown</i>	Interval (in seconds) during which routing information regarding better paths is suppressed. It should be at least three times the value of the <i>update</i> argument. A route enters into a <i>holddown</i> state when an update packet is received that indicates the route is unreachable. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. When holddown expires, routes advertised by other sources are accepted and the route is no longer inaccessible. The default is 180 seconds.
<i>flush</i>	Amount of time (in seconds) that must pass before the route is removed from the routing table; the interval specified should be greater than the value of the <i>invalid</i> argument. If it is less than this sum, the proper <i>holddown</i> interval cannot elapse, which results in a new route being accepted before the <i>holddown</i> interval expires. The default is 240 seconds.

validate-update-source

To have the Cisco IOS software validate the source IP address of incoming routing updates for Routing Information Protocol (RIP) and Interior Gateway Routing Protocol (IGRP) routing protocols, use the **validate-update-source** router configuration command. To disable this function, use the **no** form of this command.

validate-update-source

no validate-update-source

Syntax Description

This command has no arguments or keywords.

version

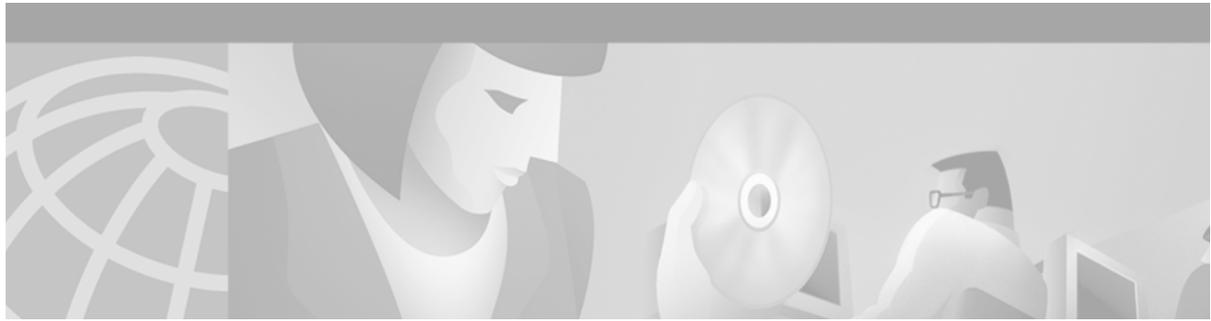
To specify a Routing Information Protocol (RIP) version used globally by the router, use the **version** router configuration command. To restore the default value, use the **no** form of this command.

version {1 | 2}

no version

Syntax Description

1	Specifies RIP Version 1.
2	Specifies RIP Version 2.



IGRP Commands

This chapter describes the function and syntax of the Interior Gateway Routing Protocol (IGRP) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*.

ip split-horizon (IGRP)

To enable the split horizon mechanism, use the **ip split-horizon** interface configuration command. To disable the split horizon mechanism, use the **no** form of this command.

ip split-horizon

no ip split-horizon

Syntax Description This command has no arguments or keywords.

metric holddown

To keep new Interior Gateway Routing Protocol (IGRP) routing information from being used for a certain period of time, use the **metric holddown** router configuration command. To disable this feature, use the **no** form of this command.

metric holddown

no metric holddown

Syntax Description This command has no arguments or keywords.

metric maximum-hops

To have the IP routing software advertise as unreachable those routes with a hop count higher than is specified by the command (Interior Gateway Routing Protocol [IGRP] only), use the **metric maximum-hops** router configuration command. To reset the value to the default, use the **no** form of this command.

metric maximum-hops *{hops-number}*

no metric maximum-hops *{hops-number}*

Syntax Description	<i>hops-number</i>	Maximum hop count (in decimal). The default value is 100 hops; the maximum number of hops that can be specified is 255.
---------------------------	--------------------	---

neighbor (IGRP)

To define a neighboring router with which to exchange routing information, use the **neighbor** router configuration command. To remove an entry, use the **no** form of this command.

neighbor *ip-address*

no neighbor *ip-address*

Syntax Description	<i>ip-address</i>	IP address of a peer router with which routing information will be exchanged.
---------------------------	-------------------	---

network (IGRP)

To specify a list of networks for the Enhanced Interior Gateway Routing Protocol (IGRP) routing process, use the **network** router configuration command. To remove an entry, use the **no** form of this command.

network *network-number*

no network *network-number*

Syntax Description	<i>network-number</i>	IP address of the directly connected networks.
---------------------------	-----------------------	--

offset-list (IGRP)

To add an offset to incoming and outgoing metrics to routes learned via Interior Gateway Routing Protocol (IGRP), use the **offset-list** router configuration command. To remove an offset list, use the **no** form of this command.

```
offset-list { access-list-number | access-list-name } { in | out } offset [interface-type
interface-number]
```

```
no offset-list { access-list-number | access-list-name } { in | out } offset [interface-type
interface-number]
```

Syntax Description	
<i>access-list-number</i>	Standard access list number to be applied. Access list number 0 indicates all access lists. If the <i>offset</i> argument is 0, no action is taken. For IGRP, the offset is added to the delay component only.
<i>access-list-name</i>	Standard access name to be applied.
in	Applies the access list to incoming metrics.
out	Applies the access list to outgoing metrics.
<i>offset</i>	Positive offset to be applied to metrics for networks matching the access list. If the offset is 0, no action is taken.
<i>interface-type</i>	(Optional) Interface type to which the offset list is applied.
<i>interface-number</i>	(Optional) Interface number to which the offset list is applied.

router igrp

To configure the Interior Gateway Routing Protocol (IGRP) routing process, use the **router igrp** global configuration command. To shut down an IGRP routing process, use the **no** form of this command.

```
router igrp as-number
```

```
no router igrp as-number
```

Syntax Description	
<i>as-number</i>	Autonomous system number that identifies the routes to the other IGRP routers. It is also used to tag the routing information.

set metric (IGRP)

To set the metric value for Interior Gateway Routing Protocol (IGRP) in a route map, use the **set metric** route-map configuration command. To return to the default metric value, use the **no** form of this command.

```
set metric bandwidth delay reliability loading mtu
```

```
no set metric bandwidth delay reliability loading mtu
```

Syntax Description		
<i>bandwidth</i>		Metric value or IGRP bandwidth of the route, in kbps. It can be in the range from 0 to 4294967295.
<i>delay</i>		Route delay (in tens of microseconds). It can be in the range from 0 to 4294967295.
<i>reliability</i>		Likelihood of successful packet transmission expressed as a number from 0 to 255. The value 255 means 100 percent reliability; 0 means no reliability.
<i>loading</i>		Effective bandwidth of the route expressed as a number from 0 to 255 (255 is 100 percent loading).
<i>mtu</i>		Minimum maximum transmission unit (MTU) size of the route, in bytes. It can be in the range from 0 to 4294967295.

timers basic (IGRP)

To adjust Interior Gateway Routing Protocol (IGRP) network timers, use the **timers basic** router configuration command. To restore the default timers, use the **no** form of this command.

```
timers basic update invalid holddown flush [sleeptime]
```

```
no timers basic
```

Syntax Description		
<i>update</i>		Rate (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol. The default is 90 seconds.
<i>invalid</i>		Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the <i>update</i> argument. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters <i>holddown</i> state. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. The default is 270 seconds.
<i>holddown</i>		Interval (in seconds) during which routing information regarding better paths is suppressed. It should be at least three times the value of the <i>update</i> argument. A route enters into a hold-down state when an update packet is received that indicates the route is unreachable. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. When <i>holddown</i> expires, routes advertised by other sources are accepted and the route is no longer inaccessible. The default is 280 seconds.
<i>flush</i>		Amount of time (in seconds) that must pass before the route is removed from the routing table; the interval specified must be at least the sum of the <i>invalid</i> argument and the <i>holddown</i> argument. If it is less than this sum, the proper <i>holddown</i> interval cannot elapse, which results in a new route being accepted before the <i>holddown</i> interval expires. The default is 630 seconds.
<i>sleeptime</i>		(Optional) Interval (in milliseconds) for postponing routing updates in the event of a flash update. The value of the <i>sleeptime</i> argument should be less than the <i>update</i> value. If the <i>sleeptime</i> value is greater than the <i>update</i> value, routing tables will become unsynchronized. The default is 0 milliseconds.

traffic-share balanced

To balance traffic distribution among routes when there are multiple routes for the same destination network that have different costs, use the **traffic-share balanced** router configuration command. To disable this function, use the **no** form of the command.

traffic-share balanced

no traffic-share balanced

Syntax Description

This command has no arguments or keywords.

■ traffic-share balanced



OSPF Commands

This chapter describes the function and syntax of the Open Shortest Path First (OSPF) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*.

area authentication

To enable authentication for an OSPF area, use the **area authentication** router configuration command. To remove an authentication specification of an area or a specified area from the configuration, use the **no** form of this command.

area *area-id* **authentication** [**message-digest**]

no area *area-id* **authentication** [**message-digest**]

Syntax Description	<i>area-id</i>	Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address.
	message-digest	(Optional) Enables Message Digest 5 (MD5) authentication on the area specified by the <i>area-id</i> argument.

area default-cost

To specify a cost for the default summary route sent into a stub or not so stubby area (NSSA), use the **area default-cost** router configuration command. To remove the assigned default route cost, use the **no** form of this command.

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost** *cost*

Syntax Description	<i>area-id</i>	Identifier for the stub or NSSA. The identifier can be specified as either a decimal value or as an IP address.
	<i>cost</i>	Cost for the default summary route used for a stub or NSSA. The acceptable value is a 24-bit number.

area filter-list

To filter prefixes advertised in type 3 link-state advertisements (LSAs) between Open Shortest Path First (OSPF) areas of an area border router (ABR), use the **area filter-list** command. To change or cancel the filter, use the no form of this command.

```
area {area-id} filter-list prefix {prefix-list-name in | out}
```

```
no area {area-id} filter-list prefix {prefix-list-name in | out}
```

Syntax Description

<i>area-id</i>	Identifier of the area for which filtering is configured. The identifier can be specified as either a decimal value or an IP address.
prefix	Indicates that a prefix list is used.
<i>prefix-list-name</i>	Name of a prefix list.
in	Prefix list applied to prefixes advertised to the specified area from other areas.
out	Prefix list applied to prefixes advertised out of the specified area to other areas.

area nssa

To configure an area as a not-so-stubby area (NSSA), use the **area nssa** router configuration command. To remove the NSSA distinction from the area, use the **no** form of this command.

```
area area-id nssa [no-redistribution] [default-information-originate]
```

```
no area area-id nssa [no-redistribution] [default-information-originate]
```

Syntax Description

<i>area-id</i>	Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address.
no-redistribution	(Optional) Used when the router is an NSSA Area Border Router (ABR) and you want the redistribute command to import routes only into the normal areas, but not into the NSSA area.
default-information-originate	(Optional) Used to generate a Type 7 default into the NSSA area. This keyword only takes effect on NSSA ABR or NSSA Autonomous System Boundary Router (ASBR).

area range

To consolidate and summarize routes at an area boundary, use the **area range** router configuration command. To disable this function, use the **no** form of this command.

```
area area-id range ip-address mask [advertise | not-advertise]
```

```
no area area-id range ip-address mask [advertise | not-advertise]
```

Syntax Description		
	<i>area-id</i>	Identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IP address.
	<i>ip-address</i>	IP address.
	<i>mask</i>	IP address mask.
	advertise	(Optional) Sets the address range status to advertise and generates a Type 3 summary link-state advertisements (LSA).
	not-advertise	(Optional) Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.

area stub

To define an area as a stub area, use the **area stub** router configuration command. To disable this function, use the **no** form of this command.

```
area area-id stub [no-summary]
```

```
no area area-id stub [no-summary]
```

Syntax Description		
	<i>area-id</i>	Identifier for the stub area; either a decimal value or an IP address.
	no-summary	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.

area virtual-link

To define an OSPF virtual link, use the **area virtual-link** router configuration command with the optional parameters. To remove a virtual link, use the **no** form of this command.

```
area area-id virtual-link router-id [authentication [message-digest | null]] [hello-interval seconds] [retransmit-interval seconds] [transmit-delay seconds] [dead-interval seconds] [[authentication-key key] | [message-digest-key key-id md5 key]]
```

```
no area area-id virtual-link router-id [authentication [message-digest | null]] [hello-interval seconds] [retransmit-interval seconds] [transmit-delay seconds] [dead-interval seconds] [[authentication-key key] | [message-digest-key key-id md5 key]]
```

```
no area area-id
```

Syntax Description		
	<i>area-id</i>	Area ID assigned to the transit area for the virtual link. This can be either a decimal value or a valid IP address. There is no default.
	<i>router-id</i>	Router ID associated with the virtual link neighbor. The router ID appears in the show ip ospf display. The router ID is internally derived by each router from the interface IP addresses. This value must be entered in the format of an IP address. There is no default.
	authentication	(Optional) Specifies authentication type.

message-digest	(Optional) Specifies that message-digest authentication is used.
null	(Optional) No authentication is used. Overrides password or message-digest authentication if configured for the area.
hello-interval <i>seconds</i>	(Optional) Time (in seconds) between the hello packets that the Cisco IOS software sends on an interface. Unsigned integer value to be advertised in the hello packets. The value must be the same for all routers and access servers attached to a common network. The default is 10 seconds.
retransmit-interval <i>seconds</i>	(Optional) Time (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. Expected round-trip delay between any two routers on the attached network. The value must be greater than the expected round-trip delay. The default is 5 seconds.
transmit-delay <i>seconds</i>	(Optional) Estimated time (in seconds) it takes to send a link-state update packet on the interface. Integer value that must be greater than zero. LSAs in the update packet have their age incremented by this amount before transmission. The default value is 1 second.
dead-interval <i>seconds</i>	(Optional) Time (in seconds) that hello packets are not seen before a neighbor declares the router down. Unsigned integer value. The default is four times the hello interval, or 40 seconds. As with the hello interval, this value must be the same for all routers and access servers attached to a common network.
authentication-key <i>key</i>	(Optional) Password to be used by neighboring routers. It is any continuous string of characters that you can enter from the keyboard up to 8 bytes long. This string acts as a key that will allow the authentication procedure to generate or verify the authentication field in the OSPF header. This key is inserted directly into the OSPF header when originating routing protocol packets. A separate password can be assigned to each network on a per-interface basis. All neighboring routers on the same network must have the same password to be able to route OSPF traffic. The password is encrypted in the configuration file if the service password-encryption command is enabled. There is no default value.
message-digest-key <i>key-id</i> md5 <i>key</i>	(Optional) Key identifier and password to be used by neighboring routers and this router for Message Digest 5 (MD5) authentication. The <i>keyid</i> argument is a number in the range from 1 to 255. The <i>key</i> is an alphanumeric string of up to 16 characters. All neighboring routers on the same network must have the same key identifier and key to be able to route OSPF traffic. There is no default value.

auto-cost

To control how OSPF calculates default metrics for the interface, use the **auto-cost** router configuration command. To assign cost based only on the interface type, use the **no** form of this command.

auto-cost reference-bandwidth *ref-bw*

no auto-cost reference-bandwidth

Syntax Description	reference-bandwidth <i>ref-bw</i> Rate in Mbps (bandwidth). The range is from 1 to 4294967; the default is 100.
---------------------------	--

clear ip ospf

To clear redistribution based on the OSPF routing process ID, use the **clear ip ospf EXEC** command.

clear ip ospf [*pid*] {**process** | **redistribution** | **counters** [**neighbor** [*neighbor-interface*]
[*neighbor-id*]]}

Syntax Description	<i>pid</i> (Optional) Process ID.
	process Reset OSPF process.
	redistribution Clear OSPF route redistribution.
	counters OSPF counters.
	neighbor Neighbor statistics per interface.
	<i>neighbor-interface</i> Neighbor interface.
	<i>neighbor-id</i> Neighbor ID.

compatible rfc1583

To restore the method used to calculate summary route costs per RFC 1583, use the **compatible rfc1583** router configuration command. To disable RFC 1583 compatibility, use the **no** form of this command.

compatible rfc1583

no compatible rfc1583

Syntax Description	This command has no arguments or keywords.
---------------------------	--

default-information originate (OSPF)

To generate a default external route into an OSPF routing domain, use the **default-information originate** router configuration command. To disable this feature, use the **no** form of this command.

```
default-information originate [always] [metric metric-value] [metric-type type-value]
[route-map map-name]
```

```
no default-information originate [always] [metric metric-value] [metric-type type-value]
[route-map map-name]
```

Syntax Description		
always		(Optional) Always advertises the default route regardless of whether the software has a default route.
metric <i>metric-value</i>		(Optional) Metric used for generating the default route. If you omit a value and do not specify a value using the default-metric router configuration command, the default metric value is 10. The value used is specific to the protocol.
metric-type <i>type-value</i>		(Optional) External link type associated with the default route advertised into the OSPF routing domain. It can be one of the following values: 1 —Type 1 external route 2 —Type 2 external route The default is Type 2 external route.
route-map <i>map-name</i>		(Optional) Routing process will generate the default route if the route map is satisfied.

default-metric (OSPF)

To set default metric values for the OSPF routing protocol, use the **default-metric** router configuration command. To return to the default state, use the **no** form of this command.

```
default-metric metric-value
```

```
no default-metric metric-value
```

Syntax Description	<i>metric-value</i>	Default metric value appropriate for the specified routing protocol.

distance ospf

To define OSPF route administrative distances based on route type, use the **distance ospf** router configuration command. To restore the default value, use the **no** form of this command.

```
distance ospf {[intra-area dist1] [inter-area dist2] [external dist3]}
```

```
no distance ospf
```

Syntax Description	intra-area <i>dist1</i>	(Optional) Sets the distance for all routes within an area. The default value is 110.
	inter-area <i>dist2</i>	(Optional) Sets the distance for all routes from one area to another area. The default value is 110.
	external <i>dist3</i>	(Optional) Sets the distance for routes from other routing domains, learned by redistribution. The default value is 110.

ignore lsa mospf

To suppress the sending of syslog messages when the router receives link-state advertisement (LSA) Type 6 Multicast OSPF (MOSPF) packets, which are unsupported, use the **ignore lsa mospf** router configuration command. To restore the sending of syslog messages, use the **no** form of this command.

ignore lsa mospf

no ignore lsa mospf

Syntax Description This command has no arguments or keywords.

ip ospf authentication

To specify the authentication type for an interface, use the **ip ospf authentication** interface configuration command. To remove the authentication type for an interface, use the **no** form of this command.

ip ospf authentication [**message-digest** | **null**]

no ip ospf authentication

Syntax Description	message-digest	(Optional) Specifies that message-digest authentication will be used.
	null	(Optional) No authentication is used. Useful for overriding password or message-digest authentication if configured for an area.

ip ospf authentication-key

To assign a password to be used by neighboring routers that are using the OSPF simple password authentication, use the **ip ospf authentication-key** interface configuration command. To remove a previously assigned OSPF password, use the **no** form of this command.

ip ospf authentication-key *password*

no ip ospf authentication-key

Syntax Description	<i>password</i>	Any continuous string of characters that can be entered from the keyboard up to 8 bytes in length.
---------------------------	-----------------	--

ip ospf cost

To explicitly specify the cost of sending a packet on an interface, use the **ip ospf cost** interface configuration command. To reset the path cost to the default value, use the **no** form of this command.

ip ospf cost *interface-cost*

no ip ospf cost *interface-cost*

Syntax Description	<i>interface-cost</i>	Unsigned integer value expressed as the link-state metric. It can be a value in the range from 1 to 65535.
---------------------------	-----------------------	--

ip ospf database-filter

To filter outgoing link-state advertisements (LSAs) to an OSPF interface, use the **ip ospf database-filter** interface configuration command. To restore the forwarding of LSAs to the interface, use the **no** form of this command.

ip ospf database-filter all out

no ip ospf database-filter all out

Syntax Description	This command has no arguments or keywords.
---------------------------	--

ip ospf dead-interval

To set the interval at which hello packets must not be seen before neighbors declare the router down, use the **ip ospf dead-interval** interface configuration command. To return to the default time, use the **no** form of this command.

ip ospf dead-interval *seconds*

no ip ospf dead-interval

Syntax Description	<i>seconds</i>	Specifies the interval (in seconds); the value must be the same for all nodes on the network.
---------------------------	----------------	---

ip ospf demand-circuit

To configure OSPF to treat the interface as an OSPF demand circuit, use the **ip ospf demand-circuit** interface configuration command. To remove the demand circuit designation from the interface, use the **no** form of this command.

ip ospf demand-circuit

no ip ospf demand-circuit

Syntax Description This command has no arguments or keywords.

ip ospf flood-reduction

To suppress the unnecessary flooding of link-state advertisements (LSAs) in stable topologies, use the **ip ospf flood-reduction** interface configuration command. To disable this feature, use the **no** form of this command.

ip ospf flood-reduction

no ip ospf flood-reduction

Syntax Description This command has no arguments or keywords.

ip ospf hello-interval

To specify the interval between hello packets that the Cisco IOS software sends on the interface, use the **ip ospf hello-interval** interface configuration command. To return to the default time, use the **no** form of this command.

ip ospf hello-interval *seconds*

no ip ospf hello-interval

Syntax Description *seconds* Specifies the interval (in seconds). The value must be the same for all nodes on a specific network.

ip ospf message-digest-key

To enable OSPF Message Digest 5 (MD5) authentication, use the **ip ospf message-digest-key** interface configuration command. To remove an old MD5 key, use the **no** form of this command.

```
ip ospf message-digest-key key-id md5 key
```

```
no ip ospf message-digest-key key-id
```

Syntax Description		
	<i>key-id</i>	An identifier in the range from 1 to 255.
	<i>key</i>	Alphanumeric password of up to 16 bytes.

ip ospf mtu-ignore

To disable OSPF MTU mismatch detection on receiving DBD packets, use the **ip ospf mtu-ignore** interface configuration command. To reset to default, use the **no** form of this command.

```
ip ospf mtu-ignore
```

```
no ip ospf mtu-ignore
```

Syntax Description	
	This command has no arguments or keywords.

ip ospf name-lookup

To configure OSPF to look up Domain Name System (DNS) names for use in all OSPF **show EXEC** command displays, use the **ip ospf name-lookup** global configuration command. To disable this function, use the **no** form of this command.

```
ip ospf name-lookup
```

```
no ip ospf name-lookup
```

Syntax Description	
	This command has no arguments or keywords.

ip ospf network

To configure the OSPF network type to a type other than the default for a given medium, use the **ip ospf network** interface configuration command. To return to the default value, use the **no** form of this command.

```
ip ospf network {broadcast | non-broadcast | {point-to-multipoint [non-broadcast] | point-to-point}}
```

```
no ip ospf network
```

Syntax Description	broadcast	Sets the network type to broadcast.
	non-broadcast	Sets the network type to nonbroadcast multiaccess (NBMA).
	point-to-multipoint [non-broadcast]	Sets the network type to point-to-multipoint. The optional non-broadcast keyword sets the point-to-multipoint network to be nonbroadcast. If you use the non-broadcast keyword, the neighbor command is required.
	point-to-point	Sets the network type to point-to-point.

ip ospf priority

To set the router priority, which helps determine the designated router for this network, use the **ip ospf priority** interface configuration command. To return to the default value, use the **no** form of this command.

ip ospf priority *number-value*

no ip ospf priority *number-value*

Syntax Description	<i>number-value</i>	A number value that specifies the priority of the router. The range is from 0 to 255.
---------------------------	---------------------	---

ip ospf retransmit-interval

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface, use the **ip ospf retransmit-interval** interface configuration command. To return to the default value, use the **no** form of this command.

ip ospf retransmit-interval *seconds*

no ip ospf retransmit-interval

Syntax Description	<i>seconds</i>	Time (in seconds) between retransmissions. It must be greater than the expected round-trip delay between any two routers on the attached network. The range is from 1 to 65535 seconds. The default is 5 seconds.
---------------------------	----------------	---

ip ospf transmit-delay

To set the estimated time required to send a link-state update packet on the interface, use the **ip ospf transmit-delay** interface configuration command. To return to the default value, use the **no** form of this command.

ip ospf transmit-delay *seconds*

no ip ospf transmit-delay

Syntax Description	<i>seconds</i>	Time (in seconds) required to send a link-state update. The range is from 1 to 65535 seconds. The default is 1 second.
---------------------------	----------------	--

log-adj-changes

To configure the router to send a syslog message when the state of an OSPF neighbor changes, use the **log-adj-changes** router configuration command. To turn off this function, use the **no** form of this command.

log-adj-changes [**detail**]

no log-adj-changes [**detail**]

Syntax Description	detail	(Optional) Restores the full adjacency changes logging.
---------------------------	---------------	---

neighbor (OSPF)

To configure OSPF routers interconnecting to nonbroadcast networks, use the **neighbor** router configuration command. To remove a configuration, use the **no** form of this command.

neighbor *ip-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter** **all**]

no neighbor *ip-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter** **all**]

Syntax Description	<i>ip-address</i>	Interface IP address of the neighbor.
	priority <i>number</i>	(Optional) A number that indicates the router priority value of the nonbroadcast neighbor associated with the IP address specified. The default is 0. This keyword does not apply to point-to-multipoint interfaces.
	poll-interval <i>seconds</i>	(Optional) A number value that represents the poll interval time (in seconds). RFC 1247 recommends that this value be much larger than the hello interval. The default is 120 seconds (2 minutes). This keyword does not apply to point-to-multipoint interfaces.

cost number	(Optional) Assigns a cost to the neighbor, in the form of an integer from 1 to 65535. Neighbors with no specific cost configured will assume the cost of the interface, based on the ip ospf cost command. For point-to-multipoint interfaces, the cost keyword and the <i>number</i> argument are the only options that are applicable. This keyword does not apply to nonbroadcast multiaccess (NBMA) networks.
database-filter	(Optional) Filters outgoing link-state advertisements (LSAs) to an OSPF neighbor.

neighbor database-filter

To filter outgoing link-state advertisements (LSAs) to an OSPF neighbor, use the **neighbor database-filter** router configuration command. To restore the forwarding of LSAs to the neighbor, use the **no** form of this command.

neighbor *ip-address* **database-filter all out**

no neighbor *ip-address* **database-filter all out**

Syntax Description

<i>ip-address all out</i>	IP address of the neighbor to which outgoing LSAs are blocked.
---------------------------	--

network area

To define the interfaces on which OSPF runs and to define the area ID for those interfaces, use the **network area** router configuration command. To disable OSPF routing for interfaces defined with the *address wildcard-mask* pair, use the **no** form of this command.

network *ip-address wildcard-mask* **area** *area-id*

no network *ip-address wildcard-mask* **area** *area-id*

Syntax Description

<i>ip-address</i>	IP address.
<i>wildcard-mask</i>	IP-address-type mask that includes “don’t care” bits.
<i>area-id</i>	Area that is to be associated with the OSPF address range. It can be specified as either a decimal value or as an IP address. If you intend to associate areas with IP subnets, you can specify a subnet address as the <i>area-id</i> .

router-id

To use a fixed router ID, use the **router-id** router configuration command. To force OSPF to use the previous OSPF router ID behavior, use the **no** form of this command.

router-id *ip-address*

no router-id *ip-address*

Syntax Description

<i>ip-address</i>	Router ID in IP address format.
-------------------	---------------------------------

router ospf

To configure an OSPF routing process, use the **router ospf** global configuration command. To terminate an OSPF routing process, use the **no** form of this command.

```
router ospf process-id
no router ospf process-id
```

Syntax Description	<i>process-id</i>	Internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process.
---------------------------	-------------------	---

show ip ospf

To display general information about OSPF routing processes, use the **show ip ospf** EXEC command.

```
show ip ospf [process-id]
```

Syntax Description	<i>process-id</i>	(Optional) Process ID. If this argument is included, only information for the specified routing process is included.
---------------------------	-------------------	--

show ip ospf border-routers

To display the internal OSPF routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the **show ip ospf border-routers** privileged EXEC command.

```
show ip ospf border-routers
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--

show ip ospf database

To display lists of information related to the OSPF database for a specific router, use the **show ip ospf database** EXEC command. The various forms of this command deliver information about different OSPF link-state advertisements (LSAs).

```
show ip ospf [process-id [area-id]] database
show ip ospf [process-id [area-id]] database [adv-router [ip-address]]
```

```
show ip ospf [process-id [area-id]] database [asbr-summary] [link-state-id]

show ip ospf [process-id [area-id]] database [asbr-summary] [link-state-id] [adv-router
[ip-address]]

show ip ospf [process-id [area-id]] database [asbr-summary] [link-state-id] [self-originate]
[link-state-id]

show ip ospf [process-id [area-id]] database [database-summary]

show ip ospf [process-id [area-id]] database [external] [link-state-id]

show ip ospf [process-id [area-id]] database [external] [link-state-id] [adv-router [ip-address]]

show ip ospf [process-id [area-id]] database [external] [link-state-id] [self-originate]
[link-state-id]

show ip ospf [process-id [area-id]] database [network][link-state-id]

show ip ospf [process-id [area-id]] database [network] [link-state-id] [adv-router [ip-address]]

show ip ospf [process-id [area-id]] database [network] [link-state-id] [self-originate]
[link-state-id]

show ip ospf [process-id [area-id]] database [nssa-external] [link-state-id]

show ip ospf [process-id [area-id]] database [nssa-external] [link-state-id] [adv-router
[ip-address]]

show ip ospf [process-id [area-id]] database [nssa-external] [link-state-id] [self-originate]
[link-state-id]

show ip ospf [process-id [area-id]] database [opaque-area] [link-state-id]

show ip ospf [process-id [area-id]] database [opaque-area] [link-state-id] [adv-router
[ip-address]]

show ip ospf [process-id [area-id]] database [opaque-area] [link-state-id] [self-originate]
[link-state-id]

show ip ospf [process-id [area-id]] database [opaque-as] [link-state-id]

show ip ospf [process-id [area-id]] database [opaque-as] [link-state-id] [adv-router
[ip-address]]
```

```
show ip ospf [process-id [area-id]] database [opaque-as] [link-state-id] [self-originate]
[link-state-id]
```

```
show ip ospf [process-id [area-id]] database [opaque-link] [link-state-id]
```

```
show ip ospf [process-id [area-id]] database [opaque-link] [link-state-id] [adv-router
[ip-address]]
```

```
show ip ospf [process-id [area-id]] database [opaque-link] [link-state-id] [self-originate]
[link-state-id]
```

```
show ip ospf [process-id [area-id]] database [router] [link-state-id]
```

```
show ip ospf [process-id [area-id]] database [router] [adv-router [ip-address]]
```

```
show ip ospf [process-id [area-id]] database [router] [self-originate] [link-state-id]
```

```
show ip ospf [process-id [area-id]] database [self-originate] [link-state-id]
```

```
show ip ospf [process-id [area-id]] database [summary] [link-state-id]
```

```
show ip ospf [process-id [area-id]] database [summary] [link-state-id] [adv-router [ip-address]]
```

```
show ip ospf [process-id [area-id]] database [summary] [link-state-id] [self-originate]
[link-state-id]
```

Syntax Description

<i>process-id</i>	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPF routing process.
<i>area-id</i>	(Optional) Area number associated with the OSPF address range defined in the network router configuration command used to define the particular area.
adv-router [<i>ip-address</i>]	(Optional) Displays all the link-state advertisements (LSAs) of the specified router. If no IP address is included, the information is about the local router itself (in this case, the same as the self-originate keyword).
asbr-summary	(Optional) Displays information only about the Autonomous System Boundary Router (ASBR) summary LSAs.

<i>link-state-id</i>	<p>(Optional) Portion of the Internet environment that is being described by the advertisement. The value entered depends on the type of the LSA. The value must be entered in the form of an IP address.</p> <p>When the LSA is describing a network, the <i>link-state-id</i> argument can take one of two forms:</p> <ul style="list-style-type: none"> • The network IP address (as in Type 3 summary link advertisements and in autonomous system external link advertisements). • A derived address obtained from the link-state ID. (Note that masking a network will link the advertisement link-state ID with the network subnet mask yielding the network IP address.) <p>When the LSA is describing a router, the link-state ID is always the OSPF router ID of the described router.</p> <p>When an autonomous system external advertisement (Type 5) is describing a default route, its link-state ID is set to the default destination (0.0.0.0).</p>
database-summary	(Optional) Displays how many of each type of LSA for each area there are in the database, and the total.
external	(Optional) Displays information only about the external LSAs.
network	(Optional) Displays information only about the network LSAs.
nssa-external	(Optional) Displays information only about the not so stubby area (NSSA) external LSAs.
opaque-area	(Optional) Displays information about the opaque Type 10 LSAs. Type 10 denotes an area-local scope. Refer to RFC 2370 for more information on the opaque LSA options.
opaque-as	(Optional) Displays information about the opaque Type 11 LSAs. Type 11 denotes that the LSA is flooded throughout the autonomous system.
opaque-link	(Optional) Displays information about the opaque Type 9 LSAs. Type 9 denotes a link-local scope.
router	(Optional) Displays information only about the router LSAs.
self-originate	(Optional) Displays only self-originated LSAs (from the local router).
summary	(Optional) Displays information only about the summary LSAs.

show ip ospf flood-list

To display a list of OSPF link-state advertisements (LSAs) waiting to be flooded over an interface, use the **show ip ospf flood-list EXEC** command.

```
show ip ospf flood-list interface-type interface-number
```

Syntax Description

<i>interface-type</i>	Interface type over which the LSAs will be flooded.
<i>interface-number</i>	Interface number over which the LSAs will be flooded.

show ip ospf interface

To display OSPF-related interface information, use the **show ip ospf interface** EXEC command.

```
show ip ospf interface [interface-type interface-number]
```

Syntax Description	<i>interface-type</i>	(Optional) Interface type.
	<i>interface-number</i>	(Optional) Interface number.

show ip ospf neighbor

To display OSPF-neighbor information on a per-interface basis, use the **show ip ospf neighbor** EXEC command.

```
show ip ospf neighbor [interface-type interface-number] [neighbor-id] [detail]
```

Syntax Description	<i>interface-type</i>	(Optional) Interface type.
	<i>interface-number</i>	(Optional) Interface number.
	<i>neighbor-id</i>	(Optional) Neighbor ID.
	detail	(Optional) Displays all neighbors given in detail (list all neighbors).

show ip ospf request-list

To display a list of all link-state advertisements (LSAs) requested by a router, use the **show ip ospf request-list** EXEC command.

```
show ip ospf request-list [neighbor] [interface] [interface-neighbor]
```

Syntax Description	<i>neighbor</i>	(Optional) Displays the list of all LSAs requested by the router from this neighbor.
	<i>interface</i>	(Optional) Displays the list of all LSAs requested by the router from this interface.
	<i>interface-neighbor</i>	(Optional) Displays the list of all LSAs requested by the router on this interface from this neighbor.

show ip ospf retransmission-list

To display a list of all link-state advertisements (LSAs) waiting to be resent, use the **show ip ospf retransmission-list** EXEC command.

```
show ip ospf retransmission-list [neighbor] [interface] [interface-neighbor]
```

Syntax Description	<i>neighbor</i>	(Optional) Displays the list of all LSAs waiting to be resent for this neighbor.
	<i>interface</i>	(Optional) Displays the list of all LSAs waiting to be resent on this interface.
	<i>interface-neighbor</i>	(Optional) Displays the list of all LSAs waiting to be resent on this interface from this neighbor.

show ip ospf summary-address

To display a list of all summary address redistribution information configured under an OSPF process, use the **show ip ospf summary-address** EXEC command.

```
show ip ospf [process-id] summary-address
```

Syntax Description	<i>process-id</i>	(Optional) OSPF area ID.
---------------------------	-------------------	--------------------------

show ip ospf virtual-links

To display parameters and the current state of OSPF virtual links, use the **show ip ospf virtual-links** EXEC command.

```
show ip ospf virtual-links
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--

summary-address (OSPF)

To create aggregate addresses for OSPF, use the **summary-address** router configuration command. To restore the default, use the **no** form of this command.

```
summary-address summary-address mask prefix mask [not-advertise] [tag tag]
```

```
no summary-address address mask prefix mask [not-advertise] [tag tag]
```

Syntax Description	<i>summary-address</i>	Summary address designated for a range of addresses.
	<i>mask</i>	IP subnet mask used for the summary route.
	<i>prefix</i>	IP route prefix for the destination.
	<i>mask</i>	IP subnet mask used for the summary route.
	not-advertise	(Optional) Suppress routes that match the specified prefix/mask pair. This keyword applies to OSPF only.
	tag tag	(Optional) Tag value that can be used as a “match” value for controlling redistribution via route maps. This keyword applies to OSPF only.

timers lsa-group-pacing

To change the interval at which OSPF link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged, use the **timers lsa-group-pacing** router configuration command. To restore the default value, use the **no** form of this command.

timers lsa-group-pacing *seconds*

no timers lsa-group-pacing

Syntax Description

<i>seconds</i>	Number of seconds in the interval at which LSAs are grouped and refreshed, checksummed, or aged. The range is from 10 to 1800 seconds. The default value is 240 seconds.
----------------	--

timers spf

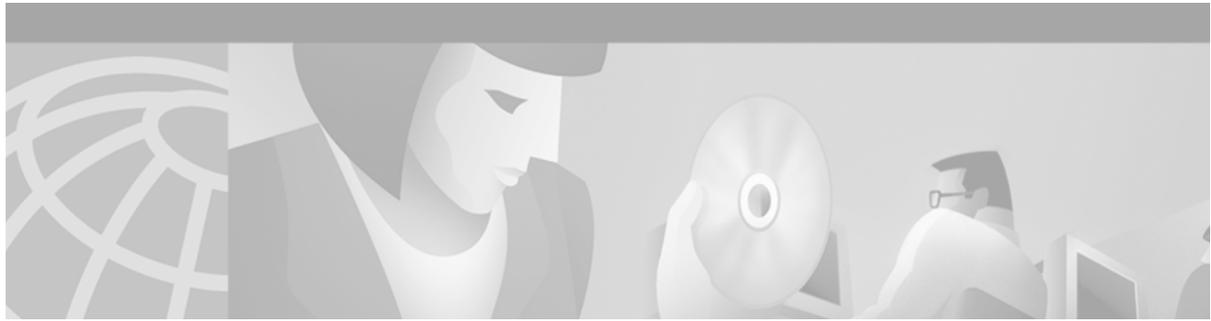
To configure the delay time between when OSPF receives a topology change and when it starts a shortest path first (SPF) calculation, and the hold time between two consecutive SPF calculations, use the **timers spf** router configuration command. To return to the default timer values, use the **no** form of this command.

timers spf *spf-delay spf-holdtime*

no timers spf *spf-delay spf-holdtime*

Syntax Description

<i>spf-delay</i>	Delay time (in seconds) between when OSPF receives a topology change and when it starts an SPF calculation. It can be an integer from 0 to 65535. The default time is 5 seconds. A value of 0 means that there is no delay; that is, the SPF calculation is started immediately.
<i>spf-holdtime</i>	Minimum time (in seconds) between two consecutive SPF calculations. It can be an integer from 0 to 65535. The default time is 10 seconds. A value of 0 means that there is no delay; that is, two SPF calculations can be done, one immediately after the other.



Enhanced IGRP Commands

This chapter describes the function and syntax of the Enhanced Interior Gateway Routing Protocol (EIGRP) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*.

auto-summary (Enhanced IGRP)

To restore the default behavior of automatic summarization of subnet routes into network-level routes, use the **auto-summary** router configuration command. To disable this function and send subprefix routing information across classful network boundaries, use the **no** form of this command.

auto-summary

no auto-summary

Syntax Description This command has no arguments or keywords.

clear ip eigrp neighbors

To delete entries from the neighbor table, use the **clear ip eigrp neighbors** EXEC command.

clear ip eigrp neighbors [*ip-address* | *interface-type interface-number*]

Syntax Description	<i>ip-address</i>	(Optional) Address of the neighbor.
	<i>interface-type</i> <i>interface-number</i>	(Optional) Interface type and number. Specifying these arguments removes the specified interface type from the neighbor table all entries learned via this interface.

default-information

To control the candidate default routing information between IGRP or Enhanced IGRP (EIGRP) processes, use the **default-information** router configuration command. To suppress IGRP or EIGRP candidate information in incoming updates, use the **no default-information in** command. To suppress IGRP or EIGRP candidate information in outbound updates, use the **no default-information out** command.

default-information { **in** | **out** } { *access-list-number* | *access-list-name* }

no default-information { **in** | **out** }

Syntax Description		
	in	Allows IGRP or EIGRP exterior or default routes to be received by an IGRP process.
	out	Allows IGRP or EIGRP exterior routes to be advertised in updates.
	<i>access-list-number</i> <i>access-list-name</i>	Number or name of an access list. It can be a number in the range from 1 to 99 or an access list name.

default-metric (IGRP and Enhanced IGRP)

To set metrics for IGRP or Enhanced IGRP (EIGRP), use the **default-metric** router configuration command. To remove the metric value and restore the default state, use the **no** form of this command.

default-metric *bandwidth delay reliability loading mtu*

no default-metric *bandwidth delay reliability loading mtu*

Syntax Description		
	<i>bandwidth</i>	Minimum bandwidth of the route in kbps. It can be 0 or any positive integer.
	<i>delay</i>	Route delay (in tens of microseconds). It can be 0 or any positive number that is a multiple of 39.1 nanoseconds.
	<i>reliability</i>	Likelihood of successful packet transmission expressed as a number from 0 to 255. The value 255 means 100 percent reliability; 0 means no reliability.
	<i>loading</i>	Effective bandwidth of the route expressed as a number from 0 to 255 (255 is 100 percent loading).
	<i>mtu</i>	Maximum transmission unit (MTU) size of the route in bytes. It can be 0 or any positive integer.

distance eigrp

To allow the use of two administrative distances—internal and external—that could be a better route to a node, use the **distance eigrp** router configuration command. To reset these values to their defaults, use the **no** form of this command.

distance eigrp *internal-distance external-distance*

no distance eigrp

Syntax Description	<i>internal-distance</i>	Administrative distance for Enhanced IGRP (EIGRP) internal routes. Internal routes are those that are learned from another entity within the same autonomous system. It can be a value from 1 to 255.
	<i>external-distance</i>	Administrative distance for EIGRP external routes. External routes are those for which the best path is learned from a neighbor external to the autonomous system. It can be a value from 1 to 255.

eigrp log-neighbor-changes

To enable the logging of changes in Enhanced IGRP (EIGRP) neighbor adjacencies, use the **eigrp log-neighbor-changes** router configuration command. To disable the logging of changes in EIGRP neighbor adjacencies, use the **no** form of this command.

eigrp log-neighbor-changes

no eigrp log-neighbor-changes

Syntax Description	This command has no arguments or keywords.
---------------------------	--

eigrp log-neighbor-warnings

To enable the logging of Enhanced IGRP (EIGRP) neighbor warning messages, use the **eigrp log-neighbor-warnings** router configuration command. To disable the logging of EIGRP neighbor warning messages, use the **no** form of this command.

eigrp log-neighbor-warnings [*seconds*]

no eigrp log-neighbor-warnings

Syntax Description	<i>seconds</i>	(Optional) The time interval (in seconds) between repeated neighbor warning messages. The range of seconds is from 1 to 65535.
---------------------------	----------------	--

eigrp stub

To configure a router as a stub using Enhanced IGRP (EIGRP), use the **eigrp stub** router configuration command. To disable the EIGRP stub routing feature, use the **no** form of this command.

eigrp stub [**receive-only** | **connected** | **static** | **summary**]

no eigrp stub [**receive-only** | **connected** | **static** | **summary**]

Syntax Description		
	receive-only	(Optional) Sets the router as a receive-only neighbor.
	connected	(Optional) Advertises connected routes.
	static	(Optional) Advertises static routes.
	summary	(Optional) Advertises summary routes.

ip authentication key-chain eigrp

To enable authentication of Enhanced IGRP (EIGRP) packets, use the **ip authentication key-chain eigrp** interface configuration command. To disable such authentication, use the **no** form of this command.

ip authentication key-chain eigrp *as-number key-chain*

no ip authentication key-chain eigrp *as-number key-chain*

Syntax Description		
	<i>as-number</i>	Autonomous system number to which the authentication applies.
	<i>key-chain</i>	Name of the authentication key chain.

ip authentication mode eigrp

To specify the type of authentication used in Enhanced IGRP (EIGRP) packets, use the **ip authentication mode eigrp** interface configuration command. To disable that type of authentication, use the **no** form of this command.

ip authentication mode eigrp *as-number md5*

no ip authentication mode eigrp *as-number md5*

Syntax Description		
	<i>as-number</i>	Autonomous system number.
	md5	Keyed Message Digest (MD5) authentication.

ip bandwidth-percent eigrp

To configure the percentage of bandwidth that may be used by Enhanced IGRP (EIGRP) on an interface, use the **ip bandwidth-percent eigrp** interface configuration command. To restore the default value, use the **no** form of this command.

ip bandwidth-percent eigrp *as-number percent*

no ip bandwidth-percent eigrp *as-number percent*

Syntax Description

<i>as-number</i>	Autonomous system number.
<i>percent</i>	Percent of bandwidth that EIGRP may use.

ip hello-interval eigrp

To configure the hello interval for the EIGRP routing process designated by an autonomous system number, use the **ip hello-interval eigrp** interface configuration command. To restore the default value, use the **no** form of this command.

ip hello-interval eigrp *as-number seconds*

no ip hello-interval eigrp *as-number seconds*

Syntax Description

<i>as-number</i>	Autonomous system number.
<i>seconds</i>	Hello interval (in seconds).

ip hold-time eigrp

To configure the hold time for a particular Enhanced IGRP (EIGRP) routing process designated by the autonomous system number, use the **ip hold-time eigrp** interface configuration command. To restore the default value, use the **no** form of this command.

ip hold-time eigrp *as-number seconds*

no ip hold-time eigrp *as-number seconds*

Syntax Description

<i>as-number</i>	Autonomous system number.
<i>seconds</i>	Hold time (in seconds).

ip split-horizon eigrp

To enable Enhanced IGRP (EIGRP) split horizon, use the **ip split-horizon eigrp** interface configuration command. To disable split horizon, use the **no** form of this command.

ip split-horizon eigrp *as-number*

no ip split-horizon eigrp *as-number*

Syntax Description	
<i>as-number</i>	Autonomous system number.

ip summary-address eigrp

To configure a summary aggregate address for a specified interface, use the **ip summary-address eigrp** interface configuration command. To disable a configuration, use the **no** form of this command.

ip summary-address eigrp *as-number network-address subnet-mask [admin-distance]*

no ip summary-address eigrp *as-number network-address subnet-mask [admin-distance]*

Syntax Description	
<i>as-number</i>	Autonomous system number.
<i>network-address</i>	IP summary aggregate address to apply to an interface.
<i>subnet-mask</i>	Subnet mask.
<i>admin-distance</i>	(Optional) Administrative distance. A value from 0 to 255.

metric weights (IGRP and Enhanced IGRP)

To allow the tuning of the IGRP or Enhanced IGRP (EIGRP) metric calculations, use the **metric weights** router configuration command. To reset the values to their defaults, use the **no** form of this command.

metric weights *tos k1 k2 k3 k4 k5*

no metric weights

Syntax Description	
<i>tos</i>	Type of service. Currently, it must always be zero.
<i>k1-k5</i>	Constants that convert an IGRP or EIGRP metric vector into a scalar quantity.

network (Enhanced IGRP)

To specify a list of networks for the Enhanced IGRP (EIGRP) routing process, use the **network** router configuration command. To remove an entry, use the **no** form of this command.

network *network-number* [*network-mask*]

no network *network-number* [*network-mask*]

Syntax Description		
<i>network-number</i>		IP address of the directly connected networks.
<i>network-mask</i>		(Optional) Network mask.

offset-list (Enhanced IGRP)

To add an offset to incoming and outgoing metrics to routes learned via Enhanced IGRP (EIGRP), use the **offset-list** router configuration command. To remove an offset list, use the **no** form of this command.

offset-list {*access-list-number* | *access-list-name*} {**in** | **out**} *offset* [*interface-type* *interface-number*]

no offset-list {*access-list-number* | *access-list-name*} {**in** | **out**} *offset* [*interface-type* *interface-number*]

Syntax Description		
<i>access-list-number</i> <i>access-list-name</i>		Standard access list number or name to be applied. Access list number 0 indicates all access lists. If the <i>offset</i> value is 0, no action is taken. For IGRP, the offset is added to the delay component only.
in		Applies the access list to incoming metrics.
out		Applies the access list to outgoing metrics.
<i>offset</i>		Positive offset to be applied to metrics for networks matching the access list. If the offset is 0, no action is taken.
<i>interface-type</i>		(Optional) Interface type to which the offset list is applied.
<i>interface-number</i>		(Optional) Interface number to which the offset list is applied.

router eigrp

To configure the Enhanced IGRP (EIGRP) routing process, use the **router eigrp** global configuration command. To shut down a routing process, use the **no** form of this command.

router eigrp *as-number*

no router eigrp *as-number*

Syntax Description		
<i>as-number</i>		Autonomous system number that identifies the routes to the other EIGRP routers. It is also used to tag the routing information.

set metric (Enhanced IGRP)

To set the metric value for Enhanced IGRP (EIGRP) in a route map, use the **set metric** route-map configuration command. To return to the default metric value, use the **no** form of this command.

set metric *bandwidth delay reliability loading mtu*

no set metric *bandwidth delay reliability loading mtu*

Syntax Description	
<i>bandwidth</i>	Metric value or IGRP bandwidth of the route in kbps. It can be in the range 0 to 4294967295.
<i>delay</i>	Route delay (in tens of microseconds). It can be in the range from 0 to 4294967295.
<i>reliability</i>	Likelihood of successful packet transmission expressed as a number from 0 to 255. The value 255 means 100 percent reliability; 0 means no reliability.
<i>loading</i>	Effective bandwidth of the route expressed as a number from 0 to 255 (255 is 100 percent loading).
<i>mtu</i>	Minimum maximum transmission unit (MTU) size of the route, in bytes. It can be in the range from 0 to 4294967295.

show ip eigrp interfaces

To display information about interfaces configured for Enhanced IGRP (EIGRP), use the **show ip eigrp interfaces** EXEC command.

show ip eigrp interfaces [*interface-type interface-number*] [*as-number*]

Syntax Description	
<i>interface-type</i>	(Optional) Interface type.
<i>interface-number</i>	(Optional) Interface number.
<i>as-number</i>	(Optional) Autonomous system number.

show ip eigrp neighbors

To display the neighbors discovered by Enhanced IGRP (EIGRP), use the **show ip eigrp neighbors** EXEC command.

show ip eigrp neighbors [*interface-type* | *as-number* | **static**]

Syntax Description	
<i>interface-type</i>	(Optional) Interface type.
<i>as-number</i>	(Optional) Autonomous system number.
static	(Optional) Static routes.

show ip eigrp topology

To display the Enhanced IGRP (EIGRP) topology table, use the **show ip eigrp topology** EXEC command.

```
show ip eigrp topology [as-number | [[ip-address] mask]]
```

Syntax	Description
<i>as-number</i>	(Optional) Autonomous system number.
<i>ip-address</i>	(Optional) IP address. When specified with a mask, a detailed description of the entry is provided.
<i>mask</i>	(Optional) Subnet mask.

show ip eigrp traffic

To display the number of Enhanced IGRP (EIGRP) packets sent and received, use the **show ip eigrp traffic** EXEC command.

```
show ip eigrp traffic [as-number]
```

Syntax	Description
<i>as-number</i>	(Optional) Autonomous system number.

timers active-time

To adjust routing wait time, use the **timers active-time** router configuration command. To disable this function, use the **no** form of the command.

```
timers active-time [1-4294967295 | disabled]
```

```
no timers active-time
```

Syntax	Description
<i>1-4294967295</i>	EIGRP active-time limit (in minutes).
disabled	Disables the timers and permits the routing wait time to remain active indefinitely.

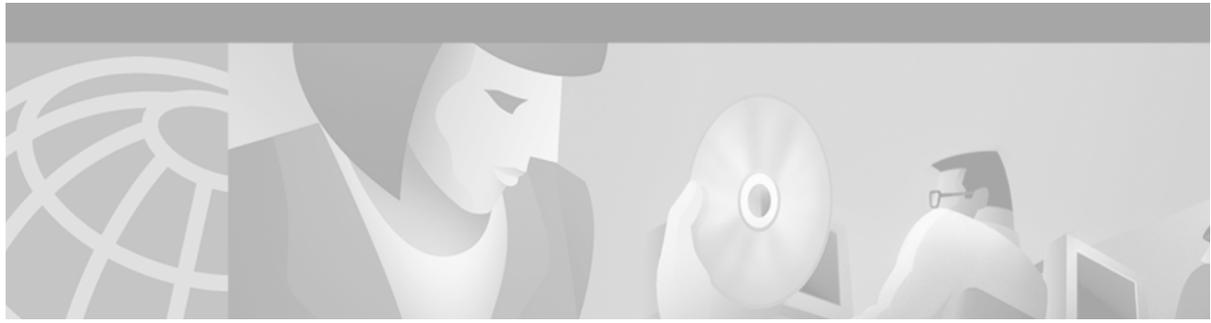
traffic-share balanced

To control how traffic is distributed among routes when there are multiple routes for the same destination network that have different costs, use the **traffic-share balanced** router configuration command. To disable this function, use the **no** form of the command.

traffic-share balanced

no traffic-share balanced

Syntax Description This command has no arguments or keywords.



Integrated IS-IS Commands

This chapter describes the function and syntax of the Intermediate System-to-Intermediate System (IS-IS) protocol commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*.

area-password

To configure the IS-IS area authentication password, use the **area-password** router configuration command. To disable the password, use the **no** form of this command.

```
area-password password
```

```
no area-password [password]
```

Syntax Description

password

Password you assign.

default-information originate (IS-IS)

To generate a default route into an IS-IS routing domain, use the **default-information originate** router configuration command. To disable this feature, use the **no** form of this command.

```
default-information originate [route-map map-name]
```

```
no default-information originate [route-map map-name]
```

Syntax Description

route-map *map-name*

(Optional) Routing process will generate the default route if the route map is satisfied.

domain-password

To configure the IS-IS routing domain authentication password, use the **domain-password** router configuration command. To disable a password, use the **no** form of this command.

domain-password *password*

no domain-password [*password*]

Syntax Description	<i>password</i>	Password you assign.
--------------------	-----------------	----------------------

ip router isis

To configure an IS-IS routing process for IP on an interface and to attach an area designator to the routing process, use the **ip router isis** interface configuration command. To disable IS-IS for IP, use the **no** form of the command.

ip router isis *area-tag*

no ip router isis *area-tag*

Syntax Description	<i>area-tag</i>	Each area in a multiarea configuration should have a nonnull area tag to facilitate identification of the area. Meaningful name for a routing process. If it is not specified, a null tag is assumed and the process is referenced with a null tag. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router. Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration.
--------------------	-----------------	--

isis circuit-type

To configure the type of adjacency, use the **isis circuit-type** interface configuration command. To reset the circuit type to Level 1 and Level 2, use the **no** form of this command.

isis circuit-type [**level-1** | **level-1-2** | **level-2-only**]

no isis circuit-type

Syntax Description	level-1	(Optional) Configures a router for Level 1 adjacency only.
	level-1-2	(Optional) Configures a router for Level 1 and Level 2 adjacency.
	level-2-only	(Optional) Configures a router for the Level 2 adjacency only.

isis csnp-interval

To configure the IS-IS complete sequence number PDUs (CSNPs) interval, use the **isis csnp-interval** interface configuration command. To restore the default value, use the **no** form of this command.

isis csnp-interval *seconds* [**level-1** | **level-2**]

no isis csnp-interval [**level-1** | **level-2**]

Syntax Description		
	<i>seconds</i>	Interval of time between transmission of CSNPs on multiaccess networks. This interval only applies for the designated router. The default is 10 seconds.
	level-1	(Optional) Configures the interval of time between transmission of CSNPs for Level 1 independently.
	level-2	(Optional) Configures the interval of time between transmission of CSNPs for Level 2 independently.

isis display delimiter

To make output from multiarea displays easier to read by specifying the delimiter to use to separate displays of information, use the **isis display delimiter** global configuration command. To disable this output format, use the **no** form of the command.

isis display delimiter [**return** *count* | *character count*]

no isis display delimiter [**return** *count* | *character count*]

Syntax Description		
	return	(Optional) Delimit with carriage returns.
	<i>count</i>	(Optional) Number of carriage returns or length of string to use for the delimiter.
	<i>character</i>	(Optional) Character to use for the delimiter string.

isis hello-interval

To specify the length of time between hello packets that the Cisco IOS software sends, use the **isis hello-interval** interface configuration command. To restore the default value, use the **no** form of this command.

isis hello-interval *seconds* [**level-1** | **level-2**]

no isis hello-interval [**level-1** | **level-2**]

Syntax Description	<i>seconds</i>	An integer value. By default, a value three times the hello interval <i>seconds</i> is advertised as the hold time in the hello packets sent. (Change multiplier of 3 by specifying the isis hello-multiplier command.) With smaller hello intervals, topological changes are detected faster, but there is more routing traffic. The default is 10 seconds.
level-1		(Optional) Configures the hello interval for Level 1 independently. Use this on X.25, Switched Multimegabit Data Service (SMDS), and Frame Relay multiaccess networks.
level-2		(Optional) Configures the hello interval for Level 2 independently. Use this on X.25, SMDS, and Frame Relay multiaccess networks.

isis hello-multiplier

To specify the number of IS-IS hello packets a neighbor must miss before the router should declare the adjacency as down, use the **isis hello-multiplier** interface configuration command. To restore the default value, use the **no** form of this command.

isis hello-multiplier *multiplier* [**level-1** | **level-2**]

no isis hello-multiplier [**level-1** | **level-2**]

Syntax Description	<i>multiplier</i>	Integer value from 3 to 1000. The advertised hold time in IS-IS hello packets will be set to the hello multiplier times the hello interval. Neighbors will declare an adjacency to this router down after not having received any IS-IS hello packets during the advertised hold time. The hold time (and thus the hello multiplier and the hello interval) can be set on a per-interface basis, and can be different between different routers in one area. Using a smaller hello multiplier will give fast convergence, but can result in more routing instability. Increment the hello multiplier to a larger value to help network stability when needed. Never configure a hello multiplier lower than the default value of 3.
level-1		(Optional) Configures the hello multiplier independently for Level 1 adjacencies.
level-2		(Optional) Configures the hello multiplier independently for Level 2 adjacencies.

isis lsp-interval

To configure the time delay between successive IS-IS link-state packet (LSP) transmissions, use the **isis lsp-interval** interface configuration command. To restore the default value, use the **no** form of this command.

isis lsp-interval *milliseconds*

no isis lsp-interval

Syntax Description	<i>milliseconds</i>	Time delay between successive LSPs (in milliseconds).
---------------------------	---------------------	---

isis mesh-group

To optimize link-state packet (LSP) flooding in nonbroadcast multiaccess (NBMA) networks with highly meshed, point-to-point topologies, use the **isis mesh-group** interface configuration command. To remove a subinterface from a mesh group, use the **no** form of this command.

isis mesh-group [*number* | **blocked**]

no isis mesh-group [*number* | **blocked**]

Syntax Description	<i>number</i>	(Optional) A number identifying the mesh group of which this interface is a member.
Syntax Description	blocked	(Optional) Keyword specifying that no LSP flooding will take place on this subinterface.

isis metric

To configure the metric for an interface, use the **isis metric** interface configuration command. To restore the default metric value, use the **no** form of this command.

isis metric *default-metric* [**level-1** | **level-2**]

no isis metric [**level-1** | **level-2**]

Syntax Description	<i>default-metric</i>	Metric assigned to the link and used to calculate the cost from each other router via the links in the network to other destinations. You can configure this metric for Level 1 or Level 2 routing. The range is from 0 to 63. The default value is 10.
Syntax Description	level-1	(Optional) This metric should be used only in the shortest path first (SPF) calculation for Level 1 (intra-area) routing.
Syntax Description	level-2	(Optional) This metric should be used only in the SPF calculation for Level 2 (interarea) routing.

isis password

To configure the authentication password for an interface, use the **isis password** interface configuration command. To disable authentication for IS-IS, use the **no** form of this command.

isis password *password* [**level-1** | **level-2**]

no isis password [**level-1** | **level-2**]

Syntax Description	<i>password</i>	Authentication password you assign for an interface.
	level-1	(Optional) Configures the authentication password for Level 1 independently. For Level 1 routing, the router acts as a station router only.
	level-2	(Optional) Configures the authentication password for Level 2 independently. For Level 2 routing, the router acts as an area router only.

isis priority

To configure the priority of designated routers, use the **isis priority** interface configuration command. To reset the default priority, use the **no** form of this command.

isis priority *number-value* [**level-1** | **level-2**]

no isis priority [**level-1** | **level-2**]

Syntax Description	<i>number-value</i>	Sets the priority of a router and is a number from 0 to 127. The default value is 64.
	level-1	(Optional) Sets the priority for Level 1 independently.
	level-2	(Optional) Sets the priority for Level 2 independently.

isis retransmit-interval

To configure the amount of time between retransmission of each IS-IS link-state packet (LSP) on a point-to-point link, use the **isis retransmit-interval** interface configuration command. To restore the default value, use the **no** form of this command.

isis retransmit-interval *seconds*

no isis retransmit-interval *seconds*

Syntax Description	<i>seconds</i>	Time (in seconds) between retransmission of each LSP. It is an integer that should be greater than the expected round-trip delay between any two routers on the attached network. The default is 5 seconds.
---------------------------	----------------	---

isis retransmit-throttle-interval

To configure the amount of time between retransmissions on each IS-IS link-state packet (LSP) on a point-to-point interface, use the **isis retransmit-throttle-interval** interface configuration command. To restore the default value, use the **no** form of this command.

isis retransmit-throttle-interval *milliseconds*

no isis retransmit-throttle-interval

Syntax Description

<i>milliseconds</i>	Minimum delay (in milliseconds) between LSP retransmissions on the interface.
---------------------	---

is-type

To configure the routing level for an instance of the IS-IS routing process, use the **is-type** router configuration command. To reset the default value, use the **no** form of this command.

is-type [**level-1** | **level-1-2** | **level-2-only**]

no is-type [**level-1** | **level-1-2** | **level-2-only**]

Syntax Description

level-1	(Optional) Router performs only Level 1 (intra-area) routing. This router only learns about destinations inside its area. Level 2 (interarea) routing is performed by the closest Level 1-2 router.
level-1-2	(Optional) Router performs both Level 1 and Level 2 routing. This router runs two instances of the routing process. It has one link-state packet database (LSDB) for destinations inside the area (Level 1 routing) and runs an shortest path first (SPF) calculation to discover the area topology. It also has another LSDB with link-state packets (LSPs) of all other backbone (Level 2) routers, and runs another SPF calculation to discover the topology of the backbone, and the existence of all other areas.
level-2-only	(Optional) Routing process acts as a Level 2 (interarea) router only. This router is part of the backbone, and does not communicate with Level 1-only routers in its own area.

net

To configure an IS-IS network entity title (NET) for a Connectionless Network Service (CLNS) routing process, use the **net** router configuration command. To remove a NET, use the **no** form of this command.

net *network-entity-title*

no net *network-entity-title*

Syntax Description

network-entity-title

NET that specifies the area address and the system ID for a CLNS routing process. This argument can be either an address or a name.

partition avoidance

To cause an IS-IS Level 1-2 border router to stop advertising the Level 1 area prefix into the Level 2 backbone when full connectivity is lost between the border router, all adjacent Level 1 routers, and end hosts, use the **partition avoidance** router configuration command. To disable this output format, use the **no** form of the command.

partition avoidance *area-tag*

no partition avoidance *area-tag*

Syntax Description

area-tag

Meaningful name for a routing process. If it is not specified, a null tag is assumed and the process is referenced with a null tag. This name must be unique among all IP or Connectionless Network Service Protocol (CLNS) router processes for a given router.

Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration.

router isis

To enable the IS-IS routing protocol and to specify an IS-IS process, use the **router isis** global configuration command. To disable IS-IS routing, use the **no** form of this command.

router isis *area-tag*

no router isis *area-tag*

Syntax Description

area-tag

Meaningful name for a routing process. If it is not specified, a null tag is assumed and the process is referenced with a null tag. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router.

Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration.

set-overload-bit

To configure the router to signal other routers not to use it as an intermediate hop in their shortest path first (SPF) calculations, use the **set-overload-bit** router configuration command. To remove the designation, use the **no** form of this command.

set-overload-bit

no set-overload-bit

Syntax Description This command has no arguments or keywords.

show isis database

To display the IS-IS link-state database, use the **show isis database EXEC** command.

show isis *area-tag* database [level-1] [level-2] [l1] [l2] [detail] [lspid]

Syntax Description	<i>area-tag</i>	Meaningful name for a routing process. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router. If an area tag is not specified, a null tag is assumed and the process is referenced with a null tag. If an area tag is specified, output is limited to the specified area. Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration.
	level-1	(Optional) Displays the IS-IS link-state database for Level 1.
	level-2	(Optional) Displays the IS-IS link-state database for Level 2.
	l1	(Optional) Abbreviation for the level-1 option.
	l2	(Optional) Abbreviation for the level-2 option.
	detail	(Optional) When specified, the contents of each link-state packet (LSP) are displayed. Otherwise, a summary display is provided.
	lspid	(Optional) Link-state protocol data unit (PDU) identifier. When specified, the contents of a single LSP are displayed by its ID number.

show isis spf-log

To display how often and why the router has run a full shortest path first (SPF) calculation, use the **show isis spf-log** user EXEC command.

```
show isis area-tag spf-log
```

Syntax Description	<i>area-tag</i>	
		Meaningful name for a routing process. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router. If an area tag is not specified, a null tag is assumed and the process is referenced with a null tag. If an area tag is specified, output is limited to the specified area.
		Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration.

show isis topology

To display a list of all connected routers in all areas, use the **show isis topology** EXEC command.

```
show isis area-tag topology
```

Syntax Description	<i>area-tag</i>	
		Meaningful name for a routing process. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router. If an area tag is not specified, a null tag is assumed and the process is referenced with a null tag. If an area tag is specified, output is limited to the specified area.
		Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration.

summary-address (IS-IS)

To create aggregate addresses for IS-IS or Open Shortest Path First (OSPF), use the **summary-address** router configuration command. To restore the default, use the **no** form of this command.

```
summary-address address mask {level-1 | level-1-2 | level-2} prefix mask
```

```
no summary-address address mask {level-1 | level-1-2 | level-2}
```

Syntax Description	<i>address</i>	
	<i>address</i>	Summary address designated for a range of addresses.
	<i>mask</i>	IP subnet mask used for the summary route.
	level-1	Only routes redistributed into Level 1 are summarized with the configured address/mask value.

level-1-2	Summary routes are applied when redistributing routes into Level 1 and Level 2 IS-IS, and when Level 2 IS-IS advertised Level 1 routes reachable in its area.
level-2	Routes learned by Level 1 routing are summarized into the Level 2 backbone with the configured address/mask value. Redistributed routes into Level 2 IS-IS will be summarized also.
<i>prefix</i>	IP route prefix for the destination.
<i>mask</i>	IP subnet mask used for the summary route.



BGP Commands

This chapter describes the function and syntax of the Border Gateway Protocol (BGP) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*.

aggregate-address

To create an aggregate entry in a BGP or multicast BGP database, use the **aggregate-address** command in address family or router configuration mode. To disable this function, use the **no** form of this command.

```
aggregate-address address mask [as-set] [summary-only] [suppress-map map-name]  
[advertise-map map-name] [attribute-map map-name]
```

```
no aggregate-address address mask [as-set] [summary-only] [suppress-map map-name]  
[advertise-map map-name] [attribute-map map-name]
```

Syntax Description

<i>address</i>	Aggregate address.
<i>mask</i>	Aggregate mask.
as-set	(Optional) Generates autonomous system set path information.
summary-only	(Optional) Filters all more-specific routes from updates.
suppress-map <i>map-name</i>	(Optional) Name of the route map used to select the routes to be suppressed.
advertise-map <i>map-name</i>	(Optional) Name of the route map used to select the routes to create AS_SET origin communities.
attribute-map <i>map-name</i>	(Optional) Name of route map used to set the attribute of the aggregate route.

auto-summary (BGP)

To restore the default behavior of automatic summarization of subnet routes into network-level routes, use the **auto-summary** command in address family or router configuration mode. To disable this feature and send subprefix routing information across classful network boundaries, use the **no** form of this command.

auto-summary

no auto-summary

Syntax Description This command has no arguments or keywords.

bgp always-compare-med

To allow the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems, use the **bgp always-compare-med** router configuration command. To disallow the comparison, use the **no** form of this command.

bgp always-compare-med

no bgp always-compare-med

Syntax Description This command has no arguments or keywords.

bgp bestpath as-path ignore

To prevent the router from considering as-path as a factor in the algorithm for choosing a route, use the **bgp bestpath as-path ignore** router configuration command. To allow the router to consider as-path in choosing a route, use the **no** form of this command.

bgp bestpath as-path ignore

no bgp bestpath as-path ignore

Syntax Description This command has no arguments or keywords.

bgp bestpath compare-routerid

To compare similar routes received from external BGP (eBGP) peers during the best path selection process and switch the best path to the route with the lowest router ID, use the **bgp bestpath compare-routerid** command in router configuration mode. To return the router to the default setting, use the **no** form of this command.

bgp bestpath compare-routerid

no bgp bestpath compare-routerid

Syntax Description This command has no arguments or keywords.

bgp bestpath med confed

To enable multiple exit discriminator (MED) comparison among paths learned from confederation peers, use the **bgp bestpath med confed** router configuration command. To prevent the software from considering the MED attribute in comparing paths, use the **no** form of this command.

bgp bestpath med confed

no bgp bestpath med confed

Syntax Description This command has no arguments or keywords.

bgp bestpath med missing-as-worst

To have Cisco IOS software consider a missing multiple exit discriminator (MED) attribute in a path as having a value of infinity, making the path without a MED value the least desirable path, use the **bgp bestpath med missing-as-worst** router configuration command. To return the router to the default (assign a value of 0 to the missing MED), use the **no** form of this command.

bgp bestpath med missing-as-worst

no bgp bestpath med missing-as-worst

Syntax Description This command has no arguments or keywords.

bgp client-to-client reflection

To restore route reflection from a BGP route reflector to clients, use the **bgp client-to-client reflection** command in address family or router configuration mode. To disable client-to-client reflection, use the **no** form of this command.

bgp client-to-client reflection

no bgp client-to-client reflection

Syntax Description This command has no arguments or keywords.

bgp cluster-id

To configure the cluster ID if the BGP cluster has more than one route reflector, use the **bgp cluster-id** router configuration command. To remove the cluster ID, use the **no** form of this command.

bgp cluster-id *cluster-id*

no bgp cluster-id *cluster-id*

Syntax Description *cluster-id* Cluster ID of this router acting as a route reflector; maximum of 4 bytes.

bgp confederation identifier

To specify a BGP confederation identifier, use the **bgp confederation identifier** router configuration command. To remove the confederation identifier, use the **no** form of this command.

bgp confederation identifier *as-number*

no bgp confederation identifier *as-number*

Syntax Description *as-number* Autonomous system number that internally includes multiple autonomous systems.

bgp confederation peers

To configure the autonomous systems that belong to the confederation, use the **bgp confederation peers** router configuration command. To remove an autonomous system from the confederation, use the **no** form of this command.

bgp confederation peers *as-number* [... *as-number*]

no bgp confederation peers *as-number* [... *as-number*]

Syntax Description

<i>as-number</i>	Autonomous system numbers for BGP peers that will belong to the confederation.
------------------	--

bgp dampening

To enable BGP route dampening or change various BGP route dampening factors, use the **bgp dampening** command in address family or router configuration mode. To disable the function or restore the default values, use the **no** form of this command.

bgp dampening [*half-life reuse suppress max-suppress-time*] [**route-map** *map-name*]

no bgp dampening [*half-life reuse suppress max-suppress-time*] [**route-map** *map-name*]

Syntax Description

<i>half-life</i>	(Optional) Time (in minutes) after which a penalty is decreased. Once the route has been assigned a penalty, the penalty is decreased by half after the half-life period (which is 15 minutes by default). The process of reducing the penalty happens every 5 seconds. The range of the half-life period is 1 to 45 minutes. The default is 15 minutes.
<i>reuse</i>	(Optional) If the penalty for a flapping route decreases enough to fall below this value, the route is unsuppressed. The process of unsuppressing routes occurs at 10-second increments. The range of the reuse value is from 1 to 20000; the default is 750.
<i>suppress</i>	(Optional) A route is suppressed when its penalty exceeds this limit. The range is from 1 to 20000; the default is 2000.
<i>max-suppress-time</i>	(Optional) Maximum time (in minutes) a route can be suppressed. The range is from 1 to 20000; the default is 4 times the <i>half-life</i> . If the <i>half-life</i> value is allowed to default, the maximum suppress time defaults to 60 minutes.
route-map <i>map-name</i>	(Optional) Name of route map that controls where BGP route dampening is enabled.

bgp default ipv4-unicast

To enable the IP version 4 (IPv4) unicast address family on all neighbors, use the **bgp default ipv4-unicast** command in address family or router configuration mode. To disable the IPv4 unicast address family on all neighbors, use the **no** form of this command.

bgp default ipv4-unicast

no bgp default ipv4-unicast

Syntax Description This command has no arguments or keywords.

bgp default local-preference

To change the default local preference value, use the **bgp default local-preference** router configuration command. To return to the default setting, use the **no** form of this command.

bgp default local-preference *number*

no bgp default local-preference *number*

Syntax Description *number* Local preference value from 0 to 4294967295. Higher is more preferred.

bgp deterministic med

To have Cisco IOS software compare the Multi Exit Discriminator (MED) variable when choosing among routes advertised by different peers in the same autonomous system, use the **bgp deterministic med** router configuration command. To disallow the comparison, use the **no** form of this command.

bgp deterministic med

no bgp deterministic med

Syntax Description This command has no arguments or keywords.

bgp fast-external-fallover

To immediately reset the BGP sessions of any directly adjacent external peers if the link used to reach them goes down, use the **bgp fast-external-fallover** command in address family or router configuration mode. To disable this function, use the **no** form of this command.

bgp fast-external-fallover

no bgp fast-external-fallover

Syntax Description This command has no arguments or keywords.

bgp log-neighbor-changes

To enable logging of BGP neighbor resets, use the **bgp log-neighbor-changes** command in address family or router configuration mode. To disable the logging of changes in BGP neighbor adjacencies, use the **no** form of this command.

bgp log-neighbor-changes

no bgp log-neighbor-changes

Syntax Description This command has no arguments or keywords.

bgp redistribute-internal

To allow the redistribution of internal Border Gateway Protocol (iBGP) routes into an Interior Gateway Protocol (IGP) such as Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF), use the **bgp redistribute-internal** command in address family configuration mode. To restore the system to the default condition, use the **no** form of this command.

bgp redistribute-internal

no bgp redistribute-internal

Syntax Description This command has no arguments or keywords.

bgp router-id

To configure a fixed router ID for a BGP-speaking router, use the **bgp router-id** router configuration command. To remove the **bgp router-id** command from the configuration file and restore the default value of the router ID, use the **no** form of this command.

```
bgp router-id {ip-address}
```

```
no bgp router-id {ip-address}
```

Syntax Description	<i>ip-address</i>	IP address of the router.
---------------------------	-------------------	---------------------------

clear ip bgp

To reset a BGP connection using BGP soft reconfiguration, use the **clear ip bgp** privileged EXEC command at the system prompt.

```
clear ip bgp [* | neighbor-address | peer-group-name] [soft [in | out]]
```

Syntax Description	*	Resets all current BGP sessions.
	<i>neighbor-address</i>	Resets only the identified BGP neighbor.
	<i>peer-group-name</i>	Resets the specified BGP peer group.
	soft	(Optional) Soft reset. Does not reset the session.
	in out	(Optional) Triggers inbound or outbound soft reconfiguration. If the in or out option is not specified, both inbound and outbound soft reset are triggered.

clear ip bgp dampening

To clear BGP route dampening information and unsuppress the suppressed routes, use the **clear ip bgp dampening** privileged EXEC command.

```
clear ip bgp dampening [ip-address network-mask]
```

Syntax Description	<i>ip-address</i>	(Optional) IP address of the network about which to clear dampening information.
	<i>network-mask</i>	(Optional) Network mask applied to the <i>ip-address</i> argument.

clear ip bgp external

To clear external Border Gateway Protocol (eBGP) peers, use the **clear ip bgp external** command in privileged EXEC mode.

```
clear ip bgp external [in | out]
```

```
clear ip bgp external [soft [in | out]]
```

```
clear ip bgp external {ipv4 | ipv6 {multicast | unicast {in | out | soft}}}
```

```
clear ip bgp external [vpn4 unicast {in | out | soft}]
```

Syntax Description	in out	(Optional) Triggers inbound or outbound soft reconfiguration.
	soft	(Optional) Triggers soft reconfiguration.
	ipv4 ipv6 vpn4	(Optional) Triggers reset of IPv4, IPv6, or VPNv4 address family session.
	multicast	(Optional) Triggers reset of IPv4 or IPv6 multicast address family session.
	unicast	(Optional) Triggers reset of IPv4, IPv6, or VPNv4 unicast family session.

clear ip bgp flap-statistics

To clear BGP flap statistics, use the **clear ip bgp flap-statistics** privileged EXEC command.

```
clear ip bgp ip-address flap-statistics [{regexp regexp} | {filter-list list-name} | {ip-address network-mask}]
```

Syntax Description	regexp regexp	(Optional) Clears flap statistics for all the paths that match the regular expression.
	filter-list list-name	(Optional) Clears flap statistics for all the paths that pass the access list.
	ip-address	(Optional) Clears flap statistics for a single entry at this IP address. If this argument is placed before flap-statistics , the router clears flap statistics for all paths from the neighbor at this address.
	network-mask	(Optional) Network mask applied to the <i>ip-address</i> argument.

clear ip bgp peer-group

To clear all the members of a BGP peer group, use the **clear ip bgp peer-group** privileged EXEC command.

```
clear ip bgp peer-group tag
```

Syntax Description	tag	Name of the BGP peer group to clear.
--------------------	-----	--------------------------------------

clear ip prefix-list

To reset the hit count of the prefix list entries, use the **clear ip prefix-list** privileged EXEC command.

```
clear ip prefix-list [prefix-list-name] [network/length]
```

Syntax Description		
	<i>prefix-list-name</i>	(Optional) The name of the prefix list from which the hit count is to be cleared.
	<i>network/length</i>	(Optional) The network number and length (in bits) of the network mask.

default-information originate (BGP)

To originate network 0.0.0.0 into the BGP, use the **default-information originate** command in address family or router configuration mode. To disable this function, use the **no** form of this command.

```
default-information originate
```

```
no default-information originate
```

Syntax Description	
	This command has no arguments or keywords.

default-metric (BGP)

To set default metric values for the BGP, use the **default-metric** command in address family or router configuration mode. To return to the default state, use the **no** form of this command.

```
default-metric number
```

```
no default-metric number
```

Syntax Description		
	<i>number</i>	Default metric value appropriate for the specified routing protocol.

distance bgp

To allow the use of external, internal, and local administrative distances that could be a better route than other external, internal, or local routes to a node, use the **distance bgp** command in address family or router configuration mode. To return to the default values, use the **no** form of this command.

```
distance bgp external-distance internal-distance local-distance
```

```
no distance bgp
```

Syntax Description

<i>external-distance</i>	Administrative distance for BGP external routes. External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Acceptable values are from 1 to 255. The default is 20. Routes with a distance of 255 are not installed in the routing table.
<i>internal-distance</i>	Administrative distance for BGP internal routes. Internal routes are those routes that are learned from another BGP entity within the same autonomous system. Acceptable values are from 1 to 255. The default is 200. Routes with a distance of 255 are not installed in the routing table.
<i>local-distance</i>	Administrative distance for BGP local routes. Local routes are those networks listed with a network router configuration command, often as back doors, for that router or for networks that are being redistributed from another process. Acceptable values are from 1 to 255. The default is 200. Routes with a distance of 255 are not installed in the routing table.

distribute-list in

To filter networks received in updates, use the **distribute-list in** command in address family or router configuration mode. To disable this function, use the **no** form of this command.

```
distribute-list {access-list-number | prefix prefix-list-name} in [interface-type interface-number]
```

```
no distribute-list {access-list-number | prefix prefix-list-name} in [interface-type interface-number]
```

Syntax Description

<i>access-list-number</i>	Standard IP access list number. The list defines which networks are to be received and which are to be suppressed in routing updates.
prefix <i>prefix-list-name</i>	Name of a prefix list. The list defines which networks are to be received and which are to be suppressed in routing updates, based upon matching the network prefix to the prefixes in the list.
in	Applies the access list to incoming routing updates.
<i>interface-type</i>	(Optional) Interface type.
<i>interface-number</i>	(Optional) Interface number on which the access list should be applied to incoming updates. If no interface is specified, the access list will be applied to all incoming updates.

distribute-list out

To suppress networks from being advertised in updates, use the **distribute-list out** command in address family or router configuration mode. To disable this function, use the **no** form of this command.

```
distribute-list {access-list-number | prefix prefix-list-name} out [interface-name | routing-process | as-number]
```

```
no distribute-list {access-list-number | prefix prefix-list-name} out [interface-name | routing-process | as-number]
```

Syntax Description		
	<i>access-list-number</i>	Standard IP access list number. The list defines which networks are to be received and which are to be suppressed in routing updates.
	prefix <i>prefix-list-name</i>	Name of a prefix list. The list defines which networks are to be received and which are to be suppressed in routing updates, based upon matching the network prefix to the prefixes in the list.
	out	Applies the access list to outgoing routing updates.
	<i>interface-name</i>	(Optional) Name of a particular interface.
	<i>routing-process</i>	(Optional) Name of a particular routing process, or the keyword static or connected .
	<i>as-number</i>	(Optional) Autonomous system number.

ip as-path access-list

To define a BGP autonomous system path access list, use the **ip as-path access-list** global configuration command. To disable use of the access list, use the **no** form of this command.

```
ip as-path access-list access-list-number {permit | deny} as-regexp
```

```
no ip as-path access-list access-list-number
```

Syntax Description		
	<i>access-list-number</i>	Integer from 1 to 199 that indicates the regular expression access list number.
	permit	Permits access for matching conditions.
	deny	Denies access to matching conditions.
	<i>as-regexp</i>	Autonomous system in the access list using a regular expression. Refer to the “Regular Expressions” appendix in the <i>Cisco IOS Terminal Services Configuration Guide</i> for information about forming regular expressions.

ip bgp-community new-format

To display BGP communities in the format AA:NN (autonomous system-community number/2-byte number), use the **ip bgp-community new-format** global configuration command. To reenabte the previous display format for BGP communities (one 32-bit number), use the **no** form of this command.

```
ip bgp-community new-format
```

```
no ip bgp-community new-format
```

Syntax Description	
	This command has no argument or keywords.

ip community-list

To create a community list for BGP and control access to it, use the **ip community-list** global configuration command. To delete the community list, use the **no** form of this command.

```
ip community-list community-list-number {permit | deny} community-number
```

```
no ip community-list community-list-number
```

Syntax Description	<i>community-list-number</i>	Integer from 1 to 99 that identifies one or more permit or deny groups of communities.
	permit	Permits access for a matching condition.
	deny	Denies access for a matching condition.
	<i>community-number</i>	Community number configured by a set community command. Valid value is one of the following: <ul style="list-style-type: none"> • A number from 1 to 4294967200. You can specify a single number or multiple numbers separated by a space. • internet—The Internet community. • no-export—Routes with this community are sent to peers in other subautonomous systems within a confederation. Do not advertise this route to an eBGP peer. External systems are those outside the confederation. If there is no confederation, an external system is any eBGP peer. • local-as—Send this route to peers in other subautonomous systems within the local confederation. Do not advertise this route to an external system. • no-advertise—Do not advertise this route to any peer (internal or external).

ip prefix-list

To create an entry in a prefix list, use the **ip prefix-list** global configuration command. To delete the entry, use the **no** form of this command.

```
ip prefix-list list-name [seq seq-value] {deny | permit network/length}[ge ge-value] [le le-value]
```

```
no ip prefix-list list-name [seq seq-value] {deny | permit network/length}[ge ge-value] [le le-value]
```

Syntax Description	<i>list-name</i>	Name of a prefix list.
	seq	(Optional) Applies the sequence number to the prefix list entry being created or deleted.
	<i>seq-value</i>	(Optional) Specifies the sequence number for the prefix list entry.
	deny	Denies access for a matching condition.

permit	Permits access for a matching condition.
<i>network/length</i>	(Mandatory) The network number and length (in bits) of the network mask.
ge	(Optional) Applies the <i>ge-value</i> to the range specified.
<i>ge-value</i>	(Optional) Specifies the lesser value of a range (the “from” portion of the range description).
le	(Optional) Applies the <i>le-value</i> to the range specified.
<i>le-value</i>	(Optional) Specifies the greater value of a range (the “to” portion of the range description).

ip prefix-list description

To add a text description of a prefix list, use the **ip prefix-list description** global configuration command. To remove the text description, use the **no** form of this command.

ip prefix-list *list-name* **description** *text*

no ip prefix-list *list-name* **description** *text*

Syntax Description

<i>list-name</i>	Prefix list name.
<i>text</i>	Text description of the prefix list.

ip prefix-list sequence-number

To enable the generation of sequence numbers for entries in a prefix list, use the **ip prefix-list sequence-number** global configuration command. To remove the text description, use the **no** form of this command.

ip prefix-list **sequence-number**

no ip prefix-list **sequence-number**

Syntax Description

This command has no arguments or keywords.

match as-path

To match a BGP autonomous system path access list, use the **match as-path** route-map configuration command. To remove a path list entry, use the **no** form of this command.

match as-path *path-list-number*

no match as-path *path-list-number*

Syntax Description

<i>path-list-number</i>	Autonomous system path access list. An integer from 1 to 199.
-------------------------	---

match community-list

To match a BGP community, use the **match community-list** route-map configuration command. To remove the community list entry, use the **no** form of this command.

match community-list *community-list-number* [**exact**]

no match community-list *community-list-number* [**exact**]

Syntax Description		
	<i>community-list-number</i>	Community list number in the range from 1 to 99.
	exact	(Optional) Indicates that an exact match is required. All of the communities and only those communities in the community list must be present.

maximum-paths

To control the maximum number of parallel routes an IP routing protocol can support, use the **maximum-paths** command in address family or router configuration mode. To restore the default value, use the **no** form of this command.

maximum-paths *number*

no maximum-paths

Syntax Description		
	<i>number</i>	Maximum number of parallel routes an IP routing protocol installs in a routing table, in the range from 1 to 6.

neighbor advertisement-interval

To set the minimum interval between the sending of BGP routing updates, use the **neighbor advertisement-interval** command in address family or router configuration mode. To remove an entry, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **advertisement-interval** *seconds*

no neighbor {*ip-address* | *peer-group-name*} **advertisement-interval** *seconds*

Syntax Description		
	<i>ip-address</i>	IP address of the number.
	<i>peer-group-name</i>	Name of a BGP peer group.
	<i>seconds</i>	Time (in seconds) is specified by an integer from 0 to 600.

neighbor advertise-map non-exist-map

To configure a router to conditionally advertise routes with Border Gateway Protocol (BGP), use the **neighbor advertise-map non-exist-map** router configuration command. To disable the BGP Conditional Advertisement feature, use the **no** form of this command.

```
neighbor {ip-address} advertise-map {map1-name} non-exist-map {map2-name}
```

```
no neighbor {ip-address} advertise-map {map1-name} non-exist-map {map2-name}
```

Syntax Description

<i>ip-address</i>	Specifies the IP address of the router that should receive conditional advertisements for a given set of routes.
<i>map-name</i>	Specifies the name of the advertise-map and the non-exist-map.

neighbor default-originate

To allow a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route, use the **neighbor default-originate** command in address family or router configuration mode. To send no route as a default, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} default-originate [route-map map-name]
```

```
no neighbor {ip-address | peer-group-name} default-originate [route-map map-name]
```

Syntax Description

<i>ip-address</i>	IP address of the Neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
route-map <i>map-name</i>	(Optional) Name of the route map. The route map allows route 0.0.0.0 to be injected conditionally.

neighbor description

To associate a description with a neighbor, use the **neighbor description** router configuration command. To remove the description, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} description text
```

```
no neighbor {ip-address | peer-group-name} description [text]
```

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>text</i>	Text (up to 80 characters) that describes the neighbor.

neighbor distribute-list

To distribute BGP neighbor information as specified in an access list, use the **neighbor distribute-list** command in address family or router configuration mode. To remove an entry, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} distribute-list {access-list-number | access-list-name
prefix-list-name} {in | out}
```

```
no neighbor {ip-address | peer-group-name} distribute-list {access-list-number |
access-list-name prefix-list-name} {in | out}
```

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>access-list-number</i> <i>access-list-name</i>	Number or name of a standard or extended access list. It can be an integer from 1 to 199.
<i>prefix-list-name</i>	Name of a BGP prefix list.
in	Access list is applied to incoming advertisements to that neighbor.
out	Access list is applied to outgoing advertisements from that neighbor.

neighbor ebgp-multihop

To accept and attempt BGP connections to external peers residing on networks that are not directly connected, use the **neighbor ebgp-multihop** router configuration command. To return to the default, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} ebgp-multihop [ttl]
```

```
no neighbor {ip-address | peer-group-name} ebgp-multihop
```

Syntax Description

<i>ip-address</i>	IP address of the BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>ttl</i>	(Optional) Time-to-live in the range from 1 to 255 hops.

neighbor filter-list

To set up a BGP filter, use the **neighbor filter-list** command in address family or router configuration mode. To disable this function, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} filter-list access-list-number {in | out}
```

```
no neighbor {ip-address | peer-group-name} filter-list access-list-number {in | out}
```

Syntax Description		
	<i>ip-address</i>	IP address of the neighbor.
	<i>peer-group-name</i>	Name of a BGP peer group.
	<i>access-list-number</i>	Number of an autonomous system path access list. You define this access list with the ip as-path access-list command.
	in	Access list applied to incoming routes.
	out	Access list applied to outgoing routes.

neighbor local-as

To allow customization of the autonomous system number for external Border Gateway Protocol (eBGP) peer groupings, use the **neighbor local-as** command in address family or router configuration mode. To disable this function, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} local-as as-number
```

```
no neighbor {ip-address | peer-group-name} local-as as-number
```

Syntax Description		
	<i>ip-address</i>	IP address of the local BGP-speaking neighbor.
	<i>peer-group-name</i>	Name of a BGP peer group.
	<i>as-number</i>	Valid autonomous system number from 1 to 65535. Do not specify the autonomous system number to which the neighbor belongs.

neighbor maximum-prefix

To control how many prefixes can be received from a neighbor, use the **neighbor maximum-prefix** router configuration command. To disable this function, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} maximum-prefix maximum [threshold]  
[warning-only]
```

```
no neighbor {ip-address | peer-group-name} maximum-prefix maximum
```

Syntax Description		
	<i>ip-address</i>	IP address of the neighbor.
	<i>peer-group-name</i>	Name of a BGP peer group.
	<i>maximum</i>	Maximum number of prefixes allowed from this neighbor.
	<i>threshold</i>	(Optional) Integer specifying at what percentage of <i>maximum</i> the router starts to generate a warning message. The range is from 1 to 100; the default is 75 (percent).
	warning-only	(Optional) Allows the router to generate a log message when the <i>maximum</i> is exceeded, instead of terminating the peering.

neighbor next-hop-self

To configure the router as the next hop for a BGP-speaking neighbor or peer group, use the **neighbor next-hop-self** router configuration command. To disable this feature, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} next-hop-self
```

```
no neighbor {ip-address | peer-group-name} next-hop-self
```

Syntax Description

<i>ip-address</i>	IP address of the BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.

neighbor password

To enable Message Digest 5 (MD5) authentication on a TCP connection between two BGP peers, use the **neighbor password** router configuration command. To disable this function, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} password string
```

```
no neighbor {ip-address | peer-group-name} password
```

Syntax Description

<i>ip-address</i>	IP address of the BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>string</i>	Case-sensitive password of up to 80 characters. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces. You cannot specify a password in the format <i>number-space-anything</i> . The space after the number causes problems.

neighbor peer-group (assigning members)

To configure a BGP neighbor to be a member of a peer group, use the **neighbor peer-group** command in address family or router configuration mode. To remove the neighbor from the peer group, use the **no** form of this command.

```
neighbor ip-address peer-group peer-group-name
```

```
no neighbor ip-address peer-group peer-group-name
```

Syntax Description

<i>ip-address</i>	IP address of the BGP neighbor that belongs to the peer group specified by the <i>peer-group-name</i> argument.
<i>peer-group-name</i>	Name of the BGP peer group to which this neighbor belongs.

neighbor peer-group (creating)

To create a BGP or multiprotocol BGP peer group, use the **neighbor peer-group** command in address family or router configuration mode. To remove the peer group and all of its members, use the **no** form of this command.

neighbor *peer-group-name* **peer-group**

no neighbor *peer-group-name* **peer-group**

Syntax Description		
	<i>peer-group-name</i>	Name of the BGP peer group.

neighbor prefix-list

To distribute BGP neighbor information as specified in a prefix list, use the **neighbor prefix-list** command in address family or router configuration mode. To remove an entry, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **prefix-list** *prefix-list-name* {**in** | **out**}

no neighbor {*ip-address* | *peer-group-name*} **prefix-list** *prefix-list-name* {**in** | **out**}

Syntax Description		
	<i>ip-address</i>	IP address of neighbor.
	<i>peer-group-name</i>	Name of a BGP peer group.
	<i>prefix-list-name</i>	Name of a prefix list.
	in	Access list is applied to incoming advertisements to that neighbor.
	out	Access list is applied to outgoing advertisements from that neighbor.

neighbor remote-as

To add an entry to the BGP or multiprotocol BGP neighbor table, use the **neighbor remote-as** router configuration command. To remove an entry from the table, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **remote-as** *as-number*

no neighbor {*ip-address* | *peer-group-name*} **remote-as** *as-number*

Syntax Description		
	<i>ip-address</i>	IP address of the neighbor.
	<i>peer-group-name</i>	Name of a BGP peer group.
	<i>as-number</i>	Autonomous system to which the neighbor belongs.

neighbor remove-private-as

To remove private autonomous system numbers from the autonomous system path, a list of autonomous system numbers that a route passes through to reach a BGP peer, in outbound routing updates, use the **neighbor remove-private-as** router configuration command. To disable this function, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} remove-private-as
```

```
no neighbor {ip-address | peer-group-name} remove-private-as
```

Syntax Description		
	<i>ip-address</i>	IP address of the BGP-speaking neighbor.
	<i>peer-group-name</i>	Name of a BGP peer group.

neighbor route-map

To apply a route map to incoming or outgoing routes, use the **neighbor route-map** command in address family or router configuration mode. To remove a route map, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} route-map map-name {in | out}
```

```
no neighbor {ip-address | peer-group-name} route-map map-name {in | out}
```

Syntax Description		
	<i>ip-address</i>	IP address of the neighbor.
	<i>peer-group-name</i>	Name of a BGP or multiprotocol BGP peer group.
	<i>map-name</i>	Name of a route map.
	in	Applies route map to incoming routes.
	out	Applies route map to outgoing routes.

neighbor route-reflector-client

To configure the router as a BGP route reflector and configure the specified neighbor as its client, use the **neighbor route-reflector-client** command in address family or router configuration mode. To indicate that the neighbor is not a client, use the **no** form of this command.

```
neighbor ip-address route-reflector-client
```

```
no neighbor ip-address route-reflector-client
```

Syntax Description		
	<i>ip-address</i>	IP address of the BGP neighbor being identified as a client.

neighbor send-community

To specify that a communities attribute should be sent to a BGP neighbor, use the **neighbor send-community** command in address family or router configuration mode. To remove the entry, use the **no** form of this command.

neighbor { *ip-address* | *peer-group-name* } **send-community**

no neighbor { *ip-address* | *peer-group-name* } **send-community**

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.

neighbor shutdown

To disable a neighbor or peer group, use the **neighbor shutdown** router configuration command. To reenabte the neighbor or peer group, use the **no** form of this command.

neighbor { *ip-address* | *peer-group-name* } **shutdown**

no neighbor { *ip-address* | *peer-group-name* } **shutdown**

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.

neighbor soft-reconfiguration

To configure the Cisco IOS software to start storing updates, use the **neighbor soft-reconfiguration** router configuration command. To not store received updates, use the **no** form of this command.

neighbor { *ip-address* | *peer-group-name* } **soft-reconfiguration** [**inbound**]

no neighbor { *ip-address* | *peer-group-name* } **soft-reconfiguration** [**inbound**]

Syntax Description

<i>ip-address</i>	IP address of the BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
inbound	(Optional) Indicates that the update to be stored is an incoming update.

neighbor timers

To set the timers for a specific BGP peer or peer group, use the **neighbor timers** router configuration command. To clear the timers for a specific BGP peer or peer group, use the **no** form of this command.

neighbor [*ip-address* | *peer-group-name*] **timers** *keepalive* *holdtime*

no neighbor [*ip-address* | *peer-group-name*] **timers** *keepalive* *holdtime*

Syntax Description	
<i>ip-address</i>	(Optional) A BGP peer or peer group IP address.
<i>peer-group-name</i>	(Optional) Name of the BGP peer group.
<i>keepalive</i>	Frequency (in seconds) with which the Cisco IOS software sends <i>keepalive</i> messages to its peer. The default is 60 seconds.
<i>holdtime</i>	Interval (in seconds) after not receiving a <i>keepalive</i> message that the software declares a peer dead. The default is 180 seconds.

neighbor unsuppress-map

To selectively advertise routes previously suppressed by the **aggregate-address** command, use the **neighbor unsuppress-map** command in address family or router configuration mode. To restore the system to the default condition, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **unsuppress-map** *route-map-name*

no neighbor {*ip-address* | *peer-group-name*} **unsuppress-map** *route-map-name*

Syntax Description	
<i>ip-address</i>	IP address of the BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>route-map-name</i>	Name of a route map.

neighbor update-source

To have the Cisco IOS software allow internal BGP (iBGP) sessions to use any operational interface for TCP connections, use the **neighbor update-source** router configuration command. To restore the interface assignment to the closest interface, which is called the *best local address*, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **update-source** *interface-type*

no neighbor {*ip-address* | *peer-group-name*} **update-source** *interface-type*

Syntax Description	
<i>ip-address</i>	IP address of the BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>interface-type</i>	Interface type.

neighbor version

To configure the Cisco IOS software to accept only a particular BGP version, use the **neighbor version** router configuration command. To use the default version level of a neighbor, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **version** *number*

no neighbor {*ip-address* | *peer-group-name*} **version** *number*

Syntax Description		
	<i>ip-address</i>	IP address of the BGP-speaking neighbor.
	<i>peer-group-name</i>	Name of a BGP peer group.
	<i>number</i>	BGP version number. The version can be set to 2 to force the software to only use Version 2 with the specified neighbor. The default is to use Version 4 and dynamically negotiate down to Version 2 if requested.

neighbor weight

To assign a weight to a neighbor connection, use the **neighbor weight** command in address family or router configuration mode. To remove a weight assignment, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **weight** *number*

no neighbor {*ip-address* | *peer-group-name*} **weight** *number*

Syntax Description		
	<i>ip-address</i>	IP address of the neighbor.
	<i>peer-group-name</i>	Name of a BGP peer group.
	<i>number</i>	Weight to assign. Acceptable values are from 0 to 65535.

network (BGP and multiprotocol BGP)

To specify the networks to be advertised by the BGP and multiprotocol BGP routing processes, use the **network** command in address family or router configuration mode. To remove an entry, use the **no** form of this command.

network *network-number* [**mask** *network-mask*]

no network *network-number* [**mask** *network-mask*]

Syntax Description		
	<i>network-number</i>	Network that BGP or multiprotocol BGP will advertise.
	mask	(Optional) Network or subnetwork mask.
	<i>network-mask</i>	(Optional) Network mask address.

network backdoor

To specify a backdoor route to a BGP-learned prefix that provides better information about the network, use the **network backdoor** command in address family or router configuration mode. To remove an address from the list, use the **no** form of this command.

network *ip-address* **backdoor**

no network *ip-address* **backdoor**

Syntax Description

<i>ip-address</i>	IP address of the network to which you want a backdoor route.
-------------------	---

network weight

To assign an absolute weight to a BGP network, use the **network weight** router configuration command. To delete an entry, use the **no** form of the command.

network *ip-address network-mask* **weight** *number* [**route-map** *map-name*]

no network *ip-address network-mask* **weight** *number* [**route-map** *map-name*]

Syntax Description

<i>ip-address</i>	IP address of the network.
<i>network-mask</i>	Network mask of the network.
<i>number</i>	Absolute weight, or importance. It can be an integer from 0 to 65535.
route-map <i>map-name</i>	(Optional) Name of a route map.

router bgp

To configure the BGP routing process, use the **router bgp** global configuration command. To remove a routing process, use the **no** form of this command.

router bgp *as-number*

no router bgp *as-number*

Syntax Description

<i>as-number</i>	Number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along.
------------------	---

set as-path

To modify an autonomous system path for BGP routes, use the **set as-path** route-map configuration command. To not modify the autonomous system path, use the **no** form of this command.

```
set as-path {tag | prepend as-path-string}
```

```
no set as-path {tag | prepend as-path-string}
```

Syntax Description	tag	Converts the tag of a route into an autonomous system path. Applies only when redistributing routes into BGP.
	prepend as-path-string	Appends the string following the keyword prepend to the autonomous system path of the route that is matched by the route map. Applies to inbound and outbound BGP route maps.

set comm-list delete

To remove communities from the community attribute of an inbound or outbound update, use the **set comm-list delete** route-map configuration command. To negate a previous **set comm-list delete** command, use the **no** form of this command.

```
set comm-list community-list-number delete
```

```
no set comm-list community-list-number delete
```

Syntax Description	community-list-number	A standard or extended community list number.
--------------------	-----------------------	---

set community

To set the BGP communities attribute, use the **set community** route map configuration command. To delete the entry, use the **no** form of this command.

```
set community {community-number [additive]} | none
```

```
no set community {community-number [additive]} | none
```

Syntax Description	community-number	Valid values are from 1 to 4294967200, no-export , or no-advertise .
	additive	(Optional) Adds the community to the already existing communities.
	none	Removes the community attribute from the prefixes that pass the route map.

set dampening

To set the BGP route dampening factors, use the **set dampening** route map configuration command. To disable this function, use the **no** form of this command.

set dampening *half-life reuse suppress max-suppress-time*

no set dampening

Syntax Description		
<i>half-life</i>		Time (in minutes) after which a penalty is decreased. Once the route has been assigned a penalty, the penalty is decreased by half after the half life period (which is 15 minutes by default). The process of reducing the penalty happens every 5 seconds. The range of the half life period is from 1 to 45 minutes. The default is 15 minutes.
<i>reuse</i>		Unsuppresses the route if the penalty for a flapping route decreases enough to fall below this value. The process of unsuppressing routes occurs at 10-second increments. The range of the reuse value is from 1 to 20000; the default is 750.
<i>suppress</i>		Suppresses a route when its penalty exceeds this limit. The range is from 1 to 20000; the default is 2000.
<i>max-suppress-time</i>		Maximum time (in minutes) a route can be suppressed. The range is from 1 to 20000; the default is four times the <i>half-life</i> value. If the <i>half-life</i> value is allowed to default, the maximum suppress time defaults to 60 minutes.

set ip next-hop (BGP)

To indicate where to output packets that pass a match clause of a route map for policy routing, use the **set ip next-hop** route-map configuration command. To delete an entry, use the **no** form of this command.

set ip next-hop *ip-address* [... *ip-address*] [**peer-address**]

no set ip next-hop *ip-address* [... *ip-address*] [**peer-address**]

Syntax Description		
<i>ip-address</i>		IP address of the next hop to which packets are output. It need not be an adjacent router.
peer-address		(Optional) Sets the next hop to be the BGP peering address.

set metric-type internal

To set the Multi Exit Discriminator (MED) value on prefixes advertised to external BGP (eBGP) neighbors to match the Interior Gateway Protocol (IGP) metric of the next hop, use the **set metric-type internal** route-map configuration command. To return to the default, use the **no** form of this command.

set metric-type internal

no set metric-type internal

Syntax Description This command has no arguments or keywords.

set origin (BGP)

To set the BGP origin code, use the **set origin** route-map configuration command. To delete an entry, use the **no** form of this command.

set origin { **igp** | **egp** *as-number* | **incomplete** }

no set origin { **igp** | **egp** *as-number* | **incomplete** }

Syntax Description		
igp		Remote Interior Gateway Protocol (IGP) system.
egp		Local Exterior Gateway Protocol (EGP) system.
<i>as-number</i>		Remote autonomous system number. This is an integer from 0 to 65535.
incomplete		Unknown heritage.

set weight

To specify the BGP weight for the routing table, use the **set weight** route-map configuration command. To delete an entry, use the **no** form of this command.

set weight *number*

no set weight *number*

Syntax Description	<i>number</i>	
		Weight value. It can be an integer from 0 to 65535.

show ip bgp

To display entries in the BGP routing table, use the **show ip bgp** EXEC command.

show ip bgp [*network*] [*network-mask*] [**longer-prefixes**]

Syntax Description	<i>network</i>	(Optional) Network number, entered to display a particular network in the BGP routing table.
	<i>network-mask</i>	(Optional) Displays all BGP routes matching the address and mask pair.
	longer-prefixes	(Optional) Displays the route and more specific routes.

show ip bgp cidr-only

To display routes with nonnatural network masks (that is, classless interdomain routing, or CIDR), use the **show ip bgp cidr-only EXEC** command.

```
show ip bgp cidr-only
```

Syntax Description This command has no arguments or keywords.

show ip bgp community

To display routes that belong to specified BGP communities, use the **show ip bgp community EXEC** command.

```
show ip bgp community community-number [exact]
```

Syntax Description	<i>community-number</i>	Valid value is a community number in the range from 1 to 4294967200, or AA:NN (autonomous system-community number/2-byte number), internet , no-export , local-as , or no-advertise .
	exact	(Optional) Displays only routes that have the same specified communities.

show ip bgp community-list

To display routes that are permitted by the BGP community list, use the **show ip bgp community-list EXEC** command.

```
show ip bgp community-list community-list-number [exact]
```

Syntax Description	<i>community-list-number</i>	Community list number in the range from 1 to 99.
	exact	(Optional) Displays only routes that have an exact match.

show ip bgp dampened-paths

To display BGP dampened routes, use the **show ip bgp dampened-paths** EXEC command.

```
show ip bgp dampened-paths
```

Syntax Description This command has no arguments or keywords.

show ip bgp filter-list

To display routes that conform to a specified filter list, use the **show ip bgp filter-list** EXEC command.

```
show ip bgp filter-list access-list-number
```

Syntax Description

<i>access-list-number</i>	Number of an autonomous system path access list. It can be a number from 1 to 199.
---------------------------	--

show ip bgp flap-statistics

To display BGP flap statistics, use the **show ip bgp flap-statistics** EXEC command.

```
show ip bgp flap-statistics [{regexp regexp} | {filter-list access-list} | {ip-address mask  
[longer-prefix]}]
```

Syntax Description

regexp <i>regexp</i>	(Optional) Clears flap statistics for all the paths that match the regular expression.
filter-list <i>access-list</i>	(Optional) Clears flap statistics for all the paths that pass the access list.
<i>ip-address</i>	(Optional) Clears flap statistics for a single entry at this IP address.
<i>mask</i>	(Optional) Network mask applied to the value.
longer-prefix	(Optional) Displays flap statistics for more specific entries.

show ip bgp inconsistent-as

To display routes with inconsistent originating autonomous systems, use the **show ip bgp inconsistent-as** EXEC command.

```
show ip bgp inconsistent-as
```

Syntax Description This command has no arguments or keywords.

show ip bgp ipv4

To display entries in the IP version 4 (IPv4) Border Gateway Protocol (BGP) routing table, use the **show ip bgp ipv4** command in EXEC mode.

```
show ip bgp ipv4 {multicast | unicast}
```

Syntax Description	multicast	Displays entries for multicast routes.
	unicast	Displays entries for unicast routes.

show ip bgp neighbors

To display information about the TCP and BGP connections to neighbors, use the **show ip bgp neighbors** EXEC command.

```
show ip bgp neighbors [neighbor-address] [received-routes | routes | advertised-routes | {paths  
  regexp} | dampened-routes]
```

Syntax Description	<i>neighbor-address</i>	(Optional) Address of the neighbor whose routes you have learned from. If you omit this argument, all neighbors are displayed.
	received-routes	(Optional) Displays all received routes (both accepted and rejected) from the specified neighbor.
	routes	(Optional) Displays all routes that are received and accepted. This is a subset of the output from the received-routes keyword.
	advertised-routes	(Optional) Displays all the routes the router has advertised to the neighbor.
	paths <i>regexp</i>	(Optional) Regular expression that is used to match the paths received.
	dampened-routes	(Optional) Displays the dampened routes to the neighbor at the IP address specified.

show ip bgp paths

To display all the BGP paths in the database, use the **show ip bgp paths** EXEC command.

```
show ip bgp paths
```

Syntax Description	This command has no arguments or keywords.
--------------------	--

show ip bgp peer-group

To display information about BGP peer groups, use the **show ip bgp peer-group** EXEC command.

```
show ip bgp peer-group [peer-group-name] [summary]
```

Syntax Description	<i>peer-group-name</i>	(Optional) Displays information about that specific peer group.
	summary	(Optional) Displays a summary of the status of all the members of a peer group.

show ip bgp regexp

To display routes matching the autonomous system path regular expression, use the **show ip bgp regexp** EXEC command.

```
show ip bgp regexp regexp
```

Syntax Description	<i>regexp</i>	Regular expression to match the BGP autonomous system paths.
---------------------------	---------------	--

show ip bgp summary

To display the status of all BGP connections, use the **show ip bgp summary** EXEC command.

```
show ip bgp summary
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--

show ip prefix-list

To display information about a prefix list or prefix list entries, use the **show ip prefix-list** command user and privileged EXEC mode.

```
show ip prefix-list [detail | summary] prefix-list-name [network/length] [seq sequence-number]  
[longer] [first-match]
```

Syntax Description	detail summary	(Optional) Displays detailed or summarized information about all prefix lists.
	<i>prefix-list-name</i>	(Optional) The name of a specific prefix list.
	<i>network/length</i>	(Optional) The network number and length (in bits) of the network mask.
	seq	(Optional) Applies the sequence number to the prefix list entry.
	<i>sequence-number</i>	(Optional) The sequence number of the prefix list entry.
	longer	(Optional) Displays all entries of a prefix list that are more specific than the given <i>network/length</i> .
	first-match	(Optional) Displays the entry of a prefix list that matches the given <i>network/length</i> .

synchronization

To enable the synchronization between BGP and your Interior Gateway Protocol (IGP) system, use the **synchronization** command in address family or router configuration mode. To enable the Cisco IOS software to advertise a network route without waiting for the IGP, use the **no** form of this command.

synchronization

no synchronization

Syntax Description This command has no arguments or keywords.

table-map

To modify metric and tag values when the IP routing table is updated with BGP learned routes, use the **table-map** command in address family or router configuration mode. To disable this function, use the **no** form of the command.

table-map *map-name*

no table-map *map-name*

Syntax Description	<i>map-name</i>	Route map name, from the route-map command.
---------------------------	-----------------	--

timers bgp

To adjust BGP network timers, use the **timers bgp** router configuration command. To reset the BGP timing defaults, use the **no** form of this command.

timers bgp *keepalive holdtime*

no timers bgp

Syntax Description	<i>keepalive</i>	Frequency (in seconds) with which the Cisco IOS software sends <i>keepalive</i> messages to its peer. The default is 60 seconds.
	<i>holdtime</i>	Interval (in seconds) after not receiving a <i>keepalive</i> message that the software declares a peer dead. The default is 180 seconds.



Multiprotocol BGP Extensions for IP Multicast Commands

This chapter describes the function and syntax of the multiprotocol BGP commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*.

Commands in this chapter that have been replaced by new or existing commands are no longer documented. Table 20 maps the old commands to their replacements.

Table 20 Mapping Old Commands to Replacement Commands

Old Command	Replacement Command
<code>distance mbgp</code>	<code>distance bgp</code>
<code>match nlri</code>	<code>address-family ipv4</code> <code>address-family vpnv4</code>
<code>set nlri</code>	<code>address-family ipv4</code> or <code>address-family vpnv4</code>
<code>show ip mbgp</code>	<code>show ip bgp ipv4 multicast</code>
<code>show ip mbgp summary</code>	<code>show ip bgp ipv4 multicast summary</code>

address-family ipv4

To enter address family configuration mode for configuring routing sessions such as BGP that use standard IP Version 4 address prefixes, use the **address-family ipv4** router configuration command. To disable address family configuration mode, use the **no** form of this command.

```
address-family ipv4 [multicast | unicast | vrf vrf-name]
```

```
no address-family ipv4 [multicast | unicast | vrf vrf-name]
```

Syntax Description

<code>multicast</code>	(Optional) Specifies IP Version 4 multicast address prefixes.
<code>unicast</code>	(Optional) Specifies IP Version 4 unicast address prefixes.

vrf <i>vrf-name</i>	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance to associate with subsequent IP Version 4 address family configuration mode commands.
----------------------------	--

address-family vpnv4

To enter address family configuration mode for configuring routing sessions, such as BGP, that use standard Virtual Private Network (VPN) Version 4 address prefixes, use the **address-family vpnv4** router configuration command. To disable address family configuration mode, use the **no** form of this command.

address-family vpnv4 [**unicast**]

no address-family vpnv4 [**unicast**]

Syntax Description

unicast	(Optional) Specifies VPN Version 4 unicast address prefixes.
----------------	--

distance mbgp

The **distance mbgp** command is replaced by the **distance bgp** command. See the description of the **distance bgp** command in the “BGP Commands” chapter for more information.

ip dvmrp metric

To configure the metric associated with a set of destinations for Distance Vector Multicast Routing Protocol (DVMRP) reports, use the **ip dvmrp metric** interface configuration command. (Note that this command has two different syntax possibilities.) To disable this function, use the **no** form of this command.

ip dvmrp metric *metric* [**route-map** *map-name*] [**mbgp**] [**list** *access-list-number*] [[*protocol process-id*] | **dvmrp**]

no ip dvmrp metric *metric* [**route-map** *map-name*] [**mbgp**] [**list** *access-list-number*] [[*protocol process-id*] | **dvmrp**]

Syntax Description

<i>metric</i>	Metric associated with a set of destinations for DVMRP reports. It can be a value from 0 to 32. A value of 0 means that the route is not advertised. A value of 32 is equivalent to infinity (unreachable).
route-map <i>map-name</i>	(Optional) Name of a route map. If you specify this argument, only the destinations that match the route map are reported with the configured metric. Unicast routes are subject to route map conditions before being injected into DVMRP. Route maps cannot be used for DVMRP routes.
mbgp	(Optional) Configures redistribution of only IP Version 4 multicast routes into DVMRP.

list <i>access-list-number</i>	(Optional) Number of an access list. If you specify this argument, only the multicast destinations that match the access list are reported with the configured metric. Any destinations not advertised because of split horizon do not use the configured metric.
<i>protocol</i>	(Optional) Name of unicast routing protocol, such as bgp , dvmrp , eigrp , igrp , isis , ospf , rip , or static . If you specify these values, only routes learned by the specified routing protocol are advertised in DVMRP report messages.
<i>process-id</i>	(Optional) Process ID number of the unicast routing protocol.
dvmrp	(Optional) Allows routes from the DVMRP routing table to be advertised with the configured <i>metric</i> value, or filtered.

ip multicast cache-headers

To allocate a circular buffer to store IP Version 4 multicast packet headers that the router receives, use the **ip multicast cache-headers** global configuration command. To disable the buffer, use the **no** form of this command.

ip multicast cache-headers [**rtp**]

no ip multicast cache-headers

Syntax Description

rtp	(Optional) Caches Real-Time Transport Protocol (RTP) headers.
------------	---

match nlri

The **match nlri** command is replaced by the **address-family ipv4** and **address-family vpnv4** commands. See the description of the **address-family ipv4** or **address-family vpnv4** command for more information.

redistribute dvmrp

To configure redistribution of Distance Vector Multicast Routing Protocol (DVMRP) routes into multiprotocol BGP, use the **redistribute dvmrp** command in address family or router configuration mode. To stop such redistribution, use the **no** form of this command.

redistribute dvmrp [**route-map** *map-name*]

no redistribute dvmrp [**route-map** *map-name*]

Syntax Description

route-map <i>map-name</i>	(Optional) Name of the route map that contains various BGP attribute settings.
----------------------------------	--

set nlri

The **set nlri** command is replaced by the **address-family ipv4** and **address-family vpv4** commands. See the description of the **address-family ipv4** or **address-family vpv4** command for more information.

show ip mbgp

The **show ip mbgp** command is replaced by the **show ip bgp ipv4 multicast** command. See the description of the **show ip bgp ipv4 multicast** command for more information.

show ip bgp ipv4 multicast

To display IP Version 4 multicast database-related information, use the **show ip bgp ipv4 multicast EXEC** command.

```
show ip bgp ipv4 multicast [command]
```

Syntax Description

command

(Optional) Any multiprotocol BGP command supported by the **show ip bgp ipv4 multicast** command.

show ip mbgp summary

The **show ip mbgp summary** command is replaced by the **show ip bgp ipv4 multicast summary** command. See the description of the **show ip bgp ipv4 multicast summary** command for more information.

show ip bgp ipv4 multicast summary

To display a summary of IP Version 4 multicast database-related information, use the **show ip bgp ipv4 multicast summary EXEC** command.

```
show ip bgp ipv4 multicast summary
```

Syntax Description

This command has no arguments or keywords.



IP Routing Protocol-Independent Commands

This chapter describes the function and syntax of the IP-routing protocol-independent commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*.

accept-lifetime

To set the time period during which the authentication key on a key chain is received as valid, use the **accept-lifetime** key chain key configuration command. To revert to the default value, use the **no** form of this command.

accept-lifetime *start-time* { **infinite** | *end-time* | **duration** *seconds* }

no accept-lifetime [*start-time* { **infinite** | *end-time* | **duration** *seconds* }]

Syntax Description

<i>start-time</i>	Beginning time that the key specified by the key command is valid to be received. The syntax can be either of the following: <i>hh:mm:ss Month date year</i> <i>hh:mm:ss date Month year</i> <i>hh</i> —hours <i>mm</i> —minutes <i>ss</i> —seconds <i>Month</i> —first three letters of the month <i>date</i> —date (1-31) <i>year</i> —year (four digits) The default start time and the earliest acceptable date is January 1, 1993.
infinite	Key is valid to be received from the <i>start-time</i> value on.
<i>end-time</i>	Key is valid to be received from the <i>start-time</i> value until the <i>end-time</i> value. The syntax is the same as that for the <i>start-time</i> value. The <i>end-time</i> value must be after the <i>start-time</i> value. The default end time is an infinite time period.
duration <i>seconds</i>	Length of time (in seconds) that the key is valid to be received.

distance (IP)

To define an administrative distance, use the **distance** router configuration command. To remove a distance definition, use the **no** form of this command.

```
distance weight {ip-address {ip-address-mask}} [ip-standard-list] [ip-extended-list]
```

```
no distance weight {ip-address {ip-address-mask}} [ip-standard-list] [ip-extended-list]
```

Syntax Description		
<i>weight</i>		Administrative distance. This can be an integer from 10 to 255. (The values 0 to 9 are reserved for internal use.) Used alone, the <i>weight</i> argument specifies a default administrative distance that the Cisco IOS software uses when no other specification exists for a routing information source. Routes with a distance of 255 are not installed in the routing table.
<i>ip-address</i>		IP address in four-part, dotted notation.
<i>ip-address-mask</i>		IP address mask in four-part, dotted decimal format. A bit set to 1 in the <i>mask</i> argument instructs the software to ignore the corresponding bit in the address value.
<i>ip-standard-list</i> <i>ip-extended-list</i>		(Optional) Number or name of a standard or extended IP access list to be applied to incoming routing updates.

distribute-list in (IP)

To filter networks received in updates, use the **distribute-list in** router configuration command. To change or cancel the filter, use the **no** form of this command.

```
distribute-list {access-list-number | access-list-name} in [interface-type interface-number]
```

```
no distribute-list {access-list-number | access-list-name} in [interface-type interface-number]
```

Syntax Description		
<i>access-list-number</i> <i>access-list-name</i>		Standard IP access list number or name. The list defines which networks are to be received and which are to be suppressed in routing updates.
in		Applies the access list to incoming routing updates.
<i>interface-type</i>		(Optional) Interface type.
<i>interface-number</i>		(Optional) Interface number on which the access list should be applied to incoming updates. If no interface is specified, the access list will be applied to all incoming updates.

distribute-list out (IP)

To suppress networks from being advertised in updates, use the **distribute-list out** router configuration command. To cancel this function, use the **no** form of this command.

distribute-list { *access-list-number* | *access-list-name* } **out** [*interface-name* | *routing-process* | *as-number*]

no distribute-list { *access-list-number* | *access-list-name* } **out** [*interface-name* | *routing-process* | *as-number*]

Syntax Description		
<i>access-list-number</i> <i>access-list-name</i>		Standard IP access list number or name. The list defines which networks are to be sent and which are to be suppressed in routing updates.
out		Applies the access list to outgoing routing updates.
<i>interface-name</i>		(Optional) Name of a particular interface.
<i>routing-process</i>		(Optional) Name of a particular routing process, or the static or connected keyword.
<i>as-number</i>		(Optional) Autonomous system number.

ip default-network

To select a network as a candidate route for computing the gateway of last resort, use the **ip default-network** global configuration command. To remove a route, use the **no** form of this command.

ip default-network *network-number*

no ip default-network *network-number*

Syntax Description		
<i>network-number</i>		Number of the network.

ip local policy route-map

To identify a route map to use for local policy routing, use the **ip local policy route-map** global configuration command. To disable local policy routing, use the **no** form of this command.

ip local policy route-map *map-tag*

no ip local policy route-map *map-tag*

Syntax Description		
<i>map-tag</i>		Name of the route map to use for local policy routing. The name must match a <i>map-tag</i> value specified by a route-map command.

ip policy route-map

To identify a route map to use for policy routing on an interface, use the **ip policy route-map** interface configuration command. To disable policy routing on the interface, use the **no** form of this command.

ip policy route-map *map-tag*

no ip policy route-map *map-tag*

Syntax Description	<i>map-tag</i>
	Name of the route map to use for policy routing. The name must match a <i>map-tag</i> value specified by a route-map command.

ip route

To establish static routes, use the **ip route** global configuration command. To remove static routes, use the **no** form of this command.

ip route *prefix mask* {*ip-address* | *interface-type interface-number*} [*distance*] [**tag** *tag*]
[**permanent**]

no ip route *prefix mask*

Syntax Description	
<i>prefix</i>	IP route prefix for the destination.
<i>mask</i>	Prefix mask for the destination.
<i>ip-address</i>	IP address of the next hop that can be used to reach that network.
<i>interface-type</i> <i>interface-number</i>	Network interface type and interface number.
<i>distance</i>	(Optional) An administrative distance.
tag <i>tag</i>	(Optional) Tag value that can be used as a “match” value for controlling redistribution via route maps.
permanent	(Optional) Specifies that the route will not be removed, even if the interface shuts down.

key

To identify an authentication key on a key chain, use the **key** key chain configuration command. To remove the key from the key chain, use the **no** form of this command.

key *key-id*

no key *key-id*

Syntax Description	<i>key-id</i>
	Identification number of an authentication key on a key chain. The range of keys is from 0 to 2147483647. The key identification numbers need not be consecutive.

key chain

To enable authentication for routing protocols, identify a group of authentication keys by using the **key chain** global configuration command. To remove the key chain, use the **no** form of this command.

key chain *name-of-chain*

no key chain *name-of-chain*

Syntax Description	<i>name-of-chain</i>	Name of a key chain. A key chain must have at least one key and can have up to 2,147,483,647 keys.
---------------------------	----------------------	--

key-string (authentication)

To specify the authentication string for a key, use the **key-string** key chain key configuration command. To remove the authentication string, use the **no** form of this command.

key-string *text*

no key-string [*text*]

Syntax Description	<i>text</i>	Authentication string that must be sent and received in the packets using the routing protocol being authenticated. The string can contain from 1 to 80 uppercase and lowercase alphanumeric characters, except that the first character cannot be a number.
---------------------------	-------------	--

match interface (IP)

To distribute any routes that have their next hop out one of the interfaces specified, use the **match interface** route-map configuration command. To remove the **match interface** entry, use the **no** form of this command.

match interface *interface-type interface-number* [... *interface-type interface-number*]

no match interface *interface-type interface-number* [... *interface-type interface-number*]

Syntax Description	<i>interface-type</i>	Interface type.
	<i>interface-number</i>	Interface number.

match ip address

To distribute any routes that have a destination network number address that is permitted by a standard or extended access list, or to perform policy routing on packets, use the **match ip address** route-map configuration command. To remove the **match ip address** entry, use the **no** form of this command.

```
match ip address { access-list-number | access-list-name } [...access-list-number |
...access-list-name]
```

```
no match ip address { access-list-number | access-list-name } [...access-list-number |
...access-list-name]
```

Syntax Description

<i>access-list-number</i> <i>access-list-name</i>	Number or name of a standard or extended access list. It can be an integer from 1 to 199.
--	---

match ip next-hop

To redistribute any routes that have a next hop router address passed by one of the access lists specified, use the **match ip next-hop** route-map configuration command. To remove the next hop entry, use the **no** form of this command.

```
match ip next-hop { access-list-number | access-list-name } [...access-list-number |
...access-list-name]
```

```
no match ip next-hop { access-list-number | access-list-name } [...access-list-number |
...access-list-name]
```

Syntax Description

<i>access-list-number</i> <i>access-list-name</i>	Number or name of a standard or extended access list. It can be an integer from 1 to 199.
--	---

match ip route-source

To redistribute routes that have been advertised by routers and access servers at the address specified by the access lists, use the **match ip route-source** route-map configuration command. To remove the route-source entry, use the **no** form of this command.

```
match ip route-source { access-list-number | access-list-name } [...access-list-number |
...access-list-name]
```

```
no match ip route-source { access-list-number | access-list-name } [...access-list-number |
...access-list-name]
```

Syntax Description

<i>access-list-number</i> <i>access-list-name</i>	Number or name of a standard or extended access list. It can be an integer from 1 to 199.
--	---

match length

To base policy routing on the Level 3 length of a packet, use the **match length** route-map configuration command. To remove the entry, use the **no** form of this command.

match length *minimum-length maximum-length*

no match length *minimum-length maximum-length*

Syntax Description	
<i>minimum-length</i>	Minimum Level 3 length of the packet, inclusive, allowed for a match. Range is from 0 to 0x7FFFFFFF.
<i>maximum-length</i>	Maximum Level 3 length of the packet, inclusive, allowed for a match. Range is from 0 to 0x7FFFFFFF.

match metric (IP)

To redistribute routes with the metric specified, use the **match metric** route-map configuration command. To remove the entry, use the **no** form of this command.

match metric *metric-value*

no match metric *metric-value*

Syntax Description	
<i>metric-value</i>	Route metric, which can be an IGRP five-part metric. It is a metric value from 0 to 4294967295.

match route-type (IP)

To redistribute routes of the specified type, use the **match route-type** route-map configuration command. To remove the route type entry, use the **no** form of this command.

match route-type {**local** | **internal** | **external** [**type-1** | **type-2**] | **level-1** | **level-2**}

no match route-type {**local** | **internal** | **external** [**type-1** | **type-2**] | **level-1** | **level-2**}

Syntax Description	
local	Locally generated Border Gateway Protocol (BGP) routes.
internal	Open Shortest Path First (OSPF) intra-area and interarea routes or Enhanced Interior Gateway Routing Protocol (EIGRP) internal routes.
external [type-1 type-2]	OSPF external routes, or EIGRP external routes. For OSPF, the external type-1 keyword matches only Type 1 external routes and the external type-2 keyword matches only Type 2 external routes.
level-1	Intermediate System-to-Intermediate System (IS-IS) Level 1 routes.
level-2	IS-IS Level 2 routes.

match tag

To redistribute routes in the routing table that match the specified tags, use the **match tag** route-map configuration command. To remove the tag entry, use the **no** form of this command.

match tag *tag-value* [...*tag-value*]

no match tag *tag-value* [...*tag-value*]

Syntax Description	<i>tag-value</i>	List of one or more route tag values. Each can be an integer from 0 to 4294967295.
---------------------------	------------------	--

maximum-paths

To control the maximum number of parallel routes an IP routing protocol can support, use the **maximum-paths** router configuration command. To restore the default value, use the **no** form of this command.

maximum-paths *number-paths*

no maximum-paths

Syntax Description	<i>number-paths</i>	Maximum number of parallel routes an IP routing protocol installs in a routing table, in the range from 1 to 6.
---------------------------	---------------------	---

passive-interface

To disable sending routing updates on an interface, use the **passive-interface** router configuration command. To reenble the sending of routing updates, use the **no** form of this command.

passive-interface [**default**] {*interface-type interface-number*}

no passive-interface *interface-type interface-number*

Syntax Description	default	(Optional) All interfaces become passive.
	<i>interface-type</i>	Interface type.
	<i>interface-number</i>	Interface number.

redistribute (IP)

To redistribute routes from one routing domain into another routing domain, use the **redistribute** command in router configuration mode. To disable redistribution, use the **no** form of this command.

```
redistribute protocol [process-id] {level-1 | level-1-2 | level-2} [as-number]
[metric metric-value] [metric-type type-value] [match {internal | external 1 | external 2}]
[tag tag-value] [route-map map-tag] [weight number-value] [subnets]
```

```
no redistribute protocol [process-id] {level-1 | level-1-2 | level-2} [as-number]
[metric metric-value] [metric-type type-value] [match {internal | external 1 | external 2}]
[tag tag-value] [route-map map-tag] [weight number-value] [subnets]
```

Syntax Description	
<i>protocol</i>	<p>Source protocol from which routes are being redistributed. It can be one of the following keywords: bgp, connected, egp, igrp, isis, ospf, static [ip], or rip.</p> <p>The static [ip] keyword is used to redistribute IP static routes. The optional ip keyword is used when redistributing into the Intermediate System-to-Intermediate System (IS-IS) protocol.</p> <p>The connected keyword refers to routes that are established automatically by virtue of having enabled IP on an interface. For routing protocols such as Open Shortest Path First (OSPF) and IS-IS, these routes will be redistributed as external to the autonomous system.</p>
<i>process-id</i>	<p>(Optional) For the bgp, egp, or igrp keyword, this is an autonomous system number, which is a 16-bit decimal number.</p> <p>For the isis keyword, this is an optional tag value that defines a meaningful name for a routing process. You can specify only one IS-IS process per router. Creating a name for a routing process means that you use names when configuring routing.</p> <p>For the ospf keyword, this is an appropriate OSPF process ID from which routes are to be redistributed. This identifies the routing process. This value takes the form of a nonzero decimal number.</p> <p>For the rip keyword, no <i>process-id</i> value is needed.</p>
level-1	Specifies that for IS-IS Level 1 routes are redistributed into other IP routing protocols independently.
level-1-2	Specifies that for IS-IS both Level 1 and Level 2 routes are redistributed into other IP routing protocols.
level-2	Specifies that for IS-IS Level 2 routes are redistributed into other IP routing protocols independently.
<i>as-number</i>	Autonomous system number for the redistributed route.
metric <i>metric-value</i>	(Optional) Metric used for the redistributed route. If a value is not specified for this option, and no value is specified using the default-metric command, the default metric value is 0. Use a value consistent with the destination protocol.

metric-type <i>type-value</i>	<p>(Optional) For OSPF, the external link type associated with the default route advertised into the OSPF routing domain. It can be one of two values:</p> <ul style="list-style-type: none"> • 1—Type 1 external route • 2—Type 2 external route <p>If a metric-type is not specified, the Cisco IOS software adopts a Type 2 external route.</p> <p>For IS-IS, it can be one of two values:</p> <ul style="list-style-type: none"> • internal—IS-IS metric that is < 63. • external—IS-IS metric that is > 64 < 128. <p>The default is internal.</p>
match { internal external 1 external 2 }	<p>(Optional) For the criteria by which OSPF routes are redistributed into other routing domains. It can be one of the following:</p> <ul style="list-style-type: none"> • internal—Routes that are internal to a specific autonomous system. • external 1—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 external route. • external 2—Routes that are external to the autonomous system, but are imported into OSPF as Type 2 external route.
tag <i>tag-value</i>	<p>(Optional) 32-bit decimal value attached to each external route. This is not used by OSPF itself. It may be used to communicate information between Autonomous System Boundary Routers (ASBRs). If none is specified, then the remote autonomous system number is used for routes from Border Gateway Protocol (BGP) and Exterior Gateway Protocol (EGP); for other protocols, zero (0) is used.</p>
route-map	<p>(Optional) Route map that should be interrogated to filter the importation of routes from this source routing protocol to the current routing protocol. If not specified, all routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes will be imported.</p>
<i>map-tag</i>	<p>(Optional) Identifier of a configured route map.</p>
weight <i>number-value</i>	<p>(Optional) Network weight when redistributing into BGP. An integer from 0 to 65,535.</p>
subnets	<p>(Optional) For redistributing routes into OSPF, the scope of redistribution for the specified protocol.</p>

route-map (IP)

To define the conditions for redistributing routes from one routing protocol into another, or to enable policy routing, use the **route-map** global configuration command and the **match** and **set** route-map configuration commands. To delete an entry, use the **no** form of this command.

```
route-map map-tag [permit | deny] [sequence-number]
```

```
no route-map map-tag [permit | deny] [sequence-number]
```

Syntax Description	<i>map-tag</i>	Defines a meaningful name for the route map. The redistribute router configuration command uses this name to reference this route map. Multiple route maps may share the same map tag name.
	permit	(Optional) If the match criteria are met for this route map, and the permit keyword is specified, the route is redistributed as controlled by the set actions. In the case of policy routing, the packet is policy routed. If the match criteria are not met, and the permit keyword is specified, the next route map with the same map tag is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it is not redistributed by that set. The permit keyword is the default.
	deny	(Optional) If the match criteria are met for the route map, and the deny keyword is specified, the route is not redistributed or in the case of policy routing, the packet is not policy routed, and no further route maps sharing the same map tag name will be examined. If the packet is not policy routed, the normal forwarding algorithm is used.
	<i>sequence-number</i>	(Optional) Number that indicates the position a new route map is to have in the list of route maps already configured with the same name. If given with the no form of this command, the position of the route map should be deleted.

send-lifetime

To set the time period during which an authentication key on a key chain is valid to be sent, use the **send-lifetime** key chain key configuration command. To revert to the default value, use the **no** form of this command.

send-lifetime *start-time* { **infinite** | *end-time* | **duration** *seconds* }

no send-lifetime [*start-time* { **infinite** | *end-time* | **duration** *seconds* }]

Syntax Description	<i>start-time</i>	Beginning time that the key specified by the key command is valid to be sent. The syntax can be either of the following: <i>hh:mm:ss Month date year</i> <i>hh:mm:ss date Month year</i> <i>hh</i> —hours <i>mm</i> —minutes <i>ss</i> —seconds <i>Month</i> —first three letters of the month <i>date</i> —date (1-31) <i>year</i> —year (four digits) The default start time and the earliest acceptable date is January 1, 1993.
	infinite	Key is valid to be sent from the <i>start-time</i> value on.

<i>end-time</i>	Key is valid to be sent from the <i>start-time</i> value until the <i>end-time</i> value. The syntax is the same as that for the <i>start-time</i> value. The <i>end-time</i> value must be after the <i>start-time</i> value. The default end time is an infinite time period.
duration <i>seconds</i>	Length of time (in seconds) that the key is valid to be sent.

set automatic-tag

To automatically compute the tag value, use the **set automatic-tag** route-map configuration command. To disable this function, use the **no** form of this command.

set automatic-tag

no set automatic-tag

Syntax Description This command has no arguments or keywords.

set default interface

To indicate where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination, use the **set default interface** route-map configuration command. To delete an entry, use the **no** form of this command.

set default interface *interface-type interface-number* [...*interface-type interface-number*]

no set default interface *interface-type interface-number* [...*interface-type interface-number*]

Syntax Description

<i>interface-type</i>	Interface type, used with the interface number, to which packets are output.
<i>interface-number</i>	Interface number, used with the interface type, to which packets are output.

set interface

To indicate where to output packets that pass a match clause of a route map for policy routing, use the **set interface** route-map configuration command. To delete an entry, use the **no** form of this command.

set interface *interface-type interface-number* [...*interface-type interface-number*]

no set interface *interface-type interface-number* [...*interface-type interface-number*]

Syntax Description

<i>interface-type</i>	Interface type, used with the interface number, to which packets are output.
<i>interface-number</i>	Interface number, used with the interface type, to which packets are output.

set ip default next-hop

To indicate where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination, use the **set ip default next-hop** route-map configuration command. To delete an entry, use the **no** form of this command.

```
set ip default next-hop ip-address [...ip-address]
```

```
no set ip default next-hop ip-address [...ip-address]
```

Syntax Description	<i>ip-address</i>	IP address of the next hop to which packets are output. It must be an adjacent router.
---------------------------	-------------------	--

set ip next-hop

To indicate where to output packets that pass a match clause of a route map for policy routing, use the **set ip next-hop** route-map configuration command. To delete an entry, use the **no** form of this command.

```
set ip next-hop ip-address [...ip-address]
```

```
no set ip next-hop ip-address [...ip-address]
```

Syntax Description	<i>ip-address</i>	IP address of the next hop to which packets are output. It must be the address of an adjacent router.
---------------------------	-------------------	---

set ip next-hop verify-availability

To configure policy routing to verify if the next hops of a route map are Cisco Discovery Protocol (CDP) neighbors before policy routing to those next hops, use the **set ip next-hop verify-availability** route-map configuration command.

```
set ip next-hop verify-availability
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--

set ip precedence

To set the precedence value in the IP header, use the **set ip precedence** route-map configuration command. To instruct the router to leave the precedence value alone, use the **no** form of this command.

```
set ip precedence number | name
```

```
no set ip precedence
```

Syntax Description	<i>number</i> <i>name</i>	Number or name that sets the precedence bits in the IP header. The number and its corresponding name are as follows, from least important to most important:
		Number Name
		0 routine
		1 priority
		2 immediate
		3 flash
		4 flash-override
		5 critical
		6 internet
		7 network

set level (IP)

To indicate where to import routes, use the **set level** route-map configuration command. To delete an entry, use the **no** form of this command.

set level { **level-1** | **level-2** | **level-1-2** | **stub-area** | **backbone** }

no set level { **level-1** | **level-2** | **level-1-2** | **stub-area** | **backbone** }

Syntax Description		
level-1		Imports routes into a Level 1 area.
level-2		Imports routes into a Level 2 subdomain.
level-1-2		Imports routes into Level 1 and Level 2.
stub-area		Imports routes into an Open Shortest Path First (OSPF) not-so-stubby area (NSSA) area.
backbone		Imports routes into an OSPF backbone area.

set local-preference

To specify a preference value for the autonomous system path, use the **set local-preference** route-map configuration command. To delete an entry, use the **no** form of this command.

set local-preference *number-value*

no set local-preference *number-value*

Syntax Description	<i>number-value</i>	Preference value. An integer from 0 to 4294967295.

set metric (BGP, OSPF, RIP)

To set the metric value for a routing protocol, use the **set metric** route-map configuration command. To return to the default metric value, use the **no** form of this command.

```
set metric metric-value
```

```
no set metric metric-value
```

Syntax Description	<i>metric-value</i>	Metric value; an integer from -294967295 to 294967295. This argument applies to all routing protocols except Interior Gateway Routing Protocol (IGRP) and Enhanced IGRP (EIGRP).
---------------------------	---------------------	--

set metric-type

To set the metric type for the destination routing protocol, use the **set metric-type** route-map configuration command. To return to the default, use the **no** form of this command.

```
set metric-type {internal | external | type-1 | type-2}
```

```
no set metric-type {internal | external | type-1 | type-2}
```

Syntax Description	internal	Intermediate System-to-Intermediate System (IS-IS) internal metric.
	external	IS-IS external metric.
	type-1	Open Shortest Path First (OSPF) external Type 1 metric.
	type-2	OSPF external Type 2 metric.

set next-hop

To specify the address of the next hop, use the **set next-hop** route-map configuration command. To delete an entry, use the **no** form of this command.

```
set next-hop next-hop
```

```
no set next-hop next-hop
```

Syntax Description	<i>next-hop</i>	IP address of the next hop router.
---------------------------	-----------------	------------------------------------

set tag (IP)

To set a tag value of the destination routing protocol, use the **set tag** route-map configuration command. To delete the entry, use the **no** form of this command.

```
set tag tag-value
```

```
no set tag tag-value
```

Syntax Description	<i>tag-value</i>	Name for the tag. Integer from 0 to 4294967295.
---------------------------	------------------	---

show ip cache policy

To display the cache entries in the policy route cache, use the **show ip cache policy** EXEC command.

```
show ip cache policy
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--

show ip local policy

To display the route map used for local policy routing, if any, use the **show ip local policy** EXEC command.

```
show ip local policy
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--

show ip policy

To display the route map used for policy routing, use the **show ip policy** EXEC command.

```
show ip policy
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--

show ip protocols

To display the parameters and current state of the active routing protocol process, use the **show ip protocols** EXEC command.

```
show ip protocols
```

Syntax Description This command has no arguments or keywords.

show ip route

To display the current state of the routing table, use the **show ip route** EXEC command.

```
show ip route [ip-address [mask] [longer-prefixes]] | [protocol [process-id]]
```

Syntax Description	<i>ip-address</i>	(Optional) Address about which routing information should be displayed.
	<i>mask</i>	(Optional) Argument for a subnet mask.
	longer-prefixes	(Optional) Specifies that routes matching the <i>ip-address</i> and <i>mask</i> pair only should be displayed.
	<i>protocol</i>	(Optional) Name of a routing protocol; or the keyword connected , static , or summary . If you specify a routing protocol, use one of the following keywords: bgp , egp , eigrp , hello , igrp , isis , ospf , and rip .
	<i>process-id</i>	(Optional) Number used to identify a process of the specified protocol.

show ip route summary

To display the current state of the routing table, use the **show ip route summary** EXEC command.

```
show ip route summary
```

Syntax Description This command has no arguments or keywords.

show ip route supernets-only

To display information about supernets, use the **show ip route supernets-only** privileged EXEC command.

```
show ip route supernets-only
```

Syntax Description This command has no arguments or keywords.

show key chain

To display authentication key information, use the **show key chain** EXEC command.

```
show key chain [name-of-chain]
```

Syntax Description	<i>name-of-chain</i>	(Optional) Name of the key chain to display, as named in the key chain command.
---------------------------	----------------------	--

show route-map

To display configured route maps, use the **show route-map** EXEC command.

```
show route-map [map-name]
```

Syntax Description	<i>map-name</i>	(Optional) Name of a specific route map.
---------------------------	-----------------	--

show route-map ipc

To display counts of the one-way route map interprocess communication (IPC) messages sent from the rendezvous point (RP) to the Versatile Interface Processor (VIP) when NetFlow policy routing is configured, use the **show route-map ipc** EXEC command.

```
show route-map ipc
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--

traffic-share min

To configure traffic to use minimum cost routes, when there are multiple routes that have different cost routes to the same destination network, use the **traffic-share min across-interfaces** router configuration command. To disable this function, use the **no** form of this command.

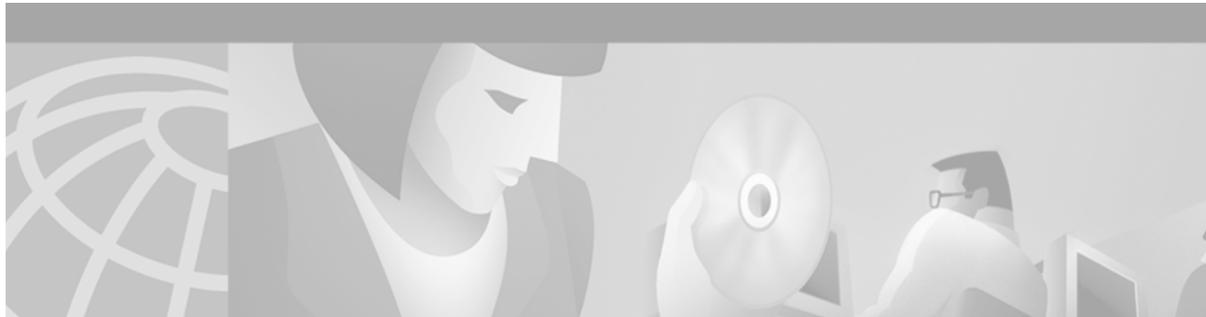
```
traffic-share min {across-interfaces}
```

```
no traffic-share min {across-interfaces}
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--



IP: Multicast



IP Multicast Routing Commands

This chapter describes the function and syntax of the IP multicast routing commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*.

clear ip cgmp

To clear all group entries from the caches of Catalyst switches, use the **clear ip cgmp** EXEC command.

```
clear ip cgmp [type number]
```

Syntax Description

<i>type number</i>	(Optional) Interface type and number.
--------------------	---------------------------------------

clear ip dvmrp route

To delete routes from the Distance Vector Multicast Routing Protocol (DVMRP) routing table, use the **clear ip dvmrp route** EXEC command.

```
clear ip dvmrp route { * | route }
```

Syntax Description

*	Clears all routes from the DVMRP table.
<i>route</i>	Clears the longest matched route. Can be an IP address, a network number, or an IP Domain Name System (DNS) name.

clear ip igmp group

To delete entries from the Internet Group Management Protocol (IGMP) cache, use the **clear ip igmp group** EXEC command.

```
clear ip igmp group [group-name | group-address | type number]
```

Syntax Description	<i>group-name</i>	(Optional) Name of the multicast group, as defined in the Domain Name System (DNS) hosts table or with the ip host command.
	<i>group-address</i>	(Optional) Address of the multicast group. This is a multicast IP address in four-part, dotted notation.
	<i>type number</i>	(Optional) Interface type and number.

clear ip mroute

To delete entries from the IP multicast routing table, use the **clear ip mroute** EXEC command.

```
clear ip mroute [* | group-name [source-name | source-address] | group-address [source-name | source-address]]
```

Syntax Description	*	Deletes all entries from the IP multicast routing table.
	<i>group-name</i>	Name of the multicast group, as defined in the Domain Name System (DNS) hosts table or with the ip host command.
	<i>group-address</i>	IP address of the multicast group. This is a multicast IP address in four-part, dotted notation.
	<i>source-name</i> <i>source-address</i>	(Optional) If you specify a group name or address, you can also specify a name or address of a multicast source that is sending to the group. A source need not be a member of the group.

clear ip pim auto-rp

To delete entries from the Auto-RP cache, use the **clear ip pim auto-rp** EXEC command.

```
clear ip pim auto-rp rp-address
```

Syntax Description	<i>rp-address</i>	Clears only the entries related to the rendezvous point (RP) at this address. If this argument is omitted, the entire Auto-RP cache is cleared.
---------------------------	-------------------	---

clear ip rtp header-compression

To clear Real-Time Transport Protocol (RTP) header compression structures and statistics, use the **clear ip rtp header-compression** EXEC command.

```
clear ip rtp header-compression [type number]
```

Syntax Description	<i>type number</i>	(Optional) Interface type and number.
---------------------------	--------------------	---------------------------------------

clear ip sap

To delete a Session Announcement Protocol (SAP) cache entry or the entire SAP cache, use the **clear ip sap** EXEC command.

```
clear ip sap [group-address | "session-name"]
```

Syntax Description		
	<i>group-address</i>	(Optional) Deletes all sessions associated with the IP group address.
	<i>"session-name"</i>	(Optional) Deletes only the SAP cache entry with the specified session name. The session name is enclosed in quotation marks (“ ”) that the user must enter.

clear ip sdr

The **clear ip sdr** command is replaced by the **clear ip sap** command. See the description of the **clear ip sap** command in this chapter for more information.

frame-relay ip rtp compression-connections

To specify the maximum number of Real-Time Transport Protocol (RTP) header compression connections that can exist on a Frame Relay interface, use the **frame-relay ip rtp compression-connections** interface configuration command. To restore the default, use the **no** form of this command.

```
frame-relay ip rtp compression-connections number
```

```
no frame-relay ip rtp compression-connections
```

Syntax Description		
	<i>number</i>	Maximum number of RTP header compression connections. The range is from 3 to 256.

frame-relay ip rtp header-compression

To enable Real-Time Transport Protocol (RTP) header compression for all Frame Relay maps on a physical interface, use the **frame-relay ip rtp header-compression** interface configuration command. To disable the compression, use the **no** form of this command.

```
frame-relay ip rtp header-compression [active | passive]
```

```
no frame-relay ip rtp header-compression [active | passive]
```

Syntax Description

active	(Optional) Compresses all outgoing RTP packets. This is the default.
passive	(Optional) Compresses the outgoing RTP/User Datagram Protocol (UDP)/IP header only if an incoming packet had a compressed header.

frame-relay map ip compress

To enable both Real-Time Transport Protocol (RTP) and TCP header compression on a link, use the **frame-relay map ip compress** interface configuration command.

```
frame-relay map ip ip-address dlc [broadcast] compress [active | passive]
[connections number]
```

Syntax Description

<i>ip-address</i>	IP address of the destination or next hop.
<i>dlci</i>	Data-link connection identifier (DLCI) number.
broadcast	(Optional) Forwards broadcasts to the specified IP address.
active	(Optional) Compresses all outgoing RTP and TCP packets. This is the default.
passive	(Optional) Compresses the outgoing RTP and TCP header only if an incoming packet had a compressed header.
connections <i>number</i>	(Optional) Specifies the maximum number of RTP and TCP header compression connections. The range is from 3 to 256.

frame-relay map ip nocompress

To disable both Real-Time Transport Protocol (RTP) and TCP header compression on a link, use the **frame-relay map ip nocompress** interface configuration command.

```
frame-relay map ip ip-address dlc [broadcast] nocompress
```

Syntax Description

<i>ip-address</i>	IP address of the destination or next hop.
<i>dlci</i>	Data-link connection identifier (DLCI) number.
broadcast	(Optional) Forwards broadcasts to the specified IP address.

frame-relay map ip rtp header-compression

To enable Real-Time Transport Protocol (RTP) header compression per data-link connection identifier (DLCI), use the **frame-relay map ip rtp header-compression** interface configuration command.

```
frame-relay map ip ip-address dlc [broadcast] rtp header-compression [active | passive]
[connections number]
```

Syntax Description	<i>ip-address</i>	IP address of the destination or next hop.
	<i>dldci</i>	DLCI number.
	broadcast	(Optional) Forwards broadcasts to the specified IP address.
	active	(Optional) Compresses outgoing RTP packets. This is the default.
	passive	(Optional) Compresses the outgoing RTP/UDP/IP header only if an incoming packet had a compressed header.
	connections number	(Optional) Specifies the maximum number of RTP header compression connections. The range is from 3 to 256.

ip cgmp

To enable Cisco Group Management Protocol (CGMP) on an interface of a router connected to a Catalyst 5000 switch, use the **ip cgmp** interface configuration command. To disable CGMP routing, use the **no** form of this command.

```
ip cgmp [proxy]
```

```
no ip cgmp
```

Syntax Description	proxy	(Optional) Enables CGMP and the CGMP proxy function.
---------------------------	--------------	--

ip dvmrp accept-filter

To configure an acceptance filter for incoming Distance Vector Multicast Routing Protocol (DVMRP) reports, use the **ip dvmrp accept-filter** interface configuration command. To disable this filter, use the **no** form of this command.

```
ip dvmrp accept-filter access-list [distance | neighbor-list access-list]
```

```
no ip dvmrp accept-filter access-list [distance | neighbor-list access-list]
```

Syntax Description	<i>access-list</i>	Access list number or name. A value of 0 means that all sources are accepted with the configured distance.
	<i>distance</i>	(Optional) Administrative distance to the destination.
	neighbor-list access-list	(Optional) Number of a neighbor list. DVMRP reports are accepted only by those neighbors on the list.

ip dvmrp auto-summary

To enable Distance Vector Multicast Routing Protocol (DVMRP) automatic summarization if it was disabled, use the **ip dvmrp auto-summary** interface configuration command. To disable the feature, use the **no** form of this command.

ip dvmrp auto-summary

no ip dvmrp auto-summary

Syntax Description This command has no arguments or keywords.

ip dvmrp default-information

To advertise network 0.0.0.0 to Distance Vector Multicast Routing Protocol (DVMRP) neighbors on an interface, use the **ip dvmrp default-information** interface configuration command. To prevent the advertisement, use the **no** form of this command.

ip dvmrp default-information { originate | only }

no ip dvmrp default-information { originate | only }

Syntax Description

originate	Other routes more specific than 0.0.0.0 may be advertised.
only	No DVMRP routes other than 0.0.0.0 are advertised.

ip dvmrp metric

To configure the metric associated with a set of destinations for Distance Vector Multicast Routing Protocol (DVMRP) reports, use the appropriate form of the **ip dvmrp metric** interface configuration command. To disable this function, use the appropriate **no** form of this command.

ip dvmrp metric *metric* [list *access-list*] [route-map *map-name*] [mbgp] [*protocol process-id*]

no ip dvmrp metric *metric* [list *access-list*] [route-map *map-name*] [mbgp] [*protocol process-id*]

Syntax Description

<i>metric</i>	Metric associated with a set of destinations for DVMRP reports. It can be a value from 0 to 32. A value of 0 means that the route is not advertised. A value of 32 is equivalent to infinity (unreachable).
list <i>access-list</i>	(Optional) Number name of an access list. If you specify this argument, only the multicast destinations that match the access list are reported with the configured metric. Any destinations not advertised because of split horizon do not use the configured metric.

route-map <i>map-name</i>	(Optional) Name of the route map. Only the destinations that match the route map are reported with the configured metric. Unicast routes are subject to route map conditions before being injected into DVMRP. Route maps cannot be used for DVMRP routes.
mbgp	(Optional) Configures redistribution of only IP version 4 (IPv4) multicast routes into DVMRP.
<i>protocol</i>	(Optional) Name of unicast routing protocol, such as bgp , eigrp , igrp , isis , ospf , rip , static , or dvmrp . If you specify these arguments, only routes learned by the specified routing protocol are advertised in DVMRP report messages.
<i>process-id</i>	(Optional) Process ID number of the unicast routing protocol.

ip dvmrp metric-offset

To change the metrics of advertised Distance Vector Multicast Routing Protocol (DVMRP) routes and thus favor or not favor a certain route, use the **ip dvmrp metric-offset** interface configuration command. To restore the default values, use the **no** form of this command.

ip dvmrp metric-offset [**in** | **out**] *increment*

no ip dvmrp metric-offset

Syntax Description	in	(Optional) The <i>increment</i> value is added to incoming DVMRP reports and is reported in mrrinfo replies. The default for in is 1.
	out	(Optional) The <i>increment</i> value is added to outgoing DVMRP reports for routes from the DVMRP routing table. The default for out is 0.
	<i>increment</i>	Value added to the metric of a DVMRP route advertised in a report message.

ip dvmrp output-report-delay

To configure an interpacket delay of a Distance Vector Multicast Routing Protocol (DVMRP) report, use the **ip dvmrp output-report-delay** interface configuration command. To restore the default values, use the **no** form of this command.

ip dvmrp output-report-delay *milliseconds* [*burst*]

no ip dvmrp output-report-delay *milliseconds* [*burst*]

Syntax Description	<i>milliseconds</i>	Number of milliseconds that elapse between transmissions of a set of DVMRP report packets. The number of packets in the set is determined by the <i>burst</i> argument. The default number of milliseconds is 100 milliseconds.
	<i>burst</i>	(Optional) The number of packets in the set being sent. The default is 2 packets.

ip dvmrp reject-non-pruners

To configure the router so that it will not peer with a Distance Vector Multicast Routing Protocol (DVMRP) neighbor if that neighbor does not support DVMRP pruning or grafting, use the **ip dvmrp reject-non-pruners** interface configuration command. To disable the function, use the **no** form of this command.

ip dvmrp reject-non-pruners

no ip dvmrp reject-non-pruners

Syntax Description This command has no arguments or keywords.

ip dvmrp routehog-notification

To change the number of Distance Vector Multicast Routing Protocol (DVMRP) routes allowed before a syslog warning message is issued, use the **ip dvmrp routehog-notification** global configuration command. To restore the default value, use the **no** form of this command.

ip dvmrp routehog-notification *route-count*

no ip dvmrp routehog-notification

Syntax Description	<i>route-count</i>	Number of routes allowed before a syslog message is triggered. The default is 10,000 routes.
---------------------------	--------------------	--

ip dvmrp route-limit

To change the limit on the number of Distance Vector Multicast Routing Protocol (DVMRP) routes that can be advertised over an interface enabled to run DVMRP, use the **ip dvmrp route-limit** global configuration command. To configure no limit, use the **no** form of this command.

ip dvmrp route-limit *count*

no ip dvmrp route-limit

Syntax Description	<i>count</i>	Number of DVMRP routes that can be advertised. The default is 7000 routes.
---------------------------	--------------	--

ip dvmrp summary-address

To configure a Distance Vector Multicast Routing Protocol (DVMRP) summary address to be advertised out the interface, use the **ip dvmrp summary-address** interface configuration command. To remove the summary address, use the **no** form of this command.

ip dvmrp summary-address *summary-address mask* [**metric value**]

no ip dvmrp summary-address *summary-address mask* [**metric value**]

Syntax Description

<i>summary-address</i>	Summary IP address that is advertised instead of the more specific route.
<i>mask</i>	Mask on the summary IP address.
<i>metric value</i>	(Optional) Metric that is advertised with the summary address. The default is 1.

ip dvmrp unicast-routing

To enable Distance Vector Multicast Routing Protocol (DVMRP) unicast routing on an interface, use the **ip dvmrp unicast-routing** interface configuration command. To disable the feature, use the **no** form of this command.

ip dvmrp unicast-routing

no ip dvmrp unicast-routing

Syntax Description

This command has no arguments or keywords.

ip igmp access-group

To control the multicast groups that hosts on the subnet serviced by an interface can join, use the **ip igmp access-group** interface configuration command. To disable groups on an interface, use the **no** form of this command.

ip igmp access-group *access-list version*

no ip igmp access-group *access-list version*

Syntax Description

<i>access-list</i>	Number or name of a standard IP access list. The access list can be a number from 1 to 99.
<i>version</i>	Changes Internet Group Management Protocol (IGMP) version. Default is version 2.

ip igmp helper-address

To cause the system to forward all Internet Group Management Protocol (IGMP) host reports and leave messages received on the interface to the specified IP address, use the **ip igmp helper-address** interface configuration command. To disable such forwarding, use the **no** form of this command.

ip igmp helper-address *ip-address*

no ip igmp helper-address

Syntax Description	<i>ip-address</i>	IP address to which IGMP host reports and leave messages are forwarded. Specify the IP address of an interface on the central router.
---------------------------	-------------------	---

ip igmp join-group

To have the router join a multicast group, use the **ip igmp join-group** interface configuration command. To cancel membership in a multicast group, use the **no** form of this command.

ip igmp join-group *group-address*

no ip igmp join-group *group-address*

Syntax Description	<i>group-address</i>	Address of the multicast group. This is a multicast IP address in four-part, dotted notation.
---------------------------	----------------------	---

ip igmp query-interval

To configure the frequency at which Cisco IOS software sends Internet Group Management Protocol (IGMP) host query messages, use the **ip igmp query-interval** interface configuration command. To return to the default frequency, use the **no** form of this command.

ip igmp query-interval *seconds*

no ip igmp query-interval

Syntax Description	<i>seconds</i>	Frequency, in seconds, at which to send IGMP host query messages. It can be a number from 0 to 65535. The default is 60 seconds.
---------------------------	----------------	--

ip igmp query-max-response-time

To configure the maximum response time advertised in Internet Group Management Protocol (IGMP) queries, use the **ip igmp query-max-response-time** interface configuration command. To restore the default value, use the **no** form of this command.

ip igmp query-max-response-time *seconds*

no ip igmp query-max-response-time

Syntax Description	<i>seconds</i>	Maximum response time, in seconds, advertised in IGMP queries. The default value is 10 seconds.
---------------------------	----------------	---

ip igmp query-timeout

To configure the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying, use the **ip igmp query-timeout** interface configuration command. To restore the default value, use the **no** form of this command.

ip igmp query-timeout *seconds*

no ip igmp query-timeout

Syntax Description	<i>seconds</i>	Number of seconds that the router waits after the previous querier has stopped querying and before it takes over as the querier.
---------------------------	----------------	--

ip igmp static-group

To configure the router to be a statically connected member of the specified group on the interface, use the **ip igmp static-group** interface configuration command. To remove the router as a member of the group, use the **no** form of this command.

ip igmp static-group *group-address*

no ip igmp static-group *group-address*

Syntax Description	<i>group-address</i>	IP multicast group address of a group to which the router belongs.
---------------------------	----------------------	--

ip igmp v3lite

To enable acceptance and processing of Internet Group Management Protocol Version 3 lite (IGMP v3lite) membership reports on an interface, use the **ip igmp v3lite** interface configuration command. To disable IGMP v3lite, use the **no** form of this command.

ip igmp v3lite

no ip igmp v3lite

Syntax Description This command has no arguments or keywords.

ip igmp version

To configure which version of Internet Group Management Protocol (IGMP) the router uses, use the **ip igmp version** interface configuration command. To restore the default value, use the **no** form of this command.

ip igmp version {1 | 2 | 3}

no ip igmp version

Syntax Description

1	IGMP Version 1.
2	IGMP Version 2.
3	IGMP Version 3.

ip mroute

To configure a multicast static route (mroute), use the **ip mroute** global configuration command. To remove the route, use the **no** form of this command.

ip mroute *source-address mask [protocol as-number] {rpf-address | type number} [distance]*

no ip mroute *source mask [protocol as-number] {rpf-address | type number} [distance]*

Syntax Description

<i>source-address</i>	IP address of the multicast source.
<i>mask</i>	Mask on the IP address of the multicast source.
<i>protocol</i>	(Optional) Unicast routing protocol that you are using.
<i>as-number</i>	(Optional) Autonomous system number of the routing protocol you are using, if applicable.

<i>rpf-address</i>	Incoming interface for the mroute. If the Reverse Path Forwarding (RPF) address <i>rpf-address</i> is a Protocol Independent Multicast (PIM) neighbor, PIM join, graft, and prune messages are sent to it. The <i>rpf-address</i> argument can be a host IP address of a directly connected system or a network/subnet number. When it is a route, a recursive lookup is done from the unicast routing table to find a directly connected system. If the <i>rpf-address</i> argument is not specified, the interface <i>type number</i> value is used as the incoming interface.
<i>type number</i>	Interface type and number for the mroute.
<i>distance</i>	(Optional) Determines whether a unicast route, a Distance Vector Multicast Routing Protocol (DVMRP) route, or a static mroute should be used for the RPF lookup. The lower distances have better preference. If the static mroute has the same distance as the other two RPF sources, the static mroute will take precedence. The default is 0.

ip multicast boundary

To configure an administratively scoped boundary, use the **ip multicast boundary** interface configuration command. To remove the boundary, use the **no** form of this command.

ip multicast boundary *access-list*

no ip multicast boundary

Syntax Description	<i>access-list</i>	Number or name identifying an access list that controls the range of group addresses affected by the boundary.
---------------------------	--------------------	--

ip multicast cache-headers

To allocate a circular buffer to store IP multicast packet headers that the router receives, use the **ip multicast cache-headers** global configuration command. To remove the buffer, use the **no** form of this command.

ip multicast cache-headers [*rtp*]

no ip multicast cache-headers

Syntax Description	<i>rtp</i>	(Optional) Caches Real-Time Transport Protocol (RTP) headers.
---------------------------	------------	---

ip multicast heartbeat

To monitor the health of multicast delivery and be alerted when the delivery fails to meet certain parameters, use the **ip multicast heartbeat** global configuration command. To disable the heartbeat, use the **no** form of the command.

ip multicast heartbeat *group-address minimum-number window-size interval*

no ip multicast heartbeat *group-address minimum-number window-size interval*

Syntax Description

<i>group-address</i>	A multicast group address (Class D address, from 224.0.0.0 to 239.255.255.255)
<i>minimum-number</i>	Number of packets to be received within a specified number of intervals.
<i>window-size</i>	Window size within which a specified number of intervals must receive a specified number of packets.
<i>interval</i>	Number of seconds interval to receive packet. Value must be a multiple of 10.

ip multicast helper-map

To allow IP multicast routing in a multicast-capable internetwork between two broadcast-only internetworks, use the **ip multicast helper-map** interface configuration command. To disable this function, use the **no** form of this command.

ip multicast helper-map { *group-address* | **broadcast** } { *broadcast-address* | *multicast-address* } *access-list*

no multicast helper-map { *group-address* | **broadcast** } { *broadcast-address* | *multicast-address* } *access-list*

Syntax Description

<i>group-address</i>	Multicast group address of traffic to be converted to broadcast traffic. Use this with the <i>broadcast-address</i> value.
broadcast	Specifies the traffic is being converted from broadcast to multicast. Use this with the <i>multicast-address</i> value.
<i>broadcast-address</i>	Address to which broadcast traffic is sent. Use this with the <i>group-address</i> value.
<i>multicast-address</i>	Specifies the IP multicast address to which the converted traffic is directed. Use this with the broadcast keyword.
<i>access-list</i>	IP extended access list number or name that controls which broadcast packets are translated, based on the User Datagram Protocol (UDP) port number.

ip multicast multipath

To enable load splitting of IP multicast traffic across multiple equal-cost paths, use the **ip multicast multipath** global configuration command. To disable this configuration, use the **no** form of this command.

ip multicast multipath

no ip multicast multipath

Syntax Description This command has no arguments or keywords.

ip multicast rate-limit

To control the rate a sender from the source list can send to a multicast group in the group list, use the **ip multicast rate-limit** interface configuration command. To remove the control, use the **no** form of this command.

ip multicast rate-limit {in | out} [video | whiteboard] [group-list *access-list*] [source-list *access-list*] *kbps*

no ip multicast rate-limit {in | out} [video | whiteboard] [group-list *access-list*] [source-list *access-list*] *kbps*

Syntax Description		
in		Only packets at the rate of the <i>kbps</i> value or slower are accepted on the interface.
out		Only a maximum of the <i>kbps</i> value will be sent on the interface.
video		(Optional) Rate limiting is performed based on the User Datagram Protocol (UDP) port number used by video traffic. Video traffic is identified by consulting the Session Announcement Protocol (SAP) cache.
whiteboard		(Optional) Rate limiting is performed based on the UDP port number used by whiteboard traffic. Whiteboard traffic is identified by consulting the SAP cache.
group-list <i>access-list</i>		(Optional) Specifies the access list number or name that controls which multicast groups are subject to the rate limit.
source-list <i>access-list</i>		(Optional) Specifies the access list number or name that controls which senders are subject to the rate limit.
<i>kbps</i>		Transmission rate (in kbps). Any packets sent at greater than this value are silently discarded. If this command is configured, the default value is 0, meaning that no traffic is permitted. Therefore, set this to a positive value if you use this command.

ip multicast ttl-threshold

To configure the time-to-live (TTL) threshold of packets being forwarded out an interface, use the **ip multicast ttl-threshold** interface configuration command. To return to the default TTL threshold, use the **no** form of this command.

ip multicast ttl-threshold *ttl-value*

no ip multicast ttl-threshold [*ttl-value*]

Syntax Description	<i>ttl-value</i>	Time-to-live value, in hops. It can be a value from 0 to 255. The default value is 0, which means that all multicast packets are forwarded out the interface.
---------------------------	------------------	---

ip multicast use-functional

To enable the mapping of IP multicast addresses to the Token Ring functional address 0xc000.0004.0000, use the **ip multicast use-functional** interface configuration command. To disable the function, use the **no** form of this command.

ip multicast use-functional

no ip multicast use-functional

Syntax Description	This command has no arguments or keywords.
---------------------------	--

ip pim

To enable Protocol Independent Multicast (PIM) on an interface, use the **ip pim** interface configuration command. To disable PIM on the interface, use the **no** form of this command.

ip pim {**sparse-mode** | **sparse-dense-mode** | **dense-mode** [**proxy-register** {**list** *access-list* | **route-map** *map-name*}]}

no ip pim

Syntax Description	sparse-mode	Enables sparse mode of operation.
	sparse-dense-mode	The interface is treated in either sparse mode or dense mode of operation, depending on which mode the multicast group operates in.
	dense-mode	Enables dense mode of operation.
	proxy-register	(Optional) Enables proxy registering on the interface of a designated router (DR) (leading toward the bordering dense mode region) for multicast traffic from sources not connected to the DR.
	list <i>access-list</i>	(Optional) Defines the extended access list number or name.
	route-map <i>map-name</i>	(Optional) Defines the route map.

ip pim accept-rp

To configure a router to accept join or prune messages destined for a specified rendezvous point (RP) and for a specific list of groups, use the **ip pim accept-rp** global configuration command. To remove that check, use the **no** form of this command.

```
ip pim accept-rp {rp-address | auto-rp} [access-list]
```

```
no ip pim accept-rp {rp-address | auto-rp} [access-list]
```

Syntax Description		
	<i>rp-address</i>	RP address of the RP allowed to send join messages to groups in the range specified by the group access list.
	auto-rp	Join and register messages are accepted only for RPs that are in the Auto-RP cache.
	<i>access-list</i>	(Optional) Access list number or name that defines which groups are subject to the check.

ip pim border

The **ip pim border** command is replaced by the **ip pim bsr-border** command. See the description of the **ip pim bsr-border** command in this chapter for more information.

ip pim bsr-border

To prevent bootstrap router (BSR) messages from being sent or received through an interface, use the **ip pim bsr-border** interface configuration command. To disable this configuration, use the **no** form of this command.

```
ip pim bsr-border
```

```
no ip pim bsr-border
```

Syntax Description This command has no arguments or keywords.

ip pim bsr-candidate

To configure the router to announce its candidacy as a bootstrap router (BSR), use the **ip pim bsr-candidate** global configuration command. To remove this router as a candidate for being a bootstrap router, use the **no** form of this command.

```
ip pim bsr-candidate type number hash-mask-length [priority]
```

```
no ip pim bsr-candidate
```

Syntax Description		
	<i>type number</i>	Interface type and number on this router from which the bootstrap router address is derived, to make it a candidate. This interface must be enabled with Protocol Independent Multicast (PIM).
	<i>hash-mask-length</i>	Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash (correspond) to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. This fact allows you to get one RP for multiple groups.
	<i>priority</i>	(Optional) Integer from 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IP address is the BSR. The default value is 0.

ip pim message-interval

To configure the frequency at which a Protocol Independent Multicast sparse mode (PIM-SM) router sends periodic join and prune messages, use the **ip pim message-interval** global configuration command. To return to the default interval, use the **no** form of this command.

ip pim message-interval *seconds*

no ip pim message-interval [*seconds*]

Syntax Description		
	<i>seconds</i>	Interval (in seconds) at which periodic PIM-SM join and prune messages are sent. It can be a number from 1 to 65535. The default is 60 seconds.

ip pim minimum-vc-rate

To configure the minimum traffic rate to keep virtual circuits (VCs) from being idled, use the **ip pim minimum-vc-rate** interface configuration command. To restore the default value, use the **no** form of this command.

ip pim minimum-vc-rate *pps*

no ip pim minimum-vc-rate

Syntax Description		
	<i>pps</i>	Rate, in packets per second, below which a VC is eligible for idling. The default value is 0, which means all VCs are eligible for idling. The range is from 0 to 4294967295.

ip pim multipoint-signalling

To enable Protocol Independent Multicast (PIM) to open ATM multipoint switched virtual circuits (VCs) for each multicast group that a receiver joins, use the **ip pim multipoint-signalling** interface configuration command. To disable the feature, use the **no** form of this command.

ip pim multipoint-signalling

no ip pim multipoint-signalling

Syntax Description This command has no arguments or keywords.

ip pim nbma-mode

To configure a multiaccess WAN interface to be in nonbroadcast multiaccess (NBMA) mode, use the **ip pim nbma-mode** interface configuration command. To disable this function, use the **no** form of this command.

ip pim nbma-mode

no ip pim nbma-mode

Syntax Description This command has no arguments or keywords.

ip pim neighbor-filter

To prevent a router from participating in Protocol Independent Multicast (PIM) (for example, to configure stub multicast routing), use the **ip pim neighbor-filter** interface configuration command. To remove the restriction, use the **no** form of this command.

ip pim neighbor-filter *access-list*

no ip pim neighbor-filter *access-list*

Syntax Description	<i>access-list</i>	Number or name of a standard IP access list that denies PIM packets from a source.
---------------------------	--------------------	--

ip pim query-interval

To configure the frequency of Protocol Independent Multicast (PIM) router query messages, use the **ip pim query-interval** interface configuration command. To return to the default interval, use the **no** form of this command.

ip pim query-interval *seconds*

no ip pim query-interval [*seconds*]

Syntax Description	<i>seconds</i>	Interval, in seconds, at which periodic PIM router query messages are sent. It can be a number from 1 to 65535. The default is 30 seconds.
---------------------------	----------------	--

ip pim register-rate-limit

To set a limit on the maximum number of Protocol Independent Multicast sparse mode (PIM-SM) register messages sent per second for each (S, G) routing entry, use the **ip pim register-rate-limit** global configuration command. To disable this limit, use the **no** form of this command.

ip pim register-rate-limit *rate*

no ip pim register-rate-limit

Syntax Description	<i>rate</i>	Maximum rate at which a router sends register messages per second. If no limit is defined, the router will not limit the rate of register messages sent.
---------------------------	-------------	--

ip pim register-source

To configure the IP source address of a register message to an interface address other than the outgoing interface address of the designated router (DR) leading toward the rendezvous point (RP), use the **ip pim register-source** global configuration command. To disable this configuration, use the **no** form of this command.

ip pim register-source *type number*

no ip pim register-source

Syntax Description	<i>type number</i>	Interface type and interface number that identify the IP source address of a register message.
---------------------------	--------------------	--

ip pim rp-address

To configure the address of a Protocol Independent Multicast (PIM) rendezvous point (RP) for a particular group, use the **ip pim rp-address** global configuration command. To remove an RP address, use the **no** form of this command.

```
ip pim rp-address rp-address [access-list] [override] [bidir]
```

```
no ip pim rp-address
```

Syntax Description		
	<i>rp-address</i>	IP address of a router to be a PIM RP. This is a unicast IP address in four-part, dotted notation.
	<i>access-list</i>	(Optional) Number or name of an access list that defines for which multicast groups the RP should be used.
	override	(Optional) Indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by Auto-RP.
	bidir	(Optional) Indicates that the multicast groups specified by the <i>access-list</i> argument are to operate in bidirectional mode. If the command is configured without this option, the groups specified will operate in PIM sparse mode.

ip pim rp-announce-filter

To filter incoming Auto-RP announcement messages coming from the rendezvous point (RP), use the **ip pim rp-announce-filter** global configuration command. To remove the filter, use the **no** form of this command.

```
ip pim rp-announce-filter rp-list access-list group-list access-list
```

```
no ip pim rp-announce-filter rp-list access-list group-list access-list
```

Syntax Description		
	rp-list <i>access-list</i>	Number or name of a standard access list of RP addresses that are allowable for the group ranges supplied in the group-list <i>access-list</i> .
	group-list <i>access-list</i>	Number or name of a standard access list that describes the multicast groups the RPs serve.

ip pim rp-candidate

To configure the router to advertise itself as a Protocol Independent Multicast (PIM) Version 2 candidate rendezvous point (RP) to the bootstrap router (BSR), use the **ip pim rp-candidate** global configuration command. To remove this router as an RP candidate, use the **no** form of this command.

```
ip pim rp-candidate type number [group-list access-list] [bidir]
```

```
no ip pim rp-candidate
```

Syntax Description	<i>type number</i>	IP address associated with this interface type and number is advertised as a candidate RP address.
	group-list <i>access-list</i>	(Optional) Standard IP access list number or name that defines the group prefixes that are advertised in association with the RP address. The access list name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid confusion with numbered access lists.
	bidir	(Optional) Indicates that the multicast groups specified by the <i>access-list</i> argument are to operate in bidirectional mode. If the command is configured without this option, the groups specified will operate in PIM sparse mode.

ip pim send-rp-announce

To use Auto-RP to configure groups for which the router will act as a rendezvous point (RP), use the **ip pim send-rp-announce** global configuration command. To deconfigure this router as an RP, use the **no** form of this command.

```
ip pim send-rp-announce type number scope tvl-value [group-list access-list] [interval seconds]
[bidir]
```

```
no ip pim send-rp-announce
```

Syntax Description	<i>type number</i>	Interface type and number that identify the RP address.
	scope <i>tvl-value</i>	Time-to-live (TTL) value that limits the number of Auto-RP announcements.
	group-list <i>access-list</i>	(Optional) Standard IP access list number or name that defines the group prefixes that are advertised in association with the RP address. The access list name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid confusion with numbered access lists.
	interval <i>seconds</i>	(Optional) Specifies the interval between RP announcements in seconds. The total hold time of the RP announcements is automatically set to three times the value of the interval. The default interval is 60 seconds.
	bidir	(Optional) Indicates that the multicast groups specified by the <i>access-list</i> argument are to operate in bidirectional mode. If the command is configured without this option, the groups specified will operate in Protocol Independent Multicast sparse mode (PIM-SM).

ip pim send-rp-discovery

To configure the router to be an rendezvous point (RP) mapping agent, use the **ip pim send-rp-discovery** global configuration command. To restore the default value, use the **no** form of this command.

```
ip pim send-rp-discovery scope ttl-value
```

```
no ip pim send-rp-discovery
```

Syntax Description	scope <i>ttl-value</i>	Time-to-live (TTL) value in the IP header that keeps the discovery messages within this number of hops.
--------------------	------------------------	---

ip pim spt-threshold

To configure when a Protocol Independent Multicast (PIM) leaf router should join the shortest path source tree for the specified group, use the **ip pim spt-threshold** global configuration command. To restore the default value, use the **no** form of this command.

```
ip pim spt-threshold {kbps | infinity} [group-list access-list]
```

```
no ip pim spt-threshold
```

Syntax Description	<i>kbps</i>	Traffic rate (in kbps).
	infinity	Causes all sources for the specified group to use the shared tree.
	group-list <i>access-list</i>	(Optional) Indicates which groups the threshold applies to. Must be an IP standard access list number or name. If the value is 0 or is omitted, the threshold applies to all groups.

ip pim ssm

To define the Source Specific Multicast (SSM) range of IP multicast addresses, use the **ip pim ssm** global configuration command. To disable the SSM range, use the **no** form of this command.

```
ip pim ssm {default | range access-list}
```

```
no ip pim ssm
```

Syntax Description	default	(Optional) Defines the SSM range access list to 232/8.
	range <i>access-list</i>	(Optional) Standard IP access list number or name defining the SSM range.

ip pim state-refresh disable

To disable the processing and forwarding of PIM Dense Mode State Refresh feature control messages on a Protocol Independent Multicast (PIM) router, use the **ip pim state-refresh disable** global configuration command. To re-enable the processing and forwarding of PIM Dense Mode State Refresh control messages, use the **no** form of this command.

ip pim state-refresh disable

no ip pim state-refresh disable

Syntax Description This command has no arguments or keywords.

ip pim state-refresh origination-interval

To configure the origination of and the interval for the PIM Dense Mode State Refresh feature control messages on a Protocol Independent Multicast (PIM) router, use the **ip pim state-refresh origination-interval** interface configuration command. To stop the origination of the PIM Dense Mode State Refresh control message, use the **no** form of this command.

ip pim state-refresh origination-interval *interval*

no ip pim state-refresh origination-interval

Syntax Description	<i>interval</i>	(Optional) The number of seconds between PIM Dense Mode State Refresh control messages. The default is 60 seconds. The available interval range is from 4 to 100 seconds.
---------------------------	-----------------	---

ip pim vc-count

To change the maximum number of virtual circuits (VCs) that Protocol Independent Multicast (PIM) can open, use the **ip pim vc-count** interface configuration command. To restore the default value, use the **no** form of this command.

ip pim vc-count *number*

no ip pim vc-count

Syntax Description	<i>number</i>	Maximum number of VCs that PIM can open. The default is 200 VCs. The range is from 1 to 65535.
---------------------------	---------------	--

ip pim version

To configure the Protocol Independent Multicast (PIM) version of the interface, use the **ip pim version** interface configuration command. To restore the default value, use the **no** form of this command.

ip pim version [1 | 2]

no ip pim version

Syntax Description

1	(Optional) Configures PIM Version 1.
2	(Optional) Configures PIM Version 2.

ip rgmp

To enable the Router-Port Group Management Protocol (RGMP) on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces, use the **ip rgmp** interface configuration command. To disable RGMP on the interfaces, use the **no** form of this command.

ip rgmp

no ip rgmp

Syntax Description

This command has no arguments or keywords.

ip rtp compression-connections

To specify the total number of Real-Time Transport Protocol (RTP) header compression connections that can exist on an interface, use the **ip rtp compression-connections** interface configuration command. To restore the default value, use the **no** form of this command.

ip rtp compression-connections *number*

no ip rtp compression-connections

Syntax Description

<i>number</i>	Number of RTP header compression connections the cache supports, in the range from 3 to 1000. The default is 32 connections (16 calls).
---------------	---

ip rtp header-compression

To enable Real-Time Transport Protocol (RTP) header compression, use the **ip rtp header-compression** interface configuration command. To disable RTP header compression, use the **no** form of this command.

ip rtp header-compression [*passive*]

no ip rtp header-compression [*passive*]

Syntax Description	passive	(Optional) Compresses outgoing RTP packets only if incoming RTP packets on the same interface are compressed.
---------------------------	----------------	---

ip sap cache-timeout

To limit how long a Session Announcement Protocol (SAP) cache entry stays active in the cache, use the **ip sap cache-timeout** global configuration command. To restore the default value, use the **no** form of this command.

ip sap cache-timeout *minutes*

no ip sap cache-timeout

Syntax Description	<i>minutes</i>	Time (in minutes) that a SAP cache entry is active in the cache.
---------------------------	----------------	--

ip sap listen

To enable the Cisco IOS software to listen to session directory announcements, use the **ip sap listen** interface configuration command. To disable the function, use the **no** form of this command.

ip sap listen

no ip sap listen

Syntax Description	This command has no arguments or keywords.
---------------------------	--

ip sdr cache-timeout

The **ip sdr cache-timeout** command is replaced by the **ip sap cache-timeout** command. See the description of the **ip sap cache-timeout** command in this chapter for more information.

ip sdr listen

The **ip sdr listen** command is replaced by the **ip sap listen** command. See the description of the **ip sap listen** command in this chapter for more information.

ip urd

To enable interception of TCP packets sent to the reserved URL Rendezvous Directory (URD) port 659 on an interface and processing of URD channel subscription reports, use the **ip urd** interface configuration command. To disable URD on an interface, use the **no** form of this command.

ip urd

no ip urd

Syntax Description This command has no arguments or keywords.

show frame-relay ip rtp header-compression

To show Frame Relay Real-Time Transport Protocol (RTP) header compression statistics, use the **show frame-relay ip rtp header-compression EXEC** command.

show frame-relay ip rtp header-compression [*interface type number*]

Syntax Description *interface type number* (Optional) Interface type and number.

show ip dvmrp route

To display the contents of the Distance Vector Multicast Routing Protocol (DVMRP) routing table, use the **show ip dvmrp route EXEC** command.

show ip dvmrp route [*name | ip-address | type number*]

Syntax Description

<i>name ip-address</i>	(Optional) Name or IP address of an entry in the DVMRP routing table.
<i>type number</i>	(Optional) Interface type and number.

show ip igmp groups

To display the multicast groups with receivers that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP), use the **show ip igmp groups** EXEC command.

```
show ip igmp groups [group-name | group-address | type number] [detail]
```

Syntax Description		
	<i>group-name</i>	(Optional) Name of the multicast group, as defined in the Domain Name System (DNS) hosts table.
	<i>group-address</i>	(Optional) Address of the multicast group. This is a multicast IP address in four-part, dotted notation.
	<i>type</i>	(Optional) Interface type.
	<i>number</i>	(Optional) Interface number.
	detail	(Optional) Provides a detailed description of the sources known through IGMP Version 3 (IGMPv3), IGMP v3lite, or URL Rendezvous Directory (URD).

show ip igmp interface

To display multicast-related information about an interface, use the **show ip igmp interface** EXEC command.

```
show ip igmp interface [type number]
```

Syntax Description		
	<i>type</i>	(Optional) Interface type.
	<i>number</i>	(Optional) Interface number.

show ip mcache

To display the contents of the IP fast-switching cache, use the **show ip mcache** EXEC command.

```
show ip mcache [group-address | group-name] [source-address | source-name]
```

Syntax Description		
	<i>group-address</i> <i>group-name</i>	(Optional) Displays the fast-switching cache for the single group. Can be either a Class D IP address or a Domain Name System (DNS) name.
	<i>source-address</i> <i>source-name</i>	(Optional) If the source address or name is also specified, displays a single multicast cache entry. Can be either a unicast IP address or a DNS name.

show ip mpacket

To display the contents of the circular cache-header buffer, use the **show ip mpacket** EXEC command.

```
show ip mpacket [group-address | group-name] [source-address | source-name] [detail]
```

Syntax Description		
<i>group-address</i> <i>group-name</i>	(Optional) Displays cache headers matching the specified group address or group name.	
<i>source-address</i> <i>source-name</i>	(Optional) Displays cache headers matching the specified source address or source name.	
detail	(Optional) In addition to the summary information, displays the rest of the IP header fields on an additional line, plus the first 8 bytes after the IP header (usually the User Datagram Protocol [UDP] port numbers).	

show ip mroute

To display the contents of the IP multicast routing table, use the **show ip mroute** EXEC command.

```
show ip mroute [group-address | group-name] [source-address | source-name] [type number]
[summary] [count] [active kbps]
```

Syntax Description		
<i>group-address</i> <i>group-name</i>	(Optional) IP address or name multicast group as defined in the Domain Name System (DNS) hosts table.	
<i>source-address</i> <i>source-name</i>	(Optional) IP address or name of a multicast source.	
<i>type number</i>	(Optional) Interface type and number.	
summary	(Optional) Displays a one-line, abbreviated summary of each entry in the IP multicast routing table.	
count	(Optional) Displays statistics about the group and source, including number of packets, packets per second, average packet size, and bits per second.	
active kbps	(Optional) Displays the rate that active sources are sending to multicast groups. Active sources are those sending at the <i>kbps</i> value or higher. The <i>kbps</i> argument defaults to 4 kbps.	

show ip pim bsr

To display the bootstrap router (BSR) information, use the **show ip pim bsr** EXEC command.

```
show ip pim bsr
```

Syntax Description	This command has no arguments or keywords.

show ip pim interface

To display information about interfaces configured for Protocol Independent Multicast (PIM), use the **show ip pim interface** EXEC command.

```
show ip pim interface [type number] [df | count] [rp-address] [detail]
```

Syntax Description		
	<i>type number</i>	(Optional) Interface type and number.
	df	(Optional) When Bidirectional PIM (bidir-PIM) is used, displays the IP address of the elected designated forwarder (DF) for each rendezvous point (RP) of an interface.
	count	(Optional) Number of packets received and sent out the interface.
	<i>rp-address</i>	(Optional) RP IP address.
	detail	(Optional) PIM details of each interface.

show ip pim neighbor

To list the Protocol Independent Multicast (PIM) neighbors discovered by the Cisco IOS software, use the **show ip pim neighbor** EXEC command.

```
show ip pim neighbor [type number]
```

Syntax Description		
	<i>type</i>	(Optional) Interface type.
	<i>number</i>	(Optional) Interface number.

show ip pim rp

To display active rendezvous points (RPs) that are cached with associated multicast routing entries, use the **show ip pim rp** EXEC command.

```
show ip pim rp [mapping | metric] [rp-address]
```

Syntax Description		
	mapping	(Optional) Displays all group-to-RP mappings of which the router is aware (either configured or learned from Auto-RP).
	metric	(Optional) Displays the unicast routing metric to the RPs configured statically or learned via Auto-RP or the bootstrap router (BSR).
	<i>rp-address</i>	(Optional) RP IP address.

show ip pim rp-hash

To display which rendezvous point (RP) is being selected for a specified group, use the **show ip pim rp-hash** EXEC command.

```
show ip pim rp-hash {group-address | group-name}
```

Syntax Description	<i>group-address</i> <i>group-name</i>	Displays the RP information for the specified group address or name as defined in the Domain Name System (DNS) hosts table.
---------------------------	--	---

show ip pim vc

To display ATM virtual circuit (VC) status information for multipoint VCs opened by Protocol Independent Multicast (PIM), use the **show ip pim vc** EXEC command.

```
show ip pim vc [group-address | group-name] [type number]
```

Syntax Description	<i>group-address</i> <i>group-name</i>	(Optional) IP multicast group or name. Displays only the single group.
	<i>type number</i>	(Optional) Interface type and number. Displays only the single ATM interface.

show ip rpf

To display how IP multicast routing does Reverse Path Forwarding (RPF), use the **show ip rpf** EXEC command.

```
show ip rpf {source-address | source-name} [metric]
```

Syntax Description	<i>source-address</i> <i>source-name</i>	Displays the RPF information for the specified source address or name.
	metric	(Optional) Displays the unicast routing metric.

show ip rtp header-compression

To show Real-Time Transport Protocol (RTP) header compression statistics, use the **show ip rtp header-compression** EXEC command.

```
show ip rtp header-compression [type number] [detail]
```

Syntax Description	<i>type number</i>	(Optional) Interface type and number.
	detail	(Optional) Displays details of each connection.

show ip sap

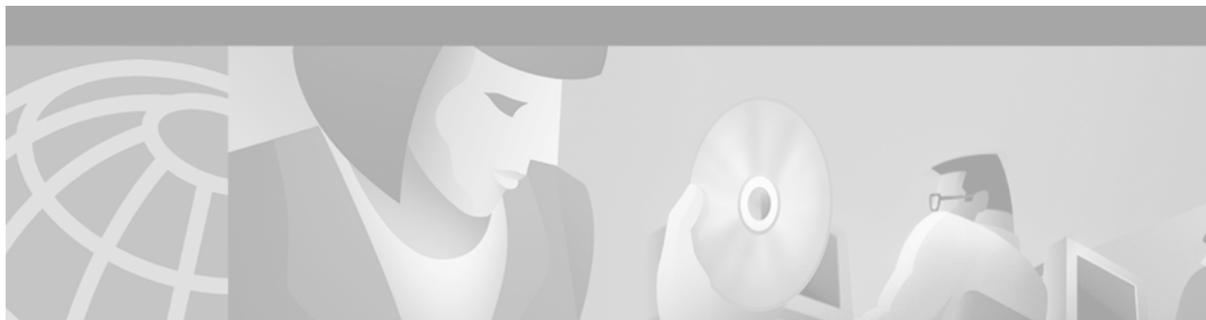
To display the Session Announcement Protocol (SAP) cache, use the **show ip sap** EXEC command.

```
show ip sap [group-address | "session-name" | detail]
```

Syntax	Description
<i>group-address</i>	(Optional) Displays the sessions defining the specified multicast group address.
" <i>session-name</i> "	(Optional) Displays the single session in detail format. The session name is enclosed in quotation marks (" ") that the user must enter.
detail	(Optional) Displays all sessions in detail format.

show ip sdr

The **show ip sdr** command is replaced by the **show ip sap** command. See the description of the **show ip sap** command in this chapter for more information.



Multicast Source Discovery Protocol Commands

This chapter describes the function and syntax of the Multicast Source Discovery Protocol (MSDP) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*.

clear ip msdp peer

To clear the TCP connection to the specified Multicast Source Discovery Protocol (MSDP) peer, use the **clear ip msdp peer** EXEC command.

```
clear ip msdp peer {peer-address | peer-name}
```

Syntax Description

<i>peer-address</i> <i>peer-name</i>	IP address or name of the MSDP peer to which the TCP connection is cleared.
--	---

clear ip msdp sa-cache

To clear Multicast Source Discovery Protocol (MSDP) Source-Active (SA) cache entries, use the **clear ip msdp sa-cache** EXEC command.

```
clear ip msdp sa-cache [group-address | group-name]
```

Syntax Description

<i>group-address</i> <i>group-name</i>	(Optional) Multicast group address or name for which Source-Active entries are cleared from the Source-Active cache.
--	--

clear ip msdp statistics

To clear statistics counters for one or all of the Multicast Source Discovery Protocol (MSDP) peers without resetting the sessions, use the **clear ip msdp statistics** EXEC command.

```
clear ip msdp statistics [peer-address | peer-name]
```

Syntax Description	<i>peer-address peer-name</i>	(Optional) Address or name of the MSDP peers whose statistics counters, reset count, and input/output count are cleared.
---------------------------	---------------------------------	--

ip msdp border

To configure a router that borders a Protocol Independent Multicast (PIM) sparse mode region and dense mode region to use Multicast Source Discovery Protocol (MSDP), use the **ip msdp border** global configuration command. To prevent this action, use the **no** form of this command.

```
ip msdp border sa-address type number
```

```
no ip msdp border sa-address type number
```

Syntax Description	<i>sa-address</i>	Active source IP address.
	<i>type number</i>	Interface type and number from which the IP address is derived and used as the rendezvous point (RP) address in Source-Active (SA) messages. Thus, MSDP peers can forward SA messages away from this border. The IP address of the interface is used as the originator ID, which is the RP field in the MSDP SA message.

ip msdp cache-sa-state

To have the router create Source-Active (SA) state, use the **ip msdp cache-sa-state** global configuration command. To prevent this action, use the **no** form of this command.

```
ip msdp cache-sa-state [list access-list]
```

```
no ip msdp cache-sa-state
```

Syntax Description	<i>list access-list</i>	(Optional) Extended IP access list number or name that defines which source/group pairs to cache.
---------------------------	-------------------------	---

ip msdp default-peer

To define a default peer from which to accept all Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages, use the **ip msdp default-peer** global configuration command. To remove the default peer, use the **no** form of this command.

```
ip msdp default-peer {peer-address | peer-name} [prefix-list list]
```

```
no ip msdp default-peer
```

Syntax Description	<i>peer-address</i> <i>peer-name</i>	IP address or Domain Name System (DNS) name of the MSDP default peer.
	prefix-list <i>list</i>	(Optional) Border Gateway Protocol (BGP) prefix list that specifies the peer will be a default peer only for the prefixes listed in the list specified by the <i>list</i> argument. A BGP prefix list must be configured for this prefix-list <i>list</i> keyword and argument to have any effect.

ip msdp description

To add descriptive text to the configuration for a Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp description** global configuration command. To remove the description, use the **no** form of this command.

```
ip msdp description {peer-name | peer-address} text
```

```
no ip msdp description {peer-name | peer-address}
```

Syntax Description	<i>peer-name</i> <i>peer-address</i>	Peer name or address to which this description applies.
	<i>text</i>	Description of the MSDP peer.

ip msdp filter-sa-request

To configure the router to send Source-Active (SA) request messages to the Multicast Source Discovery Protocol (MSDP) peer when a new joiner from a group becomes active, use the **ip msdp filter-sa-request** global configuration command. To prevent this action, use the **no** form of this command.

```
ip msdp filter-sa-request {peer-address | peer-name} [list access-list]
```

```
no ip msdp filter-sa-request {peer-address | peer-name}
```

Syntax Description	<i>peer-address</i> <i>peer-name</i>	IP address or name of the MSDP peer from which the local router requests SA messages when a new joiner for the group becomes active.
	list <i>access-list</i>	(Optional) Standard IP access list number or name that describes a multicast group address. If no access list is specified, all SA request messages are ignored.

ip msdp mesh-group

To configure a Multicast Source Discovery Protocol (MSDP) peer to be a member of a mesh group, use the **ip msdp mesh-group** global configuration command. To remove an MSDP peer from a mesh group, use the **no** form of this command.

```
ip msdp mesh-group mesh-name {peer-address | peer-name}
```

```
no ip msdp mesh-group mesh-name {peer-address | peer-name}
```

Syntax Description	<i>mesh-name</i>	Name of the mesh group.
	<i>peer-address</i> <i>peer-name</i>	IP address or name of the MSDP peer to be a member of the mesh group.

ip msdp originator-id

To allow a Multicast Source Discovery Protocol (MSDP) speaker that originates a Source-Active (SA) message to use the IP address of the interface as the rendezvous point (RP) address in the SA message, use the **ip msdp originator-id** global configuration command. To prevent the RP address from being derived in this way, use the **no** form of this command.

```
ip msdp originator-id type number
```

```
no ip msdp originator-id type number
```

Syntax Description	<i>type number</i>	Interface type and number on the local router, whose IP address is used as the RP address in SA messages.
---------------------------	--------------------	---

ip msdp peer

To configure a Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp peer** global configuration command. To remove the peer relationship, use the **no** form of this command.

```
ip msdp peer {peer-name | peer-address} [connect-source type number] [remote-as as-number]
```

```
no ip msdp peer {peer-name | peer-address}
```

Syntax Description		
	<i>peer-name</i> <i>peer-address</i>	Domain Name System (DNS) name or IP address of the router that is to be the MSDP peer.
	connect-source <i>type number</i>	(Optional) Interface type and number whose primary address becomes the source IP address for the TCP connection. This interface is on the router being configured.
	remote-as <i>as-number</i>	(Optional) Autonomous system number of the MSDP peer. This is used for display purposes only. There are cases where a peer might appear to be in another autonomous system (other than the one it really resides in) when you have an MSDP peering session but do not have a BGP peer session with that peer. In this case, if the prefix of the peer is injected by another autonomous system, it is displayed as the autonomous system number of the peer (and is misleading).

ip msdp redistribute

To configure which (S, G) entries from the multicast routing table are advertised in Source-Active (SA) messages originated to Multicast Source Discovery Protocol (MSDP) peers, use the **ip msdp redistribute** global configuration command. To remove the filter, use the **no** form of this command.

```
ip msdp redistribute [list access-list] [asn as-access-list] [route-map map-name]
```

```
no ip msdp redistribute
```

Syntax Description		
	list <i>access-list</i>	(Optional) Standard or extended IP access list number or name that controls which local sources are advertised and to which groups they send.
	asn <i>as-access-list</i>	(Optional) Standard or extended IP access list number in the range from 1 to 199. This access list number must also be configured in the ip as-path command.
	route-map <i>map-name</i>	(Optional) Defines the route map.

ip msdp sa-filter in

To configure an incoming filter list for Source-Active (SA) messages received from the specified Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp sa-filter in** global configuration command. To remove the filter, use the **no** form of this command.

```
ip msdp sa-filter in {peer-address | peer-name} [list access-list] [route-map map-name]
```

```
no ip msdp sa-filter in {peer-address | peer-name} [list access-list] [route-map map-name]
```

Syntax Description		
	<i>peer-address</i> <i>peer-name</i>	IP address or name of the MSDP peer from which the SA messages are filtered.
	list <i>access-list</i>	(Optional) IP access list number or name. If no access list is specified, all source/group pairs from the peer are filtered.
	route-map <i>map-name</i>	(Optional) Route map name. From the specified MSDP peer, passes only those SA messages that meet the match criteria in the route map <i>map-name</i> argument. If all match criteria are true, a permit keyword from the route map will pass routes through the filter. A deny keyword will filter routes.

ip msdp sa-filter out

To configure an outgoing filter list for Source-Active (SA) messages sent to the specified Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp sa-filter out** global configuration command. To remove the filter, use the **no** form of this command.

```
ip msdp sa-filter out {peer-address | peer-name} [list access-list] [route-map map-name]
```

```
no ip msdp sa-filter out {peer-address | peer-name} [list access-list] [route-map map-name]
```

Syntax Description		
	<i>peer-address</i> <i>peer-name</i>	IP address or DNS name of the MSDP peer to which the SA messages are filtered.
	list <i>access-list</i>	(Optional) Extended IP access list number or name. If no access list is specified, all source/group pairs are filtered. To the specified MSDP peer, passes only those SA messages that pass the extended access list. If both the list and the route-map keywords are used, all conditions must be true to pass any (S, G) pairs in outgoing SA messages.
	route-map <i>map-name</i>	(Optional) Route map name. To the specified MSDP peer, passes only those SA messages that meet the match criteria in the route map <i>map-name</i> argument. If all match criteria are true, a permit keyword from the route map will pass routes through the filter. A deny keyword will filter routes.

ip msdp sa-request

To configure the router to send Source-Active (SA) request messages to the Multicast Source Discovery Protocol (MSDP) peer when a new joiner from the group becomes active, use the **ip msdp sa-request** global configuration command. To prevent this action, use the **no** form of this command.

```
ip msdp sa-request {peer-address | peer-name}
```

```
no ip msdp sa-request {peer-address | peer-name}
```

Syntax Description	<i>peer-address peer-name</i>	IP address or name of the MSDP peer from which the local router requests SA messages when a new joiner for the group becomes active.
---------------------------	---------------------------------	--

ip msdp shutdown

To administratively shut down a configured Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp shutdown** global configuration command. To bring the peer back up, use the **no** form of this command.

```
ip msdp shutdown {peer-address | peer-name}
```

```
no ip msdp shutdown {peer-address | peer-name}
```

Syntax Description	<i>peer-address peer-name</i>	IP address or name of the MSDP peer to shut down.
---------------------------	---------------------------------	---

ip msdp ttl-threshold

To limit which multicast data packets are sent in Source-Active (SA) messages to a Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp ttl-threshold** global configuration command. To restore the default value, use the **no** form of this command.

```
ip msdp ttl-threshold {peer-address | peer-name} ttl-value
```

```
no ip msdp ttl-threshold {peer-address | peer-name}
```

Syntax Description	<i>peer-address peer-name</i>	IP address or name of the MSDP peer to which the <i>ttl-value</i> argument applies.
	<i>ttl-value</i>	Time-to-live (TTL) value. The default value of the <i>ttl-value</i> argument is 0, meaning all multicast data packets are forwarded to the peer until the TTL is exhausted.

show ip msdp count

To display the number of sources and groups originated in Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages, use the **show ip msdp count** EXEC command.

```
show ip msdp count [as-number]
```

Syntax Description	<i>as-number</i>	(Optional) Displays the number of sources and groups originated in SA messages from the specified autonomous system number.
---------------------------	------------------	---

show ip msdp peer

To display detailed information about the Multicast Source Discovery Protocol (MSDP) peer, use the **show ip msdp peer** EXEC command.

```
show ip msdp peer [peer-address | peer-name]
```

Syntax Description	<i>peer-address</i> <i>peer-name</i>	(Optional) Address or name of the MSDP peer for which information is displayed.
---------------------------	--	---

show ip msdp sa-cache

To display (S, G) state learned from Multicast Source Discovery Protocol (MSDP) peers, use the **show ip msdp sa-cache** EXEC command.

```
show ip msdp sa-cache [group-address | source-address | group-name | source-name]  
[group-address | source-address | group-name | source-name] [as-number]
```

Syntax Description	<i>group-address</i> <i>source-address</i> <i>group-name</i> <i>source-name</i>	(Optional) Group address, source address, group name, or source name of the group or source about which (S, G) information is displayed. If two address or names are specified, an (S, G) entry corresponding to those addresses is displayed. If only one group address is specified, all sources for that group are displayed. If no options are specified, the entire Source-Active (SA) cache is displayed.
	<i>as-number</i>	(Optional) Only state originated by the autonomous system number specified is displayed.

show ip msdp summary

To display Multicast Source Discovery Protocol (MSDP) peer status, use the **show ip msdp summary** EXEC command.

```
show ip msdp summary
```

Syntax Description This command has no arguments or keywords.

■ show ip msdp summary



PGM Host and Router Assist Commands

This chapter describes the function and syntax of the Pragmatic General Multicast (PGM) Host and Router Assist commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*.

clear ip pgm host

To reset Pragmatic General Multicast (PGM) Host connections to their default values and to clear traffic statistics, use the **clear ip pgm host** privileged EXEC command.

```
clear ip pgm host {defaults | traffic}
```

Syntax Description

defaults	Resets all PGM Host connections to their default values.
traffic	Clears all PGM Host traffic statistics.

clear ip pgm router

To clear Pragmatic General Multicast (PGM) traffic statistics, use the **clear ip pgm router** EXEC command.

```
clear ip pgm router [[traffic [type number]] | [rtx-state [group-address]]]
```

Syntax Description

traffic [type number]	(Optional) Interface type and number whose PGM traffic statistics are cleared. If no interface type and number are provided, all traffic statistics are cleared.
rtx-state [group-address]	(Optional) IP address of the multicast group whose PGM resend state is cleared. If no group address is provided, all resend state is cleared. Clearing resend state means the router will not forward any retransmissions corresponding to that state.

ip pgm host

To enable Pragmatic General Multicast (PGM) Host, use the **ip pgm host** global configuration command. To disable PGM Host and close all open PGM Host traffic sessions, use the **no** form of this command.

ip pgm host [**source-interface** {*type number*} | *connection-parameter*]

no ip pgm host

Syntax Description

source-interface <i>type number</i>	(Optional) Interface type and number on which to run PGM Host.
<i>connection-parameter</i>	(Optional) Configures advanced PGM Host connection parameters. The optional configuration parameters should only be configured by experts in PGM technology. See Table 21 for a comprehensive list of the optional connection parameters and their definitions.

Table 21 lists the available parameters for the *connection-parameter* argument. The parameters should be configured only by experts in PGM technology. Use the **no ip pgm host connection-parameter** command to return a parameter to its default value.

Table 21 ip pgm host Connection Parameters

Parameter	Definition
ihb-max <i>milliseconds</i>	(Optional) Sets the source path message (SPM) interheartbeat timer maximum. The default is 10000 milliseconds (ms).
ihb-min <i>milliseconds</i>	(Optional) Sets the SPM interheartbeat timer minimum. The default is 1000 ms.
join <i>milliseconds</i>	(Optional) Sets the amount of time the PGM Host waits, when running in router mode, for client requests. The default is 0 ms.
nak-gen-ivl <i>milliseconds</i>	(Optional) Sets the amount of time the PGM Host waits for a PGM negative acknowledgment (NAK) data packet. The default is 60000 ms.
nak-rb-ivl <i>milliseconds</i>	(Optional) Sets the amount of time the PGM Host waits before sending a PGM NAK data packet. The default is 500 ms.
nak-rdata-ivl <i>milliseconds</i>	(Optional) Sets the amount of time the PGM Host waits for a re-sent PGM NAK (NAK RDATA) data packet. The default is 2000 ms.
nak-rpt-ivl <i>milliseconds</i>	(Optional) Sets the amount of time the PGM Host waits for a PGM NAK confirmation (NAK NCF) data packet. The default is 2000 ms.
ncf-max <i>packets-per-second</i>	(Optional) Sets the maximum number of PGM NAK confirmation data packets (NAK NCFs) the PGM Host sends per second. The default is infinite.

Table 21 ip pgm host Connection Parameters (continued)

Parameter	Definition
rx-buffer-mgmt {full minimum}	(Optional) Sets the type of receive data buffers (full or minimum) for the PGM Host. The default is minimum.
spm-ambient-ivl <i>milliseconds</i>	(Optional) Sets the amount of time the PGM Host waits for a PGM SPM ambient data packet. The default is 6000 ms.
spm-rpt-ivl <i>milliseconds</i>	(Optional) Sets the amount of time the PGM Host waits for a PGM SPM repeat data packet. The default is 3000 ms.
stream-type {apdu byte}	(Optional) Sets the data stream type (apdu or byte) for the PGM Host. The default is apdu.
tpdu-size <i>number</i>	(Optional) Sets the size of the source transport data unit (TPDU) for the PGM Host. The available range is 41 through 16384 bytes. The default is 1400 bytes.
ttl <i>number</i>	(Optional) Sets the time-to-live (TTL) value on the PGM Host for sent multicast data packets. The default is 255 hops. The TTL value for a packet is decremented by 1 as the packet passes through a router.
tx-buffer-mgmt {keep return}	(Optional) Sets the type of transmit data buffers (keep or return) for the PGM Host. The default is return.
tx-adv-method {data time}	(Optional) Sets the type of advanced transmit window method (data or time) for the PGM Host. The default is time.
txw-adv-secs <i>milliseconds</i>	(Optional) Sets the size of advanced transmit window for the PGM Host. The default is 6000 ms.
txw-rte <i>bytes-per-second</i>	(Optional) Sets the data transmit rate for the PGM Host. The default is 16,384 bytes per second.
txw-secs <i>milliseconds</i>	(Optional) Sets the data transmit window size for the PGM Host. The default is 30,000 ms.
txw-timeout-max <i>milliseconds</i>	(Optional) Sets the amount of time the PGM Host waits for data packets, even if the PGM Host receives PGM NAK data packets. The default is 3,600,000 ms.

ip pgm router

To enable Pragmatic General Multicast (PGM) Router Assist and thereby allow PGM to operate more efficiently on the router, use the **ip pgm router** interface configuration command. To disable PGM Router Assist for the interface, use the **no** form of this command.

```
ip pgm router
```

```
no ip pgm router
```

Syntax Description This command has no arguments or keywords.

show ip pgm host defaults

To display the default values for Pragmatic General Multicast (PGM) Host traffic, use the **show ip pgm host defaults** EXEC command.

```
show ip pgm host defaults
```

Syntax Description This command has no arguments or keywords.

show ip pgm host sessions

To display open Pragmatic General Multicast (PGM) Host traffic sessions, use the **show ip pgm host sessions** EXEC command.

```
show ip pgm host sessions [session-number | group-address]
```

Syntax Description	<i>session-number</i>	(Optional) PGM Host traffic session number.
	<i>group-address</i>	(Optional) PGM Host multicast group address.

show ip pgm host traffic

To display Pragmatic General Multicast (PGM) Host traffic statistics, use the **show ip pgm host traffic** EXEC command.

```
show ip pgm host traffic
```

Syntax Description This command has no arguments or keywords.

show ip pgm router

To display Pragmatic General Multicast (PGM) Reliable Transport Protocol state and statistics, use the **show ip pgm router** EXEC command.

```
show ip pgm router [[interface [type number]] | [state [group-address]] | [traffic [type number]]]  
[verbose]
```

Syntax	Description
interface <i>[type number]</i>	(Optional) Displays interfaces on which PGM Router Assist is configured.
state <i>[group-address]</i>	(Optional) Displays PGM resend state information per transport session identifier (TSI). If no group address is specified, resend state for all groups is shown.
traffic <i>[type number]</i>	(Optional) Displays PGM packet counters. If no interface type and number are specified, traffic on all interfaces is displayed. These statistics do not reflect the number of PGM data packets (ODATA) that are forwarded in a session, because these are forwarded transparently by IP multicast.
verbose	(Optional) Displays extended information about outgoing interface lists, timers, Forward Error Connections (FECs), and Designated Local Retransmitters (DLRs).

■ show ip pgm router



Unidirectional Link Routing Commands

This chapter describes the function and syntax of the unidirectional link routing (UDLR) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*.

ip igmp helper-address (UDL)

To configure Internet Group Management Protocol (IGMP) helping as required for IGMP unidirectional link routing (UDLR), use the **ip igmp helper-address** interface configuration command. To disable such report forwarding, use the **no** form of this command.

ip igmp helper-address udl *type number*

no ip igmp helper-address

Syntax Description	udl <i>type number</i>	Interface type and number of a unidirectional interface.
---------------------------	-------------------------------	--

ip igmp mroute-proxy

To enable Internet Group Management Protocol (IGMP) report forwarding of proxied (*, G) mroute entries, use the **ip igmp mroute-proxy** interface configuration command. To disable this service, use the **no** form of this command.

ip igmp mroute-proxy *type number*

no ip igmp mroute-proxy *type number*

Syntax Description	<i>type number</i>	Interface type and number.
---------------------------	--------------------	----------------------------

ip igmp proxy-service

To enable the mroute proxy service, use the **ip igmp proxy-service** interface configuration command. To disable forwarding, use the **no** form of this command.

ip igmp proxy-service

no ip igmp proxy-service

Syntax Description This command has no arguments or keywords.

ip igmp unidirectional-link

To configure an interface to be unidirectional and enable it for Internet Group Management Protocol (IGMP) unidirectional link routing (UDLR), use the **ip igmp unidirectional-link** interface configuration command. To disable the unidirectional link (UDL), use the **no** form of this command.

ip igmp unidirectional-link

no ip igmp unidirectional-link

Syntax Description This command has no arguments or keywords.

ip multicast default-rpf-distance

When configuring Internet Group Management Protocol (IGMP) unidirectional link routing (UDLR), to change the distance given to the default Reverse Path Forwarding (RPF) interface, use the **ip multicast default-rpf-distance** global configuration command. To restore the default value, use the **no** form of this command.

ip multicast default-rpf-distance *distance*

no ip multicast default-rpf-distance

Syntax Description *distance* Distance given to the default RPF interface. The default value is 15.

show ip igmp udldr

To display unidirectional link routing (UDLR) information for directly connected multicast groups on interfaces that have a unidirectional link (UDL) helper address configured, use the **show ip igmp udldr EXEC** command.

```
show ip igmp udldr [group-name | group-address | type number]
```

Syntax Description		
	<i>group-name</i> <i>group-address</i>	(Optional) Name or address of the multicast group for which to show UDLR information.
	<i>type number</i>	(Optional) Interface type and number for which to show UDLR information.

tunnel udldr address-resolution

To enable the forwarding of the Address Resolution Protocol (ARP) and Next Hop Resolution Protocol (NHRP) over a unidirectional link (UDL), use the **tunnel udldr address-resolution** interface configuration command. To disable forwarding, use the **no** form of this command.

```
tunnel udldr address-resolution
```

```
no tunnel udldr address-resolution
```

Syntax Description	This command has no arguments or keywords.
--------------------	--

tunnel udldr receive-only

To configure a unidirectional, generic routing encapsulation (GRE) tunnel to act as a back channel that can receive messages, when another interface is configured for unidirectional link routing (UDLR) to send messages, use the **tunnel udldr receive-only** interface configuration command. To remove the tunnel, use the **no** form of this command.

```
tunnel udldr receive-only type number
```

```
no tunnel udldr receive-only type number
```

Syntax Description	<i>type number</i>	Interface type and number. The <i>type</i> and <i>number</i> arguments must match the unidirectional send-only interface type and number specified by the interface command. Thus, when packets are received over the tunnel, the upper layer protocols will treat the packets as if they are received over the unidirectional send-only interface.
--------------------	--------------------	--

tunnel udlr send-only

To configure a unidirectional, generic routing encapsulation (GRE) tunnel to act as a back channel that can send messages, when another interface is configured for unidirectional link routing (UDLR) to receive messages, use the **tunnel udlr send-only** interface configuration command. To remove the tunnel, use the **no** form of this command.

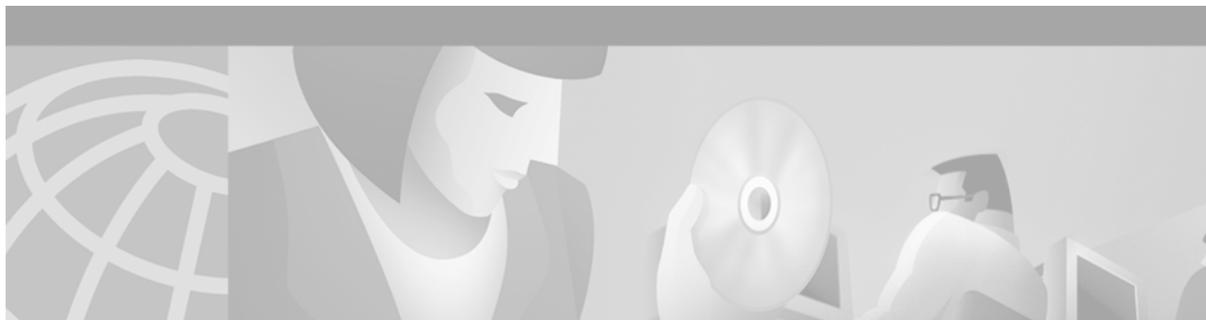
tunnel udlr send-only *type number*

no tunnel udlr send-only *type number*

Syntax Description

type number

Interface type and number. The *type* and *number* arguments must match the unidirectional receive-only interface type and number specified by the **interface** command. Thus, when packets are sent by upper layer protocols over the interface, they will be redirected and sent over this GRE tunnel.



IP Multicast Tools Commands

This chapter describes the function and syntax of the IP multicast tools commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*.

beacon

To change the frequency, duration, or scope of beacon messages that the Manager sends to Test Senders and Test Receivers during a multicast routing monitor test, use the **beacon** manager configuration command. To restore the default value, use the **no** form of this command.

```
beacon [interval seconds] [holdtime seconds] [ttl ttl-value]
```

```
no beacon [interval seconds] [holdtime seconds] [ttl ttl-value]
```

Syntax Description		
interval <i>seconds</i>	(Optional) Frequency of beacon messages (in seconds). The default value is 60 seconds, meaning one beacon message every 60 seconds.	
holdtime <i>seconds</i>	(Optional) Length of the test period in seconds. The Test Sender and Test Receiver are respectively sending and receiving test data constantly during the hold time. The default value is 1 day (86,400 seconds).	
ttl <i>ttl-value</i>	(Optional) Time-to-live (TTL) value of the beacon messages. The default value is 32 hops.	

clear ip mrm status-report

To clear the status report cache buffer, use the **clear ip mrm status-report EXEC** command.

```
clear ip mrm status-report [ip-address]
```

Syntax Description		
<i>ip-address</i>	(Optional) Address of the Test Receiver. Clears only those status reports received from the Test Receiver that has this IP address. If no address is specified, all status reports are cleared from the cache buffer.	

ip mrm

To configure an interface to operate as a Test Sender or Test Receiver, or both, for Multicast Routing Monitor (MRM), use the **ip mrm** interface configuration command. To remove the interface as a Test Sender or Test Receiver, use the **no** form of this command.

```
ip mrm { test-sender | test-receiver | test-sender-receiver }
```

```
no ip mrm { test-sender | test-receiver | test-sender-receiver }
```

Syntax Description		
	test-sender	Configures the interface to be a Test Sender.
	test-receiver	Configures the interface to be a Test Receiver.
	test-sender-receiver	Configures the interface to be both a Test Sender and Test Receiver (for different groups).

ip mrm accept-manager

To configure a Test Sender or Test Receiver to accept requests only from Managers that pass an access list, use the **ip mrm accept-manager** global configuration command. To remove the restriction, use the **no** form of this command.

```
ip mrm accept-manager { access-list } [test-sender | test-receiver]
```

```
no ip mrm accept-manager { access-list }
```

Syntax Description		
	<i>access-list</i>	Number or name of IP access list applied to the Managers.
	test-sender	(Optional) The access list applies only to the Test Sender.
	test-receiver	(Optional) The access list applies only to the Test Receiver.

ip mrm manager

To identify a Multicast Routing Monitor (MRM) test and enter the mode in which you specify the test parameters, use the **ip mrm manager** global configuration command. To remove the test, use the **no** form of this command.

```
ip mrm manager test-name
```

```
no ip mrm manager test-name
```

Syntax Description		
	<i>test-name</i>	Name of the group of MRM test parameters that follow.

manager

To specify that an interface is the Manager for Multicast Routing Monitor (MRM), and to specify the multicast group address the Test Receiver will listen to, use the **manager** manager configuration command. To remove the Manager or group address, use the **no** form of this command.

manager *type number* **group** *ip-address*

no manager *type number* **group** *ip-address*

Syntax Description

<i>type number</i>	Interface type and number of the Manager. The IP address associated with this interface is the source address of the Manager.
group <i>ip-address</i>	IP multicast group address that the Test Receiver will listen to.

mrinfo

To query which neighboring multicast routers are “peering” with the local router, use the **mrinfo** EXEC command.

mrinfo [*host-name | host-address*] [*source-address | interface*]

Syntax Description

<i>host-name host-address</i>	(Optional) Queries the Domain Name System (DNS) name or IP address of the multicast router. If omitted, the router queries itself.
<i>source-address</i>	(Optional) Source address used on mrinfo requests. If omitted, the source is based on the outbound interface for the destination.
<i>interface</i>	(Optional) Source interface used on mrinfo requests. If omitted, the source is based on the outbound interface for the destination.

mrmm

To start or stop a Multicast Routing Monitor (MRM) test, use the **mrmm** EXEC command.

mrmm *test-name* {**start** | **stop**}

Syntax Description

<i>test-name</i>	Name of the MRM test, as defined by the ip mrmm manager command.
start	Starts the MRM test specified by the <i>test-name</i> argument.
stop	Stops the MRM test specified by the <i>test-name</i> argument.

mstat

To display IP multicast packet rate and loss information, use the **mstat** user EXEC command.

```
mstat {source-name | source-address} [destination-name | destination-address] [group-name | group-address]
```

Syntax Description

<i>source-name</i> <i>source-address</i>	Domain Name System (DNS) name or the IP address of the multicast-capable source.
<i>destination-name</i> <i>destination-address</i>	(Optional) DNS name or address of the destination. If omitted, the command uses the system at which the command is typed.
<i>group-name</i> <i>group-address</i>	(Optional) DNS name or multicast address of the group to be displayed. Default address is 224.2.0.1 (the group used for multicast backbone [MBONE] Audio).

mtrace

To trace the path from a source to a destination branch for a multicast distribution tree, use the **mtrace** user EXEC command.

```
mtrace {source-name | source-address} [destination-name | destination-address] [group-name | group-address]
```

Syntax Description

<i>source-name</i> <i>source-address</i>	Domain Name System (DNS) name or the IP address of the multicast-capable source. This is a unicast address of the beginning of the path to be traced.
<i>destination-name</i> <i>destination-address</i>	(Optional) DNS name or address of the unicast destination. If omitted, the mtrace starts from the system at which the command is typed.
<i>group-name</i> <i>group-address</i>	(Optional) DNS name or multicast address of the group to be traced. Default address is 224.2.0.1 (the group used for multicast backbone [MBONE] Audio). When address 0.0.0.0 is used, the software invokes a weak mtrace . A weak mtrace is one that follows the RPF path to the source, regardless of whether any router along the path has multicast routing table state.

receivers

To establish Test Receivers for Multicast Routing Monitor (MRM), use the **receivers** command in manager configuration mode. To restore the default values, use the **no** form of this command.

```
receivers {access-list} [sender-list {access-list} [packet-delay]] [window seconds] [report-delay seconds] [loss percentage] [no-join] [monitor | poll]
```

```
no receivers {access-list} [sender-list {access-list} [packet-delay]] [window seconds] [report-delay seconds] [loss percentage] [no-join] [monitor | poll]
```

Syntax	Description
<i>access-list</i>	IP named or numbered access list that establishes the Test Receivers. Only these Test Receivers are subject to the other keywords and arguments specified in this command.
sender-list <i>access-list</i>	(Optional) Specifies the sources that the Test Receiver should monitor. If the named or numbered access list matches any access list specified in the senders command, the associated packet-delay <i>milliseconds</i> keyword and argument of that senders command are used in this command. Otherwise, the <i>packet-delay</i> argument is required in this receivers command.
<i>packet-delay</i>	(Optional) Specifies the delay between test packets (in milliseconds). If the sender-list access list matches any access list specified in the senders command, the associated packet-delay <i>milliseconds</i> keyword and argument of that senders command are used in this command. Otherwise, the <i>packet-delay</i> argument is required in this receivers command.
window <i>seconds</i>	(Optional) Duration (in seconds) of a test period. This is a sliding window of time in which packet count is collected, so that the loss percentage can be calculated. Default is 5 seconds.
report-delay <i>seconds</i>	(Optional) Delay (in seconds) between staggered status reports from multiple Test Receivers to the Manager. The delay prevents multiple receivers from sending status reports to the Manager at the same time for the same failure. Receiver 1 sends status, <i>seconds</i> later Receiver 2 sends status, <i>seconds</i> later Receiver 3 sends status, and so on. This value is relevant only if there are multiple Test Receivers. The default is 1 second.
loss <i>percentage</i>	(Optional) Threshold percentage of packet loss required before a status report is triggered. The default is 0 percent, which means that a status report is sent for any packet loss. (This value is not applied to packet duplication; a fault report is sent for any duplicated packets.)
no-join	(Optional) Specifies that the Test Receiver does not join the monitored group. The default is that the Test Receiver joins the monitored group.
monitor poll	(Optional) Specifies whether the Test Receiver monitors the test group or polls for receiver statistics. The monitor keyword means the Test Receiver reports only if the test criteria are met. The poll keyword means the Test Receiver sends status reports regularly, whether test criteria are met or not. The default is the monitor keyword.

senders

To configure Test Sender parameters used in Multicast Routing Monitor (MRM), use the **senders** manager configuration command. To restore the default values, use the **no** form of this command.

```
senders {access-list} [packet-delay milliseconds] [rtp | udp] [target-only | all-multicasts | all-test-senders] [proxy_src]
```

```
no senders {access-list} [packet-delay milliseconds] [rtp | udp] [target-only | all-multicasts | all-test-senders] [proxy_src]
```

Syntax Description	<i>access-list</i>	IP named or numbered access list that defines which Test Senders are involved in the test and which Test Senders these parameters apply to.
	packet-delay <i>milliseconds</i>	(Optional) Specifies the delay between test packets (in milliseconds). The default is 200 milliseconds, which results in 5 packets per second.
	rtp udp	(Optional) Encapsulation of test packets, either Real-Time Transport Protocol (RTP-encapsulated or User Datagram Protocol (UDP)-encapsulated. The default is RTP-encapsulated.
	target-only	(Optional) Specifies that test packets are sent out on the targeted interface only (that is, the interface with the IP address that is specified in the Test Sender request target field). By default, test packets are sent as described in the all-multicasts keyword.
	all-multicasts	(Optional) Specifies that the test packets are sent out on all interfaces that are enabled with IP multicast. This is the default way that test packets are sent.
	all-test-senders	(Optional) Specifies that test packets are sent out on all interfaces that have test-sender mode enabled. By default, test packets are sent as described in the all-multicasts keyword.
	<i>proxy_src</i>	(Optional) Source IP address for which the Test Sender will proxy test packets. Use this if you want to test, for a specific source, whether the multicast distribution tree is working.

show ip mrm interface

To display Test Sender or Test Receiver information about Multicast Routing Monitor (MRM), use the **show ip mrm interface EXEC** command.

```
show ip mrm interface [type number]
```

Syntax Description	<i>type number</i>	(Optional) Displays Test Sender or Test Receiver information for the specified interface type and number. If no interface is specified, information about all Test Senders and Test Receivers is displayed.
---------------------------	--------------------	---

show ip mrm manager

To display test information for Multicast Routing Monitor (MRM), use the **show ip mrm manager EXEC** command.

```
show ip mrm manager [test-name]
```

Syntax Description	<i>test-name</i>	(Optional) Name of the MRM test (as specified in the ip mrm manager command) for which to display information. If no name is specified, information about all Managers is displayed.
---------------------------	------------------	---

show ip mrm status-report

To display Multicast Routing Monitor (MRM) status reports of errors in the circular cache buffer, use the **show ip mrm status-report** EXEC command.

```
show ip mrm status-report [ip-address]
```

Syntax Description		
	<i>ip-address</i>	(Optional) Displays information received from this IP address only. If no address is specified, all status reports in the cache buffer are displayed.

udp-port

To change User Datagram Protocol (UDP) port numbers to which a Test Sender sends test packets or a Test Receiver sends status reports, use the **udp-port** manager configuration command. To remove the port numbers, use the **no** form of this command.

```
udp-port [test-packet port-number] [status-report port-number]
```

```
no udp-port [test-packet port-number] [status-report port-number]
```

Syntax Description		
	test-packet <i>port-number</i>	(Optional) UDP port number to which test packets are sent by a Test Sender. The port number must be even if the packets are Real-Time Transport Protocol (RTP)-encapsulated. The default port number is 16384.
	status-report <i>port-number</i>	(Optional) UDP port number to which status reports are sent by a Test Receiver. The port number must be odd if the packets are RTP Control Protocol (RTCP)-encapsulated. The default port number is 65535.



AppleTalk and Novell IPX



AppleTalk Commands: **access-list additional-zones** Through **appletalk zone**

This chapter describes the function and syntax of the AppleTalk commands: **access-list additional-zones** through **appletalk zone**. For more information about these commands, refer to the corresponding chapter in the *Cisco IOS AppleTalk and Novell IPX Command Reference*.

access-list additional-zones

To define the default action to take for access checks that apply to zones, use the **access-list additional-zones** command in global configuration mode. To remove an access list, use the **no** form of this command.

```
access-list access-list-number {deny | permit} additional-zones
```

```
no access-list access-list-number additional-zones
```

Syntax Description		
	<i>access-list-number</i>	Number of the access list. This is a decimal number from 600 to 699.
	deny	Denies access if the conditions are matched.
	permit	Permits access if the conditions are matched.

access-list cable-range

To define an AppleTalk access list for a cable range (for extended networks only), use the **access-list cable-range** command in global configuration mode. To remove an access list, use the **no** form of this command.

```
access-list access-list-number {deny | permit} cable-range cable-range  
[broadcast-deny | broadcast-permit]
```

```
no access-list access-list-number [{deny | permit} cable-range cable-range  
[broadcast-deny | broadcast-permit]]
```

Syntax Description

<i>access-list-number</i>	Number of the access list. This is a decimal number from 600 to 699.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
<i>cable-range</i>	Cable range value. The argument specifies the start and end of the cable range, separated by a hyphen. These values are decimal numbers from 1 to 65279. The starting network number must be less than or equal to the ending network number.
broadcast-deny	(Optional) Denies access to broadcast packets if the conditions are matched.
broadcast-permit	(Optional) Permits access to broadcast packets if the conditions are met.

access-list includes

To define an AppleTalk access list that overlaps any part of a range of network numbers or cable ranges (for both extended and nonextended networks), use the **access-list includes** command in global configuration mode. To remove an access list, use the **no** form of this command.

```
access-list access-list-number {deny | permit} includes cable-range
[broadcast-deny | broadcast-permit]
```

```
no access-list access-list-number {deny | permit} includes cable-range
[broadcast-deny | broadcast-permit]
```

Syntax Description

<i>access-list-number</i>	Number of the access list. This is a decimal number from 600 to 699.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
<i>cable-range</i>	Cable range or network number. The argument specifies the start and end of the cable range, separated by a hyphen. These values are decimal numbers from 1 to 65279. The starting network number must be less than or equal to the ending network number. To specify a network number, set the starting and ending network numbers to the same value.
broadcast-deny	(Optional) Denies access to broadcast packets if the conditions are matched.
broadcast-permit	(Optional) Permits access to broadcast packets if the conditions are met.

access-list nbp

To define an AppleTalk access list entry for a particular Name Binding Protocol (NBP) named entity, class of NBP named entities, NBP packet type, or NBP named entities that belong to a specific zone, use the **access-list nbp** command in global configuration mode. To remove an NBP access list entry from the access list, use the **no** form of this command.

```
access-list access-list-number {deny | permit} nbp sequence-number {BrRq | FwdRq | Lookup
| LkReply | object string | type string | zone string}
```

```
no access-list access-list-number {deny | permit} nbp sequence-number {BrRq | FwdRq |
Lookup | LkReply | object string | type string | zone string}
```

Syntax Description

<i>access-list-number</i>	Number of the access list. This is a decimal number from 600 to 699.
deny	Denies access if conditions are matched.
permit	Permits access if conditions are matched.
<i>sequence-number</i>	Number used to tie together two or three portions of an NBP name tuple and to keep track of the number of access-list nbp entries in an access list. Each command entry must have a sequence number.
BrRq	Broadcast Request packet type.
FwdRq	Forward Request packet type.
Lookup	Lookup packet type.
LkReply	Lookup Reply packet type.
object	Characterizes <i>string</i> as the portion of an NBP name that identifies a particular object or named entity.
<i>string</i>	Portion of an NBP name identifying the object , type , or zone of a named entity. The name string can be up to 32 characters long, and it can include special characters from the Apple Macintosh character set. To include a special character, type a colon followed by two hexadecimal characters. For an NBP name with a leading space, enter the first character as the special sequence :20.
type	Characterizes <i>string</i> as the portion of an NBP name that identifies a category or type of named entity.
zone	Characterizes <i>string</i> as the portion of an NBP name that identifies an AppleTalk zone .

access-list network

To define an AppleTalk access list for a single network number (that is, for a nonextended network), use the **access-list network** command in global configuration mode. To remove an access list, use the **no** form of this command.

```
access-list access-list-number {deny | permit} network network
[broadcast-deny | broadcast-permit]
```

```
no access-list access-list-number {deny | permit} network network
[broadcast-deny | broadcast-permit]
```

Syntax Description

<i>access-list-number</i>	Number of the access list. This is a decimal number from 600 to 699.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
<i>network</i>	AppleTalk network number.
broadcast-deny	(Optional) Denies access to broadcast packets if the conditions are matched.
broadcast-permit	(Optional) Permits access to broadcast packets if the conditions are met.

access-list other-access

To define the default action to take for subsequent access checks that apply to networks or cable ranges, use the **access-list other-access** command in global configuration mode. To remove an access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} **other-access**

no access-list *access-list-number* **other-access**

Syntax Description

<i>access-list-number</i>	Number of the access list. This is a decimal number from 600 to 699.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.

access-list other-nbps

To define the default action to take for access checks that apply to Name Binding Protocol (NBP) packets from named entities not otherwise explicitly denied or permitted, use the **access-list other-nbps** command in global configuration mode. To remove an access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} **other-nbps**

no access-list *access-list-number* {**deny** | **permit**} **other-nbps**

Syntax Description

<i>access-list-number</i>	Number of the access list for AppleTalk. This is a decimal number from 600 to 699.
deny	Denies access if conditions are matched.
permit	Permits access if conditions are matched.

access-list within

To define an AppleTalk access list for an extended or a nonextended network whose network number or cable range is included entirely within the specified cable range, use the **access-list within** command in global configuration mode. To remove this access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} **within** *cable-range*

no access-list *access-list-number* [{**deny** | **permit**} **within** *cable-range*]

Syntax Description

<i>access-list-number</i>	Number of the access list. This is a decimal number from 600 to 699.
deny	Denies access if the conditions are matched.

permit	Permits access if the conditions are matched.
<i>cable-range</i>	Cable range or network number. The argument specifies the start and end of the cable range, separated by a hyphen. These values are decimal numbers from 1 to 65279. The starting network number must be less than or equal to the ending network number. To specify a network number, set the starting and ending network numbers to the same value.

access-list zone

To define an AppleTalk access list that applies to a zone, use the **access-list zone** command in global configuration mode. To remove an access list, use the **no** form of this command.

```
access-list access-list-number {deny | permit} zone zone-name
```

```
no access-list access-list-number [{deny | permit} zone zone-name]
```

Syntax Description

<i>access-list-number</i>	Number of the access list. This is a decimal number from 600 to 699.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
<i>zone-name</i>	Name of the zone. The name can include special characters from the Apple Macintosh character set. To include a special character, type a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20.

appletalk access-group

To assign an access list to an interface, use the **appletalk access-group** command in interface configuration mode. To remove the access list, use the **no** form of this command.

```
appletalk access-group access-list-number [in | out]
```

```
no appletalk access-group access-list-number
```

Syntax Description

<i>access-list-number</i>	Number of the access list. This is a decimal number from 600 to 699.
in	(Optional) Filters on incoming packets.
out	(Optional) Filters on outgoing packets. This is the default direction.

appletalk address

To enable nonextended AppleTalk routing on an interface, use the **appletalk address** command in interface configuration mode. To disable nonextended AppleTalk routing, use the **no** form of this command.

appletalk address *network.node*

no appletalk address [*network.node*]

Syntax Description

network.node

AppleTalk network address assigned to the interface. The argument *network* is the 16-bit network number in the range 0 to 65279. The argument *node* is the 8-bit node number in the range 0 to 254. Both numbers are decimal and separated by a period.

appletalk alternate-addressing

To display network numbers in a two-octet format, use the **appletalk alternate-addressing** command in global configuration mode. To return to displaying network numbers in the format *network.node*, use the **no** form of this command.

appletalk alternate-addressing

no appletalk alternate-addressing

Syntax Description

This command has no arguments or keywords.

appletalk arp interval

To specify the time interval between retransmissions of Address Resolution Protocol (ARP) packets, use the **appletalk arp interval** command in global configuration mode. To restore both default intervals, use the **no** form of this command.

appletalk arp [**probe** | **request**] **interval** *interval*

no appletalk arp [**probe** | **request**] **interval** *interval*

Syntax Description

probe

(Optional) Interval to be used with AppleTalk Address Resolution Protocol (AARP) requests that are trying to determine the address of the local router when the Cisco IOS software is being configured. If you omit **probe** and **request**, **probe** is the default.

request	(Optional) Indicates that the interval specified is to be used when AARP is attempting to determine the hardware address of another node so that AARP can deliver a packet.
<i>interval</i>	Interval, in milliseconds, between AARP transmissions. The minimum value is 33 milliseconds. When used with the probe keyword, the default interval is 200 milliseconds. When used with the request keyword, the default interval is 1000 milliseconds.

appletalk arp retransmit-count

To specify the number of AppleTalk Address Resolution Protocol (AARP) probe or request transmissions, use the **appletalk arp retransmit-count** command in global configuration mode. To restore both default values, use the **no** form of this command.

appletalk arp [**probe** | **request**] **retransmit-count** *number*

no appletalk arp [**probe** | **request**] **retransmit-count** *number*

Syntax Description		
probe	(Optional) Indicates that the number specified is to be used with AARP requests that are trying to determine the address of the local router when the Cisco IOS software is being configured. If you omit probe and request , probe is the default.	
request	(Optional) Indicates that the number specified is to be used when AARP is attempting to determine the hardware address of another node so that AARP can deliver a packet.	
<i>number</i>	Number of AARP retransmissions that will occur. The minimum number is 1. When used with the probe keyword, the default value is 10 retransmissions. When used with the request keyword, the default value is 5 retransmissions. Specifying 0 selects the default value.	

appletalk arp-timeout

To specify the interval at which entries are aged out of the Address Resolution Protocol (ARP) table, use the **appletalk arp-timeout** command in interface configuration mode. To return to the default timeout, use the **no** form of this command.

appletalk arp-timeout *interval*

no appletalk arp-timeout *interval*

Syntax Description		
<i>interval</i>	Time, in minutes, after which an entry is removed from the AppleTalk ARP table. The default is 240 minutes (4 hours).	

appletalk aurp tickle-time

To set the Apple Update-Based Routing Protocol (AURP) last-heard-from timer value, use the **appletalk aurp tickle-time** command in interface configuration mode. To return to the default last-heard-from timer value, use the **no** form of this command.

appletalk aurp tickle-time *seconds*

no appletalk aurp tickle-time *seconds*

Syntax Description	<i>seconds</i>	Timeout value, in seconds. This value can be a number from 30 to infinity. The default is 90 seconds.
---------------------------	----------------	---

appletalk aurp update-interval

To set the minimum interval between Apple Update-Based Routing Protocol (AURP) routing updates, use the **appletalk aurp update-interval** command in interface configuration mode. To return to the default interval, use the **no** form of this command.

appletalk aurp update-interval *seconds*

no appletalk aurp update-interval *seconds*

Syntax Description	<i>seconds</i>	AURP routing update interval, in seconds. This interval must be a multiple of 10. The default is 30 seconds.
---------------------------	----------------	--

appletalk cable-range

To enable an extended AppleTalk network, use the **appletalk cable-range** command in interface configuration mode. To disable an extended AppleTalk network, use the **no** form of this command.

appletalk cable-range *cable-range* [*network.node*]

no appletalk cable-range *cable-range* [*network.node*]

Syntax Description	<i>cable-range</i>	Cable range value. The argument specifies the start and end of the cable range, separated by a hyphen. These values are decimal numbers from 0 to 65279. The starting network number must be less than or equal to the ending network number.
	<i>network.node</i>	(Optional) Suggested AppleTalk address for the interface. The argument <i>network</i> is the 16-bit network number, and the argument <i>node</i> is the 8-bit node number. Both numbers are decimal and separated by a period. The suggested network number must fall within the specified range of network numbers.

appletalk checksum

To enable the generation and verification of checksums for all AppleTalk packets (except routed packets), use the **appletalk checksum** command in global configuration mode. To disable checksum generation and verification, use the **no** form of this command.

appletalk checksum

no appletalk checksum

Syntax Description This command has no arguments or keywords.

appletalk client-mode

To allow users to access an AppleTalk zone when dialing into an asynchronous line (on Cisco routers, only via the auxiliary port) use the **appletalk client-mode** command in interface configuration mode. To disable this function, use the **no** form of this command.

appletalk client-mode

no appletalk client-mode

Syntax Description This command has no arguments or keywords.

appletalk discovery

To place an interface into discovery mode, use the **appletalk discovery** command in interface configuration mode. To disable discovery mode, use the **no** form of this command.

appletalk discovery

no appletalk discovery

Syntax Description This command has no arguments or keywords.

appletalk distribute-list in

To filter routing updates received from other routers over a specified interface, use the **appletalk distribute-list in** command in interface configuration mode. To remove the routing table update filter, use the **no** form of this command.

appletalk distribute-list *access-list-number* **in**

no appletalk distribute-list [*access-list-number*] **in**

Syntax Description

<i>access-list-number</i>	Number of the access list. This is a decimal number from 600 to 699.
---------------------------	--

appletalk distribute-list out

To filter routing updates transmitted to other routers, use the **appletalk distribute-list out** command in interface configuration mode. To remove the routing table update filter, use the **no** form of this command.

appletalk distribute-list *access-list-number* **out**

no appletalk distribute-list [*access-list-number*] **out**

Syntax Description

<i>access-list-number</i>	Number of the access list. This is a decimal number from 600 to 699.
---------------------------	--

appletalk domain-group

To assign a predefined domain number to an interface, use the **appletalk domain-group** command in interface configuration mode. To remove an interface from a domain, use the **no** form of this command.

appletalk domain-group *domain-number*

no appletalk domain-group [*domain-number*]

Syntax Description

<i>domain-number</i>	Number of an AppleTalk domain. It can be a decimal integer from 1 to 1,000,000.
----------------------	---

appletalk domain hop-reduction

To reduce the hop-count value in packets that are traveling between segments of a domains, use the **appletalk domain hop-reduction** command in global configuration mode. To disable the reduction of hop-count values, use the **no** form of this command.

appletalk domain *domain-number* **hop-reduction**

no appletalk domain *domain-number* **hop-reduction**

Syntax Description

<i>domain-number</i>	Number of an AppleTalk domain. It can be a decimal integer from 1 to 1,000,000.
----------------------	---

appletalk domain name

To create a domain and assign it a name and number, use the **appletalk domain name** command in global configuration mode. To remove a domain, use the **no** form of this command.

appletalk domain *domain-number* **name** *domain-name*

no appletalk domain *domain-number* **name** *domain-name*

Syntax Description

<i>domain-number</i>	Number of an AppleTalk domain. It can be a decimal integer from 1 to 1000000.
<i>domain-name</i>	Name of an AppleTalk domain. The name must be unique across the AppleTalk internetwork. It can be up to 32 characters long and can include special characters from the Apple Macintosh character set. To include a special character, type a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20.

appletalk domain remap-range

To remap ranges of AppleTalk network numbers or cable ranges between two segments of a domain, use the **appletalk domain remap-range** command in global configuration mode. To disable remapping, use the **no** form of this command.

appletalk domain *domain-number* **remap-range** {**in** | **out**} *cable-range*

no appletalk domain *domain-number* **remap-range** {**in** | **out**} [*cable-range*]

Syntax Description	<i>domain-number</i>	Number of an AppleTalk domain. It can be a decimal integer from 1 to 1,000,000.
	in	Specifies that the remapping is performed on inbound packets (that is, on packets arriving into the local interenterprise network). All network numbers or cable ranges coming from the domain are remapped into the specified range.
	out	Specifies that the remapping is performed on outbound packets (that is, on packets exiting from the local interenterprise network). All network numbers or cable ranges going to the domain are remapped into the specified range.
	<i>cable-range</i>	Specifies the start and end of the cable range, separated by a hyphen. The starting network must be the first AppleTalk network number or the beginning of the cable range to remap. The number must be immediately followed by a hyphen. The ending network must be the last AppleTalk network number or the end of the cable range to remap.

appletalk eigrp active-time

To specify the length of time for which Enhanced Interior Gateway Routing Protocol (EIGRP) routes can be active, use the **appletalk eigrp active-time** command in global configuration mode. To return to the default value of 1 minute, use the **no** form of the command.

appletalk eigrp active-time { *minutes* | **disabled** }

no appletalk eigrp active-time

Syntax Description	<i>minutes</i>	Enhanced IGRP active state time (in minutes). Valid values are from 1 to 4,294,967,295 minutes.
	disabled	Disables the Enhanced IGRP active state time limit. Routes remain active indefinitely.

appletalk eigrp-bandwidth-percentage

To configure the percentage of bandwidth that may be used by Enhanced Interior Gateway Routing Protocol (EIGRP) on an interface, use the **appletalk eigrp-bandwidth-percentage** command in interface configuration mode. To restore the default value, use the **no** form of this command.

appletalk eigrp-bandwidth-percentage *router-number percent*

no appletalk eigrp-bandwidth-percentage

Syntax Description	<i>router-number</i>	Router ID.
	<i>percent</i>	Percentage of bandwidth that Enhanced IGRP may use.

appletalk eigrp log-neighbor-changes

To enable the logging of changes in Enhanced Interior Gateway Protocol (EIGRP) neighbor adjacencies, use the **appletalk eigrp log-neighbor-changes** command in global configuration mode. To disable this function, use the **no** form of this command.

appletalk eigrp log-neighbor-changes

no appletalk eigrp log-neighbor-changes

Syntax Description This command has no arguments or keywords.

appletalk eigrp-splithorizon

To enable split horizon, use the **appletalk eigrp-splithorizon** command in interface configuration mode. To disable split horizon, use the **no** form of this command.

appletalk eigrp-splithorizon

no appletalk eigrp-splithorizon

Syntax Description This command has no arguments or keywords.

appletalk eigrp-timers

To configure the AppleTalk Enhanced Interior Gateway Protocol (EIGRP) hello packet interval and the route hold time, use the **appletalk eigrp-timers** command in interface configuration mode. To return to the default values for these timers, use the **no** form of this command.

appletalk eigrp-timers *hello-interval hold-time*

no appletalk eigrp-timers *hello-interval hold-time*

Syntax Description		
<i>hello-interval</i>		Interval between hello packets, in seconds. The default interval is 5 seconds. It can be a maximum of 30 seconds.
<i>hold-time</i>		Hold time, in seconds. The hold time is advertised in hello packets and indicates to neighbors the length of time they should consider the sender valid. The hold time can be in the range 15 to 90 seconds.

appletalk event-logging

To log significant network events, use the **appletalk event-logging** command in global configuration mode. To disable this function, use the **no** form of this command.

appletalk event-logging

no appletalk event-logging

Syntax Description This command has no arguments or keywords.

appletalk free-trade-zone

To establish a free-trade zone, use the **appletalk free-trade-zone** command in interface configuration mode. To disable a free-trade zone, use the **no** form of this command.

appletalk free-trade-zone

no appletalk free-trade-zone

Syntax Description This command has no arguments or keywords.

appletalk getzonelist-filter

To filter GetZoneList (GZL) replies, use the **appletalk getzonelist-filter** command in interface configuration mode. To remove a filter, use the **no** form of this command.

appletalk getzonelist-filter *access-list-number*

no appletalk getzonelist-filter [*access-list-number*]

Syntax Description *access-list-number* Number of the access list. This is a decimal number from 600 to 699.

appletalk glean-packets

To derive AppleTalk Address Resolution Protocol (ARP) table entries from incoming packets, use the **appletalk glean-packets** command in interface configuration mode. To disable this function, use the **no** form of this command.

appletalk glean-packets

no appletalk glean-packets

Syntax Description This command has no arguments or keywords.

appletalk ignore-verify-errors

To allow the Cisco IOS software to start functioning even if the network is misconfigured, use the **appletalk ignore-verify-errors** command in global configuration mode. To disable this function, use the **no** form of this command.

appletalk ignore-verify-errors

no appletalk ignore-verify-errors

Syntax Description This command has no arguments or keywords.

appletalk iptalk

To enable IPTalk encapsulation on a tunnel interface, use the **appletalk iptalk** command in interface configuration mode. To disable IPTalk encapsulation, use the **no** form of this command.

appletalk iptalk *network zone*

no appletalk iptalk [*network zone*]

Syntax Description	<i>network</i>	AppleTalk network address assigned to the interface. The argument <i>network</i> is the 16-bit network number in decimal.
	<i>zone</i>	Name of the zone for the connected AppleTalk network.

appletalk iptalk-baseport

To specify the User Datagram Protocol (UDP) port number when configuring IPTalk, use the **appletalk iptalk-baseport** command in global configuration mode. To return to the default UDP port number, use the **no** form of this command.

appletalk iptalk-baseport *port-number*

no appletalk iptalk-baseport [*port-number*]

Syntax Description

port-number

First UDP port number in the range of UDP ports used in mapping AppleTalk well-known Datagram Delivery Protocol (DDP) socket numbers to UDP ports.

appletalk lookup-type

To specify which Name Binding Protocol (NBP) service types are retained in the name cache, use the **appletalk lookup-type** command in global configuration mode. To disable the caching of services, use the **no** form of this command.

appletalk lookup-type *service-type*

no appletalk lookup-type *service-type*

Syntax Description

service-type

AppleTalk service types. The name of a service type can include special characters from the Apple Macintosh character set. To include a special character, type a colon followed by two hexadecimal numbers. Table 22 lists some AppleTalk service types. For zone names with a leading space character, enter the first character as the special sequence :20.

Table 22 lists some AppleTalk service types.

Table 22 *AppleTalk Service Types*

Service Type ¹	Description
Services for Cisco Routers	
ciscoRouter	Active adjacent Cisco routers. This service type is initially enabled by default.
IPADDRESS	Addresses of active MacIP server.
IPGATEWAY	Names of active MacIP server.
SNMP Agent	Active SNMP agents in Cisco routers.

Table 22 AppleTalk Service Types (continued)

Service Type ¹	Description
Services for Other Vendors' Routers	
AppleRouter	Apple internetwork router.
FastPath	Shiva LocalTalk gateway.
GatorBox	Cayman LocalTalk gateway.
systemRouter	Cisco's OEM router name.
Workstation	Macintosh running System 7. The machine type also is defined, so it is possible to easily identify all user nodes.

1. Type all service names exactly as shown. Spaces are valid. Do not use leading or trailing spaces when entering service names.

appletalk macip dynamic

To allocate IP addresses to dynamic MacIP clients, use the **appletalk macip dynamic** command in global configuration mode. To delete a MacIP dynamic address assignment, use the **no** form of this command.

appletalk macip dynamic *ip-address* [*ip-address*] **zone** *server-zone*

no appletalk macip dynamic *ip-address* [*ip-address*] **zone** *server-zone*

Syntax Description

<i>ip-address</i>	IP address, in four-part, dotted decimal notation. To specify a range, enter two IP addresses, which represent the first and last addresses in the range.
zone <i>server-zone</i>	Zone in which the MacIP server resides. The argument <i>server-zone</i> can include special characters from the Apple Macintosh character set. To include a special character, specify a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20. For a list of Macintosh characters, refer to Apple Computer's <i>Inside AppleTalk</i> publication.

appletalk macip server

To establish a MacIP server for a zone, use the **appletalk macip server** command in global configuration mode. To shut down a MacIP server, use the **no** form of this command.

appletalk macip server *ip-address* **zone** *server-zone*

no appletalk macip server *ip-address* **zone** *server-zone*

Syntax Description	<i>ip-address</i>	IP address, in four-part dotted decimal notation. It is suggested that this address match the address of an existing IP interface.
	zone <i>server-zone</i>	Zone in which the MacIP server resides. The argument <i>server-zone</i> can include special characters from the Apple Macintosh character set. To include a special character, specify a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20. For a list of Macintosh characters, refer to Apple Computer's <i>Inside AppleTalk</i> publication.

appletalk macip static

To allocate an IP address to be used by a MacIP client that has reserved a static IP address, use the **appletalk macip static** command in global configuration mode. To delete a MacIP static address assignment, use the **no** form of this command.

```
appletalk macip static ip-address [ip-address] zone server-zone
```

```
no appletalk macip static ip-address [ip-address] zone server-zone
```

Syntax Description	<i>ip-address</i>	IP address, in four-part, dotted decimal format. To specify a range, enter two IP addresses, which represent the first and last addresses in the range.
	zone <i>server-zone</i>	Zone in which the MacIP server resides. The argument <i>server-zone</i> can include special characters from the Apple Macintosh character set. To include a special character, specify a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20. For a list of Macintosh characters, refer to Apple Computer's <i>Inside AppleTalk</i> publication.

appletalk maximum-paths

To define the maximum number of equal-cost paths that the router should use when balancing the traffic load, use the **appletalk maximum-paths** command in global configuration mode. To restore the default value, use the **no** form of this command.

```
appletalk maximum-paths [paths]
```

```
no appletalk maximum-paths [paths]
```

Syntax Description	<i>paths</i>	(Optional) Maximum number of equal-cost paths to be used for balancing the traffic load. The <i>paths</i> argument is a decimal number in the range of 1 to 16.
---------------------------	--------------	---

appletalk name-lookup-interval

To set the interval between service pollings by the router on its AppleTalk interfaces, use the **appletalk name-lookup-interval** command in global configuration mode. To purge the name cache and return to the default polling interval, use the **no** form of this command.

appletalk name-lookup-interval *seconds*

no appletalk name-lookup-interval [*seconds*]

Syntax Description

seconds

Interval, in seconds, between NBP lookup pollings. This can be any positive integer; there is no upper limit. It is recommended that you use an interval between 300 seconds (5 minutes) and 1200 seconds (20 minutes). The smaller the interval, the more packets are generated to handle the names. Specifying an interval of 0 purges all entries from the name cache and disables the caching of service type information that is controlled by the **appletalk lookup-type** command, including the caching of information about our routers.

appletalk permit-partial-zones

To permit access to the other networks in a zone when access to one of those networks is denied, use the **appletalk permit-partial-zones** command in global configuration mode. To deny access to all networks in a zone if access to one of those networks is denied, use the **no** form of this command.

appletalk permit-partial-zones

no appletalk permit-partial-zones

Syntax Description

This command has no arguments or keywords.

appletalk pre-fdditalk

To enable the recognition of pre-FDDITalk packets, use the **appletalk pre-fdditalk** command in global configuration mode. To disable this function, use the **no** form of this command.

appletalk pre-fdditalk

no appletalk pre-fdditalk

Syntax Description

This command has no arguments or keywords.

appletalk protocol

To specify the routing protocol to use on an interface, use the **appletalk protocol** command in interface configuration mode. To disable a routing protocol, use the **no** form of this command.

appletalk protocol { **aurp** | **eigrp** | **rtmp** }

no appletalk protocol { **aurp** | **eigrp** | **rtmp** }

Syntax Description		
	aurp	Specifies that the routing protocol to use is AppleTalk Update-Based Routing Protocol (AURP). You can enable AURP only on tunnel interfaces.
	eigrp	Specifies that the routing protocol to use is Enhanced Interior Gateway Routing Protocol (EIGRP).
	rtmp	Specifies that the routing protocol to use is Routing Table Maintenance Protocol (RTMP), which is enabled by default.

appletalk proxy-nbp

To assign a proxy network number for each zone in which there is a router that supports only nonextended AppleTalk, use the **appletalk proxy-nbp** command in global configuration mode. To delete the proxy, use the **no** form of this command.

appletalk proxy-nbp *network-number zone-name*

no appletalk proxy-nbp [*network-number zone-name*]

Syntax Description		
	<i>network-number</i>	Network number of the proxy. It is a 16-bit decimal number and must be unique on the network. This is the network number that will be advertised by the Cisco IOS software as if it were a real network number.
	<i>zone-name</i>	Name of the zone that contains the devices that support only nonextended AppleTalk. The name can include special characters from the Apple Macintosh character set. To include a special character, type a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20.

appletalk require-route-zones

To prevent the advertisement of routes (network numbers or cable ranges) that have no assigned zone, use the **appletalk require-route-zones** command in global configuration mode. To disable this option and allow the Cisco IOS software to advertise to its neighbors routes that have no network-zone association, use the **no** form of this command.

appletalk require-route-zones

no appletalk require-route-zones

Syntax Description This command has no arguments or keywords.

appletalk route-cache

To enable fast switching on all supported interfaces, use the **appletalk route-cache** command in interface configuration mode. To disable fast switching, use the **no** form of this command.

appletalk route-cache

no appletalk route-cache

Syntax Description This command has no arguments or keywords.

appletalk route-redistribution

To redistribute Routing Table Maintenance Protocol (RTMP) routes into AppleTalk Enhanced Interior Gateway Routing Protocol (EIGRP) and vice versa, use the **appletalk route-redistribution** command in global configuration mode. To keep Enhanced IGRP and RTMP routes separate, use the **no** form of this command.

appletalk route-redistribution

no appletalk route-redistribution

Syntax Description This command has no arguments or keywords.

appletalk routing

To enable AppleTalk routing, use the **appletalk routing** command in global configuration mode. To disable AppleTalk routing, use the **no** form of this command.

appletalk routing [**eigrp** *router-number*]

no appletalk routing [**eigrp** *router-number*]

Syntax Description	eigrp <i>router-number</i>	(Optional) Specifies the Enhanced Interior Gateway Routing Protocol (EIGRP) routing protocol. The argument <i>router-number</i> is the router ID. It can be a decimal integer from 1 to 2,147,483,647. It must be unique in your AppleTalk Enhanced IGRP internetwork.
---------------------------	-----------------------------------	--

appletalk rtmp jitter

To set the interval timer on a router between subsequent AppleTalk Routing Table Maintenance Protocol (RTMP) routing updates, use the **appletalk rtmp jitter** command in global configuration mode. To disable this mode, use the **no** form of the command.

appletalk rtmp jitter *percent*

no appletalk rtmp jitter *percent*

Syntax Description	<i>percent</i>	Ranges from 0 to 100.
---------------------------	----------------	-----------------------

appletalk rtmp-stub

To enable AppleTalk Routing Table Maintenance Protocol (RTMP) stub mode, use the **appletalk rtmp-stub** command in interface configuration mode. To disable this mode, use the **no** form of the command.

appletalk rtmp-stub

no appletalk rtmp-stub

Syntax Description	This command has no arguments or keywords.
---------------------------	--

appletalk send-rtmps

To allow the Cisco IOS software to send routing updates to its neighbors, use the **appletalk send-rtmps** command in interface configuration mode. To block updates from being sent, use the **no** form of this command.

appletalk send-rtmps

no appletalk send-rtmps

Syntax Description This command has no arguments or keywords.

appletalk static cable-range

To define a static route or a floating static route on an extended network, use the **appletalk static cable-range** command in global configuration mode. To remove a static route, use the **no** form of this command.

appletalk static cable-range *cable-range* **to** *network.node* [**floating**] **zone** *zone-name*

no appletalk static cable-range *cable-range* **to** *network.node* [**floating**] [**zone** *zone-name*]

Syntax Description	<i>cable-range</i>	Cable range value. The argument specifies the start and end of the cable range, separated by a hyphen. These values are decimal number from 0 to 65,279. The starting network number must be less than or equal to the ending network number.
	to <i>network.node</i>	AppleTalk network address of the remote router. The argument <i>network</i> is the 16-bit network number in the range 0 to 65,279. The argument <i>node</i> is the 8-bit node number in the range 0 to 254. Both numbers are decimal.
	floating	(Optional) Specifies that this route is a floating static route, which is a static route that can be overridden by a dynamically learned route.
	zone <i>zone-name</i>	Name of the zone on the remote network. The name can include special characters from the Apple Macintosh character set. To include a special character, type a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20.

appletalk static network

To define a static route or a floating static route on a nonextended network, use the **appletalk static network** command in global configuration mode. To remove a static route, use the **no** form of this command.

appletalk static network *network-number* **to** *network.node* [**floating**] **zone** *zone-name*

no appletalk static network *network-number* **to** *network.node* [**floating**] [**zone** *zone-name*]

Syntax Description	<i>network-number</i>	AppleTalk network number assigned to the interface. It is a 16-bit decimal number and must be unique on the network. This is the network number that will be advertised by the Cisco IOS software as if it were a real network number.
	to <i>network.node</i>	AppleTalk network address of the remote router. The argument <i>network</i> is the 16-bit network number in the range 0 to 65279. The argument <i>node</i> is the 8-bit node number in the range 0 to 254. Both numbers are decimal.
	floating	(Optional) Specifies that this route is a floating static route, which is a static route that can be overridden by a dynamically learned route.
	zone <i>zone-name</i>	Name of the zone on the remote network. The name can include special characters from the Apple Macintosh character set. To include a special character, type a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20.

appletalk strict-rtmp-checking

To perform maximum checking of routing updates to ensure their validity, use the **appletalk strict-rtmp-checking** command in global configuration mode. To disable the maximum checking, use the **no** form of this command.

appletalk strict-rtmp-checking

no appletalk strict-rtmp-checking

Syntax Description This command has no arguments or keywords.

appletalk timers

To change the routing update timers, use the **appletalk timers** command in global configuration mode. To return to the default routing update timers, use the **no** form of this command.

appletalk timers *update-interval valid-interval invalid-interval*

no appletalk timers [*update-interval valid-interval invalid-interval*]

Syntax Description	<i>update-interval</i>	Time, in seconds, between routing updates sent to other routers on the network. The default is 10 seconds.
	<i>valid-interval</i>	Time, in seconds, that the Cisco IOS software will consider a route valid without having heard a routing update for that route. The default is 20 seconds (two times the update interval).
	<i>invalid-interval</i>	Time, in seconds, that the route is retained after the last update. The default is 60 seconds (three times the valid interval).

appletalk virtual-net

To add AppleTalk users who are logging in on an asynchronous line and using PPP encapsulation to an internal network, use the **appletalk virtual-net** command in global configuration mode. To remove an internal network, use the **no** form of this command.

appletalk virtual-net *network-number zone-name*

no appletalk virtual-net *network-number zone-name*

Syntax Description		
	<i>network-number</i>	AppleTalk network address assigned to the interface. This is a 16-bit decimal network number in the range 0 to 65279. The network address must be unique across your AppleTalk internetwork.
	<i>zone-name</i>	Name of a new or existing zone to which the AppleTalk user will belong.

appletalk zip-query-interval

To specify the interval at which the Cisco IOS software sends ZIP queries, use the **appletalk zip-query-interval** command in global configuration mode. To return to the default interval, use the **no** form of this command.

appletalk zip-query-interval *interval*

no zip-query-interval

Syntax Description		
	<i>interval</i>	Interval, in seconds, at which the software sends ZIP queries. It can be any positive integer. The default is 10 seconds.

appletalk zip-reply-filter

To configure a ZIP reply filter, use the **appletalk zip-reply-filter** command in interface configuration mode. To remove a filter, use the **no** form of this command.

appletalk zip-reply-filter *access-list-number*

no appletalk zip-reply-filter [*access-list-number*]

Syntax Description		
	<i>access-list-number</i>	Number of the access list. This is a decimal number from 600 to 699.

appletalk zone

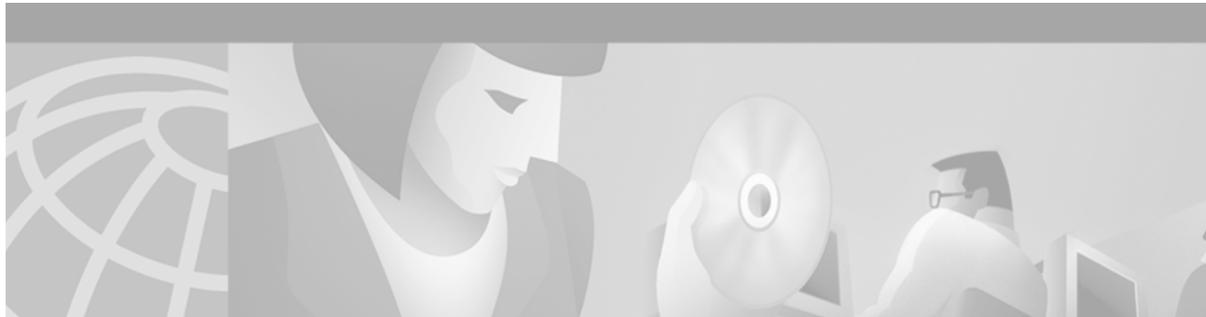
To set the zone name for the connected AppleTalk network, use the **appletalk zone** command in interface configuration mode. To delete a zone, use the **no** form of this command.

appletalk zone *zone-name*

no appletalk zone [*zone-name*]

Syntax Description

<i>zone-name</i>	Name of the zone. The name can include special characters from the Apple Macintosh character set. To include a special character, type a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20.
------------------	--



AppleTalk Commands: clear appletalk arp Through test appletalk

This chapter describes the function and syntax of the AppleTalk commands: **clear appletalk arp** through **test appletalk**. For more information about these commands, refer to the corresponding chapter in the *Cisco IOS AppleTalk and Novell IPX Command Reference*.

clear appletalk arp

To delete all entries or a specified entry from the AppleTalk Address Resolution Protocol (AARP) table, use the **clear appletalk arp** command in EXEC mode.

```
clear appletalk arp [network.node]
```

Syntax Description

network.node

(Optional) AppleTalk network address to be deleted from the AARP table. The argument *network* is the 16-bit network number in the range 0 to 65,279. The argument *node* is the 8-bit node number in the range 0 to 254. Both numbers are decimal.

clear appletalk neighbor

To delete all entries or a specified entry from the neighbor table, use the **clear appletalk neighbor** command in EXEC mode.

```
clear appletalk neighbor [neighbor-address]
```

Syntax Description

neighbor-address

(Optional) Network address of the neighboring router to be deleted from the neighbor table. The address is in the format *network.node*. The argument *network* is the 16-bit network number in the range 1 to 65,279. The argument *node* is the 8-bit node number in the range 0 to 254. Both numbers are decimal.

clear appletalk route

To delete entries from the routing table, use the **clear appletalk route** command in EXEC mode.

```
clear appletalk route [network]
```

Syntax Description	<i>network</i>	(Optional) Number of the network to which the route provides access.
---------------------------	----------------	--

clear appletalk traffic

To reset AppleTalk traffic counters, use the **clear appletalk traffic** command in EXEC mode.

```
clear appletalk traffic
```

Syntax Description	This command has no arguments or keywords.	
---------------------------	--	--

clear smrp mcache

To remove all fast-switching entries in the Sample Multicast Routing Protocol (SMRP) fast-switching cache table, use the **clear smrp mcache** command in EXEC mode.

```
clear smrp mcache
```

Syntax Description	This command has no arguments or keywords.	
---------------------------	--	--

show appletalk access-lists

To display the AppleTalk access lists currently defined, use the **show appletalk access-lists** command in EXEC mode.

```
show appletalk access-lists
```

Syntax Description	This command has no arguments or keywords.	
---------------------------	--	--

show appletalk adjacent-routes

To display routes to networks that are directly connected or that are one hop away, use the **show appletalk adjacent-routes** command in privileged EXEC mode.

```
show appletalk adjacent-routes
```

Syntax Description This command has no arguments or keywords.

show appletalk arp

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

```
show appletalk arp
```

Syntax Description This command has no arguments or keywords.

show appletalk aurp events

To display the pending events in the AppleTalk Update-Based Routing Protocol (AURP) update-events queue, use the **show appletalk aurp events** command in privileged EXEC mode.

```
show appletalk aurp events
```

Syntax Description This command has no arguments or keywords.

show appletalk aurp topology

To display entries in the AppleTalk Update-Based Routing Protocol (AURP) private path database, which consists of all paths learned from exterior routers, use the **show appletalk aurp topology** command in privileged EXEC mode.

```
show appletalk aurp topology
```

Syntax Description This command has no arguments or keywords.

show appletalk cache

To display the routes in the AppleTalk fast-switching table on an extended AppleTalk network, use the **show appletalk cache** command in EXEC mode.

show appletalk cache

Syntax Description This command has no arguments or keywords.

show appletalk domain

To display all domain-related information, use the **show appletalk domain** command in EXEC mode.

show appletalk domain [*domain-number*]

Syntax Description *domain-number* (Optional) Number of an AppleTalk domain about which to display information. It can be a decimal integer from 1 to 1,000,000.

show appletalk eigrp interfaces

To display information about interfaces configured for Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show appletalk eigrp interfaces** command in EXEC mode.

show appletalk eigrp interfaces [*type number*]

Syntax Description *type* (Optional) Interface type.
number (Optional) Interface number.

show appletalk eigrp neighbors

To display the neighbors discovered by Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show appletalk eigrp neighbors** command in EXEC mode.

show appletalk eigrp neighbors [*interface*]

Syntax Description *interface* (Optional) Displays information about the specified neighbor router.

show appletalk eigrp topology

To display the AppleTalk Enhanced Interior Gateway Routing Protocol (EIGRP) topology table, use the **show appletalk eigrp topology** command in EXEC mode.

show appletalk eigrp topology [*network-number* | **active** | **zero-successors**]

Syntax Description		
	<i>network-number</i>	(Optional) Number of the AppleTalk network whose topology table entry you want to display.
	active	(Optional) Displays the entries for all active routes.
	zero-successors	(Optional) Displays the entries for destinations for which no successors exist. These entries are destinations that the Cisco IOS software currently does not know how to reach via Enhanced IGRP. This option is useful for debugging network problems.

show appletalk globals

To display information and settings about the AppleTalk internetwork and other parameters, use the **show appletalk globals** command in EXEC mode.

show appletalk globals

Syntax Description This command has no arguments or keywords.

show appletalk interface

To display the status of the AppleTalk interfaces configured in the Cisco IOS software and the parameters configured on each interface, use the **show appletalk interface** command in privileged EXEC mode.

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

Syntax Description		
	brief	(Optional) Displays a brief summary of the status of the AppleTalk interfaces.
	<i>type</i>	(Optional) Interface type. It can be one of the following types: asynchronous, dialer, Ethernet (IEEE 802.3), Token Ring (IEEE 802.5), FDDI, High-Speed Serial Interface (HSSI), Virtual Interface, ISDN Basic Rate Interface (BRI), ATM interface, loopback, null, or serial.
	<i>number</i>	(Optional) Interface number.

show appletalk macip-clients

To display status information about all known MacIP clients, use the **show appletalk macip-clients** command in EXEC mode.

```
show appletalk macip-clients
```

Syntax Description This command has no arguments or keywords.

show appletalk macip-servers

To display status information about related servers, use the **show appletalk macip-servers** command in EXEC mode.

```
show appletalk macip-servers
```

Syntax Description This command has no arguments or keywords.

show appletalk macip-traffic

To display statistics about MacIP traffic through the router, use the **show appletalk macip-traffic** command in privileged EXEC mode.

```
show appletalk macip-traffic
```

Syntax Description This command has no arguments or keywords.

show appletalk name-cache

To display a list of Name Binding Protocol (NBP) services offered by nearby routers and other devices that support NBP, use the **show appletalk name-cache** command in privileged EXEC mode.

```
show appletalk name-cache
```

Syntax Description This command has no arguments or keywords.

show appletalk nbp

To display the contents of the Name Binding Protocol (NBP) name registration table, use the **show appletalk nbp** command in EXEC mode.

```
show appletalk nbp
```

Syntax Description This command has no arguments or keywords.

show appletalk neighbors

To display information about the AppleTalk routers that are directly connected to any of the networks to which this router is directly connected, use the **show appletalk neighbors** command in EXEC mode.

```
show appletalk neighbors [neighbor-address]
```

Syntax Description *neighbor-address* (Optional) Displays information about the specified neighbor router.

show appletalk remap

To display domain remapping information, use the **show appletalk remap** EXEC command.

```
show appletalk remap [domain domain-number [{in | out} [{to | from} domain-network]]]
```

Syntax Description	domain <i>domain-number</i>	(Optional) Number of an AppleTalk domain about which to display remapping information. It can be a decimal integer from 1 through 1,000,000.
	in	(Optional) Displays remapping information about inbound packets, that is, on packets entering the local segment of the domain.
	out	(Optional) Displays remapping information about outbound packets, that is on packets exiting from the local segment of the domain.
	to	(Optional) Displays information about the network number or cable range to which an address has been remapped.
	from	(Optional) Displays information about the original network number or cable range.
	<i>domain-network</i>	(Optional) Number of an AppleTalk network.

show appletalk route

To display all entries or specified entries in the AppleTalk routing table, use the **show appletalk route** EXEC command.

```
show appletalk route [network | type number]
```

Syntax Description	network	(Optional) Displays the routing table entry for the specified network.
	type number	(Optional) Displays the routing table entries for networks that can be reached via the specified interface type and number.

show appletalk sockets

To display all information or specified information about process-level operation in the sockets of an AppleTalk interface, use the **show appletalk sockets** privileged EXEC command.

```
show appletalk sockets [socket-number]
```

Syntax Description	socket-number	(Optional) Displays information about the specified socket number.
--------------------	---------------	--

show appletalk static

To display information about the statically defined routes, including floating static routes, use the **show appletalk static** EXEC command.

```
show appletalk static
```

Syntax Description	This command has no arguments or keywords.
--------------------	--

show appletalk traffic

To display statistics about AppleTalk traffic, including MacIP traffic, use the **show appletalk traffic** EXEC command.

```
show appletalk traffic
```

Syntax Description	This command has no arguments or keywords.
--------------------	--

show appletalk zone

To display all entries or specified entries in the zone information table, use the **show appletalk zone** EXEC command.

```
show appletalk zone [zone-name]
```

Syntax Description	<i>zone-name</i>	(Optional) Displays the entry for the specified zone.
---------------------------	------------------	---

show smrp forward

To display all entries or specific entries in the Simple Multicast Routing Protocol (SMRP) forwarding table, use the **show smrp forward** EXEC command.

```
show smrp forward [appletalk [group-address]]
```

Syntax Description	appletalk	(Optional) Displays SMRP forwarding table entries for all AppleTalk networks. Currently SMRP services are supported over AppleTalk only.
	<i>group-address</i>	(Optional) SMRP group address. All members of a group listen for multicast packets on this address.

show smrp globals

To display global information about Simple Multicast Routing Protocol (SMRP)—such as whether SMRP is enabled and running and settings for timers, most of which are used internally—use the **show smrp globals** EXEC command.

```
show smrp globals
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--

show smrp group

To display all entries or specific entries in the SMRP group table, use the **show smrp group** EXEC command.

```
show smrp group [appletalk [group-address]]
```

Syntax Description	appletalk	(Optional) Displays SMRP group table entries for all AppleTalk networks. Currently SMRP services are supported over AppleTalk networks only.
	<i>group-address</i>	(Optional) SMRP group address.

show smrp mcache

To display the SMRP fast-switching cache table, use the **show smrp mcache** EXEC command.

```
show smrp mcache [appletalk [group-address]]
```

Syntax Description	appletalk	(Optional) Displays the SMRP fast-switching cache table entries for all AppleTalk network groups. Currently, SMRP services are supported over AppleTalk only.
	<i>group-address</i>	(Optional) SMRP group address. Use this argument to display only this group's fast-switching cache table entry.

show smrp neighbor

To display all entries or specific entries in the SMRP neighbor table, use the **show smrp neighbor** EXEC command.

```
show smrp neighbor [appletalk [network-address]]
```

Syntax Description	appletalk	(Optional) Displays SMRP neighbor table entries for all AppleTalk networks. Currently SMRP services are supported over AppleTalk networks only.
	<i>network-address</i>	(Optional) Network address of the neighbor router.

show smrp port

To display all entries or specific entries in the SMRP port table, use the **show smrp port** EXEC command.

```
show smrp port [appletalk [type number]]
```

Syntax Description	appletalk	(Optional) Displays SMRP port table entries for all AppleTalk networks. Currently SMRP services are supported over AppleTalk networks only.
	<i>type</i>	(Optional) Interface type.
	<i>number</i>	(Optional) Interface number.

show smrp route

To display all entries or specific entries in the Simple Multicast Routing Protocol (SMRP) routing table, use the **show smrp route** EXEC command.

```
show smrp route [appletalk [network] | type number]
```

Syntax Description		
appletalk	(Optional)	Displays SMRP route table entries for all AppleTalk networks. Currently SMRP services are supported over AppleTalk networks only.
<i>network</i>	(Optional)	SMRP network range.
<i>type</i>	(Optional)	Interface type.
<i>number</i>	(Optional)	Interface number.

show smrp traffic

To display all entries or specific entries in the Simple Multicast Routing Protocol (SMRP) traffic table, use the **show smrp traffic EXEC** command.

```
show smrp traffic [all | group | neighbor | port | route | transaction]
```

Syntax Description		
all	(Optional)	Displays SMRP traffic for SMRP groups, neighbors, ports, routes, and transactions.
group	(Optional)	Displays SMRP traffic for SMRP groups.
neighbor	(Optional)	Displays SMRP traffic for neighbors.
port	(Optional)	Displays SMRP traffic for ports.
route	(Optional)	Displays SMRP traffic for routes.
transaction	(Optional)	Displays SMRP traffic for transactions.

smrp mroute-cache protocol appletalk

To enable Simple Multicast Routing Protocol (SMRP) fast-switching on a port, use the **smrp mroute-cache protocol appletalk** interface configuration command. To disable SMRP fast-switching, use the **no** form of this command.

```
smrp mroute-cache protocol appletalk
```

```
no smrp mroute-cache protocol appletalk
```

Syntax Description This command has no arguments or keywords.

smrp protocol appletalk

To make Simple Multicast Routing Protocol (SMRP) multicast services available over AppleTalk for a specific interface, use the **smrp protocol appletalk** interface configuration command. To disable SMRP over AppleTalk for a specific interface, use the **no** form of this command.

```
smrp protocol appletalk [network-range beginning-end]
```

```
no smrp protocol appletalk [network-range beginning-end]
```

Syntax Description	network-range	(Optional) SMRP network range for the interface. We recommend that you do not specify an SMRP network range. When you omit the range, the Cisco IOS software uses the AppleTalk cable range configured for the interface as the SMRP network range. If you specify a range, it must fall within the SMRP network range 1 to 65,535.
	<i>beginning-end</i>	(Optional) The beginning and end of the SMRP network range for this AppleTalk network. If you specify a range, it must fall within the SMRP network range 1 to 65,535.

smrp routing

To enable the use of the multicast transport services provided by the Simple Multicast Routing Protocol (SMRP), use the **smrp routing** global configuration command. To disable SMRP services for all interfaces, use the **no** form of this command.

smrp routing

no smrp routing

Syntax Description This command has no arguments or keywords.

test appletalk

To enter the test mode, use the **test appletalk** command in privileged EXEC mode.

test appletalk

Syntax Description This command has no arguments or keywords.



Novell IPX Commands: access-list (IPX extended) Through ipx nlsnp csnp-interval

This chapter describes the function and syntax of the Novell IPX commands: **access-list** (IPX extended) through **ipx nlsnp csnp-interval**. For more information about these commands, refer to the corresponding chapter in the *Cisco IOS AppleTalk and Novell IPX Command Reference*.



Note

For all commands that previously used the keyword **novell**, this keyword has been changed to **ipx**. You can still use the keyword **novell** in all commands.

access-list (IPX extended)

To define an extended Novell IPX access list, use the extended version of the **access-list** command in global configuration mode. To remove an extended access list, use the **no** form of this command.

```
access-list access-list-number { deny | permit } protocol [source-network][[.source-node]  
source-node-mask] | [.source-node source-network-mask.source-node-mask] [source-socket]  
[destination.network][[.destination-node] destination-node-mask] | [.destination-node  
destination-network-mask.destination-node-mask] [destination-socket] [log] [time-range  
time-range-name]
```

```
no access-list access-list-number { deny | permit } protocol [source-network][[.source-node]  
source-node-mask] | [.source-node source-network-mask.source-node-mask] [source-socket]  
[destination.network][[.destination-node] destination-node-mask] | [.destination-node  
destination-network-mask.destination-node-mask] [destination-socket] [log] [time-range  
time-range-name]
```

Syntax Description

<i>access-list-number</i>	Number of the access list. This is a number from 900 to 999.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
<i>protocol</i>	Name or number of an IPX protocol type. This is sometimes referred to as the packet type.

<i>source-network</i>	<p>(Optional) Number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of -1 matches all networks.</p> <p>You do not need to specify leading zeros in the network number; for example, for the network number 000000AA, you can enter AA.</p>
<i>.source-node</i>	<p>(Optional) Node on the source-network from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>).</p>
<i>source-node-mask</i>	<p>(Optional) Mask to be applied to the <i>source-node</i> argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>). Place ones in the bit positions you want to mask.</p>
<i>source-network-mask.</i>	<p>(Optional) Mask to be applied to the <i>source-network</i> argument. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask.</p> <p>The mask must immediately be followed by a period, which must in turn immediately be followed by the <i>source-node-mask</i> argument.</p>
<i>source-socket</i>	<p>(Optional) Socket name or number (hexadecimal) from which the packet is being sent.</p>
<i>destination.network</i>	<p>(Optional) Number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of -1 matches all networks.</p> <p>You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.</p>
<i>.destination-node</i>	<p>(Optional) Node on destination-network to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>).</p>
<i>destination-node-mask</i>	<p>(Optional) Mask to be applied to the <i>destination-node</i> argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>). Place ones in the bit positions you want to mask.</p>
<i>destination-network-mask.</i>	<p>(Optional) Mask to be applied to the <i>destination-network</i> argument. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask.</p> <p>The mask must immediately be followed by a period, which must in turn immediately be followed by the <i>destination-node-mask</i> argument.</p>
<i>destination-socket</i>	<p>(Optional) Socket name or number (hexadecimal) to which the packet is being sent.</p>
log	<p>(Optional) Logs IPX access control list violations whenever a packet matches a particular access list entry. The information logged includes source address, destination address, source socket, destination socket, protocol type, and action taken (permit/deny).</p>
time-range <i>time-range-name</i>	<p>(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.</p>

access-list (IPX standard)

To define a standard IPX 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-network [.source-node [source-node-mask]]
[destination-network [destination-node [destination-node-mask]]]
```

```
no access-list access-list-number { deny | permit }
source-network [.source-node [source-node-mask]] [destination-network [destination-node
[destination-node-mask]]]
```

Syntax Description

<i>access-list-number</i>	Number of the access list. This is a number from 800 to 899.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
<i>source-network</i>	Number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
<i>.source-node</i>	(Optional) Node on <i>source-network</i> from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxx.xxx.xxx</i>).
<i>source-node-mask</i>	(Optional) Mask to be applied to <i>source-node</i> . This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxx.xxx.xxx</i>). Place ones in the bit positions you want to mask.
<i>destination-network</i>	(Optional) Number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
<i>.destination-node</i>	(Optional) Node on <i>destination-network</i> to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxx.xxx.xxx</i>).
<i>destination-node-mask</i>	(Optional) Mask to be applied to <i>destination-node</i> . This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxx.xxx.xxx</i>). Place ones in the bit positions you want to mask.

access-list (NLSP)

To define an access list that denies or permits area addresses that summarize routes, use the NetWare Link-Services Protocol (NLSP) route aggregation version of the **access-list** command in global configuration mode. To remove an NLSP route aggregation access list, use the **no** form of this command.

```
access-list access-list-number {deny | permit} network network-mask [ticks ticks]
[area-count area-count]
```

```
no access-list access-list-number {deny | permit} network network-mask [ticks ticks]
[area-count area-count]
```

Syntax Description		
<i>access-list-number</i>		Number of the access list. This is a number from 1200 to 1299.
deny		Denies redistribution of explicit routes if the conditions are matched. If you have enabled route summarization with route-aggregation command, the router redistributes an aggregated route instead.
permit		Permits redistribution of explicit routes if the conditions are matched.
<i>network</i>		Network number to summarize. An IPX network number is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
<i>network-mask</i>		Specifies the portion of the network address that is common to all addresses in the route summary. The high-order bits of <i>network-mask</i> must be contiguous Fs, while the low-order bits must be contiguous zeros (0). An arbitrary mix of Fs and 0s is not permitted.
ticks ticks		(Optional) Metric assigned to the route summary. The default is 1 tick.
area-count area-count		(Optional) Maximum number of NLSP areas to which the route summary can be redistributed. The default is 6 areas.

access-list (SAP filtering)

To define an access list for filtering Service Advertising Protocol (SAP) requests, use the SAP filtering form 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 {deny | permit} network[.node] [network-mask.node-mask]
[service-type [server-name]]
```

```
no access-list access-list-number {deny | permit} network[.node] [network-mask.node-mask]
[service-type [server-name]]
```

Syntax Description		
<i>access-list-number</i>		Number of the SAP access list. This is a number from 1000 to 1099.
deny		Denies access if the conditions are matched.
permit		Permits access if the conditions are matched.
<i>network</i>		Network number. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
<i>.node</i>		(Optional) Node specified on the network. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxx.xxxx.xxx</i>).
<i>network-mask.node-mask</i>		(Optional) Mask to be applied to <i>network</i> and <i>node</i> . Place ones in the bit positions to be masked.
<i>service-type</i>		(Optional) Service type on which to filter. This is a hexadecimal number. A value of 0 means all services.
<i>server-name</i>		(Optional) Name of the server providing the specified service type. This can be any contiguous string of printable ASCII characters. Use double quotation marks (“ ”) to enclose strings containing embedded spaces. You can use an asterisk (*) at the end of the name as a wildcard to match one or more trailing characters.

area-address

To define a set of network numbers to be part of the current NetWare Link-Services Protocol (NLSP) area, use the **area-address** command in router configuration mode. To remove a set of network numbers from the current NLSP area, use the **no** form of this command.

```
area-address address mask
```

```
no area-address address mask
```

Syntax Description		
<i>address</i>		Network number prefix. This is a 32-bit hexadecimal number.
<i>mask</i>		Mask that defines the length of the network number prefix. This is a 32-bit hexadecimal number.

clear ipx accounting

To delete all entries in the accounting database when IPX accounting is enabled, use the **clear ipx accounting** command in EXEC mode.

```
clear ipx accounting [checkpoint]
```

Syntax Description		
checkpoint		(Optional) Clears the checkpoint database.

clear ipx cache

To delete entries from the IPX fast-switching cache, use the **clear ipx cache** command in EXEC mode.

```
clear ipx cache
```

Syntax Description This command has no arguments or keywords.

clear ipx nhrp

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

```
clear ipx nhrp
```

Syntax Description This command has no arguments or keywords.

clear ipx nlsnp neighbors

To delete all NetWare Link Services Protocol (NLSP) adjacencies from the adjacency database of Cisco IOS software, use the **clear ipx nlsnp neighbors** command in EXEC mode.

```
clear ipx nlsnp [tag] neighbors
```

Syntax Description	<i>tag</i>	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
---------------------------	------------	--

clear ipx route

To delete routes from the IPX routing table, use the **clear ipx route** command in EXEC mode.

```
clear ipx route {network [network-mask] | default | *}
```

Syntax Description		
	<i>network</i>	Number of the network whose routing table entry you want to delete. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
	<i>network-mask</i>	(Optional) Specifies the portion of the network address that is common to all addresses in an NLSP route summary. When used with the <i>network</i> argument, it specifies the an NLSP route summary to clear. The high-order bits specified for the <i>network-mask</i> argument must be contiguous Fs, while the low-order bits must be contiguous zeros (0). An arbitrary mix of Fs and 0s is not permitted.
	default	Deletes the default route from the routing table.
	*	Deletes all routes in the routing table.

clear ipx sap

To clear IPX SAP entries from the IPX routing table, use the **clear ipx sap** command in EXEC mode.

```
clear ipx sap { * | sap-type | sap-name }
```

Syntax Description		
	*	Clears all IPX SAP service entries by marking them invalid.
	<i>sap-type</i>	Specifies the type of services that you want to clear by marking as invalid. This is an four-digit hexadecimal number that uniquely identifies a service type. It can be a number in the range 1 to FFFF. You do not need to specify leading zeros in the service number. For example, for the service number 00AA, you can enter AA.
	<i>sap-name</i>	Specifies a certain name of service so that you can clear IPX SAP service entries that begin with the specified name. The name can be any contiguous string of printable ASCII characters. You can use an asterisk (*) at the end of the name as a wildcard to match one or more trailing characters. For example, to clear all services that begin with the name "accounting," enter the command clear ipx sap accounting* to clear all services that begin with the name "accounting". Use double quotation marks (“ ”) to enclose strings containing embedded spaces.

clear ipx traffic

To clear IPX protocol and NetWare Link Services Protocol (NLSP) traffic counters, use the **clear ipx traffic** command in privileged EXEC mode.

clear ipx [nlsnp] traffic

Syntax Description	nlsp	(Optional) Clears only the NLSP traffic counters and leaves other IPX traffic counters intact.
--------------------	------	--

deny (extended)

To set conditions for a named IPX extended 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 protocol [*source-network*][[*.source-node* *source-node-mask*] | [*.source-node source-network-mask.source-node-mask*]] [*source-socket*]
 [*destination-network*][[*.destination-node* *destination-node-mask*] | [*.destination-node destination-network-mask.destination-node-mask*]] [*destination-socket*] [**log**] [**time-range** *time-range-name*]

no deny protocol [*source-network*][[*.source-node* *source-node-mask*] | [*.source-node source-network-mask.source-node-mask*]] [*source-socket*]
 [*destination-network*][[*.destination-node* *destination-node-mask*] | [*.destination-node destination-network-mask.destination-node-mask*]] [*destination-socket*] [**log**] [**time-range** *time-range-name*]

Syntax Description	<i>protocol</i>	Name or number of an IPX protocol type. This is sometimes referred to as the packet type. You can also use the word any to match all protocol types.
	<i>source-network</i>	(Optional) Number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You can also use the keyword any to match all networks. You do not need to specify leading zeros in the network number; for example, for the network number 000000AA, you can enter AA.
	<i>.source-node</i>	(Optional) Node on the source-network from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>).
	<i>source-node-mask</i>	(Optional) Mask to be applied to the <i>source-node</i> argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>). Place ones in the bit positions you want to mask.

<i>destination-network</i>	(Optional) Number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You can also use the keyword any to match all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
<i>.destination-node</i>	(Optional) Node on the destination-network to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>).
<i>destination-node-mask</i>	(Optional) Mask to be applied to the <i>destination-node</i> argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>). Place ones in the bit positions you want to mask.
<i>destination-network-mask.</i>	(Optional) Mask to be applied to the <i>destination-network</i> argument. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask. The mask must immediately be followed by a period, which must in turn immediately be followed by the <i>destination-node-mask</i> argument.
<i>destination-socket</i>	(Optional) Socket name or number (hexadecimal) to which the packet is being sent.
log	(Optional) Logs IPX access control list violations whenever a packet matches a particular access list entry. The information logged includes source address, destination address, source socket, destination socket, protocol type, and action taken (permit/deny).
time-range <i>time-range-name</i>	(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.

deny (NLSP)

To filter explicit routes and generate an aggregated route for a named NetWare Link Services Protocol (NLSP) route aggregation 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 *network network-mask* [**ticks ticks**] [**area-count area-count**]

no deny *network network-mask* [**ticks ticks**] [**area-count area-count**]

Syntax Description	<i>network</i>	Network number to summarize. An IPX network number is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
	<i>network-mask</i>	Specifies the portion of the network address that is common to all addresses in the route summary, expressed as an 8-digit hexadecimal number. The high-order bits of <i>network-mask</i> must be contiguous 1s, while the low-order bits must be contiguous zeros (0). An arbitrary mix of 1s and 0s is not permitted.
	ticks <i>ticks</i>	(Optional) Metric assigned to the route summary. The default is 1 tick.
	area-count <i>area-count</i>	(Optional) Maximum number of NLSP areas to which the route summary can be redistributed. The default is 6 areas.

deny (SAP filtering)

To set conditions for a named IPX SAP filtering 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 network[.node] [network-mask.node-mask] [service-type [server-name]]
```

```
no deny network[.node] [network-mask.node-mask] [service-type [server-name]]
```

Syntax Description	<i>network</i>	Network number. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
	<i>.node</i>	(Optional) Node on <i>network</i> . This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>).
	<i>network-mask</i> . <i>node-mask</i>	(Optional) Mask to be applied to <i>network</i> and <i>node</i> . Place ones in the bit positions to be masked.
	<i>service-type</i>	(Optional) Service type on which to filter. This is a hexadecimal number. A value of 0 means all services.
	<i>server-name</i>	(Optional) Name of the server providing the specified service type. This can be any contiguous string of printable ASCII characters. Use double quotation marks (“ ”) to enclose strings containing embedded spaces. You can use an asterisk (*) at the end of the name as a wildcard to match one or more trailing characters.

deny (standard)

To set conditions for a named IPX 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-network[.source-node [source-node-mask]] [destination-network[.destination-node
[destination-node-mask]]]
```

```
no deny source-network[.source-node [source-node-mask]]
[destination-network[.destination-node [destination-node-mask]]]
```

Syntax Description	
<i>source-network</i>	Number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 00000AA, you can enter AA.
<i>.source-node</i>	(Optional) Node on the source-network from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (xxx.xxx.xxx).
<i>source-node-mask</i>	(Optional) Mask to be applied to the <i>source-node</i> argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (xxx.xxx.xxx). Place ones in the bit positions you want to mask.
<i>destination-network</i>	(Optional) Number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 00000AA, you can enter AA.
<i>.destination-node</i>	(Optional) Node on the destination-network to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (xxx.xxx.xxx).
<i>destination-node-mask</i>	(Optional) Mask to be applied to <i>destination-node</i> argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (xxx.xxx.xxx). Place ones in the bit positions you want to mask.

distribute-list in (IPX)

To filter networks received in updates, use the **distribute-list in** command in router configuration mode. To change or cancel the filter, use the **no** form of this command.

```
distribute-list {access-list-number | name} in [interface-name]
```

```
no distribute-list {access-list-number | name} in [interface-name]
```

Syntax Description		
	<i>access-list-number</i>	Standard IPX access list number in the range 800 to 899 or NLSP access list number in the range 1200 to 1299. The list explicitly specifies which networks are to be received and which are to be suppressed.
	<i>name</i>	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.
	in	Applies the access list to incoming routing updates.
	<i>interface-name</i>	(Optional) Interface on which the access list should be applied to incoming updates. If no interface is specified, the access list is applied to all incoming updates.

distribute-list out (IPX)

To suppress networks from being advertised in updates, use the **distribute-list out** command in router configuration mode. To cancel this function, use the **no** form of this command.

distribute-list { *access-list-number* | *name* } **out** [*interface-name* | *routing-process*]

no distribute-list { *access-list-number* | *name* } **out** [*interface-name* | *routing-process*]

Syntax Description		
	<i>access-list-number</i>	Standard IPX access list number in the range 800 to 899 or NLSP access list number in the range 1200 to 1299. The list explicitly specifies which networks are to be sent and which are to be suppressed in routing updates.
	<i>name</i>	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.
	out	Applies the access list to outgoing routing updates.
	<i>interface-name</i>	(Optional) Interface on which the access list should be applied to outgoing updates. If no interface is specified, the access list is applied to all outgoing updates.
		
	Note	When you use the distribute-list out command after entering the ipx router eigrp command to enable the Enhanced Interior Gateway Routing Protocol (EIGRP), you must use the <i>interface-name</i> argument. If you do not specify an interface, the routers will not exchange any routes or SAPs with their neighbors.
	<i>routing-process</i>	(Optional) Name of a particular routing process as follows: <ul style="list-style-type: none"> • eigrp <i>autonomous-system-number</i> • rip • nlsnp [<i>tag</i>]

distribute-sap-list in

To filter services received in updates, use the **distribute-sap-list in** command in router configuration mode. To change or cancel the filter, use the **no** form of this command.

distribute-sap-list {*access-list-number* | *name*} **in** [*interface-name*]

no distribute-sap-list {*access-list-number* | *name*} **in** [*interface-name*]

Syntax Description		
	<i>access-list-number</i>	SAP access list number in the range 1000 to 1099. The list explicitly specifies which services are to be received and which are to be suppressed.
	<i>name</i>	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.
	<i>interface-name</i>	(Optional) Interface on which the access list should be applied to incoming updates. If no interface is specified, the access list is applied to all incoming updates.

distribute-sap-list out

To suppress services from being advertised in SAP updates, use the **distribute-sap-list out** command in router configuration mode. To cancel this function, use the **no** form of this command.

distribute-sap-list {*access-list-number* | *name*} **out** [*interface-name* | *routing-process*]

no distribute-sap-list {*access-list-number* | *name*} **out** [*interface-name* | *routing-process*]

Syntax Description		
	<i>access-list-number</i>	SAP access list number in the range 1000 to 1099. The list explicitly specifies which networks are to be sent and which are to be suppressed in routing updates.
	<i>name</i>	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.
	<i>interface-name</i>	(Optional) Interface on which the access list should be applied to outgoing updates. If no interface is specified, the access list is applied to all outgoing updates.



Note

When you use the **distribute-sap-list out** command after entering the **ipx router eigrp** command to enable the Enhanced Interior Gateway Routing Protocol (EIGRP), you must use the *interface-name* argument. If you do not specify an interface, the routers will not exchange any routes or SAPs with their neighbors.

<i>routing-process</i>	(Optional) Name of a particular routing process as follows: <ul style="list-style-type: none"> • eigrp <i>autonomous-system-number</i> • nlsnp [<i>tag</i>] • rip
------------------------	---

ipx access-group

To apply generic input and output filters to an interface, use the **ipx access-group** command in interface configuration mode. To remove filters, use the **no** form of this command.

ipx access-group {*access-list-number* | *name*} [**in** | **out**]

no ipx access-group {*access-list-number* | *name*} [**in** | **out**]

Syntax Description		
<i>access-list-number</i>	Number of the access list. For standard access lists, <i>access-list-number</i> is a number from 800 to 899. For extended access lists, the value for the <i>access-list-number</i> argument is a number from 900 to 999.	
<i>name</i>	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.	
in	(Optional) Filters inbound packets. All incoming packets defined with either standard or extended access lists are filtered by the entries in this access list.	
out	(Optional) Filters outbound packets. All outgoing packets defined with either standard or extended access lists and forwarded through the interface are filtered by the entries in this access list. This is the default when you do not specify an input (in) or output (out) keyword in the command line.	

ipx access-list

To define an IPX access list by name, use the **ipx access-list** command in global configuration mode. To remove a named IPX access list, use the **no** form of this command.

ipx access-list {**standard** | **extended** | **sap** | **summary**} *name*

no ipx access-list {**standard** | **extended** | **sap** | **summary**} *name*

Syntax Description		
standard	Specifies a standard IPX access list.	
extended	Specifies an extended IPX access list.	
sap	Specifies a SAP access list.	
summary	Specifies area addresses that summarize routes using NLSP route aggregation filtering.	
<i>name</i>	Name of the access list. Names cannot contain a space or quotation mark, and they must begin with an alphabetic character to prevent ambiguity with numbered access lists.	

ipx accounting

To enable IPX accounting, use the **ipx accounting** command in interface configuration mode. To disable IPX accounting, use the **no** form of this command.

ipx accounting

no ipx accounting

Syntax Description This command has no arguments or keywords.

ipx accounting-list

To filter networks for which IPX accounting information is kept, use the **ipx accounting-list** command in global configuration mode. To remove the filter, use the **no** form of this command.

ipx accounting-list *number mask*

no ipx accounting-list *number mask*

Syntax Description	<i>number</i>	Network number. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA you can enter AA.
	<i>mask</i>	Network mask.

ipx accounting-threshold

To set the maximum number of accounting database entries, use the **ipx accounting-threshold** command in global configuration mode. To restore the default, use the **no** form of this command.

ipx accounting-threshold *threshold*

no ipx accounting-threshold *threshold*

Syntax Description	<i>threshold</i>	Maximum number of entries (source and destination address pairs) that the Cisco IOS software can accumulate.
---------------------------	------------------	--

ipx accounting-transits

To set the maximum number of transit entries that will be stored in the IPX accounting database, use the **ipx accounting-transits** command in global configuration mode. To disable this function, use the **no** form of this command.

ipx accounting-transits *count*

no ipx accounting-transits

Syntax Description*count*Number of transit entries that will be stored in the IPX accounting database.

ipx advertise-default-route-only

To advertise only the default RIP route via the specified network, use the **ipx advertise-default-route-only** command in interface configuration mode. To advertise all known RIP routes out the interface, use the **no** form of this command.

ipx advertise-default-route-only *network*

no ipx advertise-default-route-only *network*

Syntax Description*network*Number of the network through which to advertise the default route.

ipx advertise-to-lost-route

To enable the sending of lost route mechanism packets, use the **ipx advertise-to-lost-route** command in global configuration mode. To disable the flooding of network down notifications that are not part of the Novell lost route algorithm, use the **no** form of this command.

ipx advertise-to-lost-route

no ipx advertise-to-lost-route

Syntax Description

This command has no arguments or keywords.

ipx backup-server-query-interval

To change the time between successive queries of each Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor's backup server table, use the **ipx backup-server-query-interval** command in global configuration mode. To restore the default time, use the **no** form of this command.

ipx backup-server-query-interval *interval*

no ipx backup-server-query-interval

Syntax Description	<i>interval</i>	Minimum time, in seconds, between successive queries of each Enhanced IGRP neighbor's backup server table. The default is 15 seconds.
---------------------------	-----------------	---

ipx bandwidth-percent eigrp

To configure the percentage of bandwidth that may be used by Enhanced Interior Gateway Routing Protocol (EIGRP) on an interface, use the **ipx bandwidth-percent eigrp** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipx bandwidth-percent eigrp *as-number percent*

no ipx bandwidth-percent eigrp *as-number*

Syntax Description	<i>as-number</i>	Autonomous system number.
	<i>percent</i>	Percentage of bandwidth that Enhanced IGRP may use.

ipx broadcast-fastswitching

To enable the router to fast switch IPX directed broadcast packets, use the **ipx broadcast-fastswitching** command in global configuration mode. To disable fast switching of IPX directed broadcast packets, use the **no** form of this command.

ipx broadcast-fastswitching

no ipx broadcast-fastswitching

Syntax Description	This command has no arguments or keywords.
---------------------------	--

ipx default-output-rip-delay

To set the default interpacket delay for RIP updates sent on all interfaces, use the **ipx default-output-rip-delay** command in global configuration mode. To return to the initial default delay value, use the **no** form of this command.

ipx default-output-rip-delay *delay*

no ipx default-output-rip-delay

Syntax Description

delay

Delay, in milliseconds (ms), between packets in a multiple-packet RIP update. The default delay is 55 ms. Novell recommends a delay of 55 ms.

ipx default-output-sap-delay

To set a default interpacket delay for SAP updates sent on all interfaces, use the **ipx default-output-sap-delay** command in global configuration mode. To return to the initial default delay value, use the **no** form of this command.

ipx default-output-sap-delay *delay*

no ipx default-output-sap-delay

Syntax Description

delay

Delay, in milliseconds (ms), between packets in a multiple-packet SAP update. The default delay is 55 ms. Novell recommends a delay of 55 ms.

ipx default-route

To forward to the default network all packets for which a route to the destination network is unknown, use the **ipx default-route** command in global configuration mode. To disable the use of the default network, use the **no** form of this command.

ipx default-route

no ipx default-route

Syntax Description

This command has no arguments or keywords.

ipx default-triggered-rip-delay

To set the default interpacket delay for triggered RIP updates sent on all interfaces, use the **ipx default-triggered-rip-delay** command in global configuration mode. To return to the system default delay, use the **no** form of this command.

ipx default-triggered-rip-delay *delay*

no ipx default-triggered-rip-delay [*delay*]

Syntax Description	<i>delay</i>	Delay, in milliseconds (ms), between packets in a multiple-packet RIP update. The default delay is 55 ms. Novell recommends a delay of 55 ms.
---------------------------	--------------	---

ipx default-triggered-rip-holddown

To set the global default for the **ipx triggered-rip-holddown** interface configuration command, use the **ipx default-triggered-rip-holddown** command in global configuration mode. To re-establish the default value of 55 milliseconds, use the **no** form of this command.

ipx default-triggered-rip-holddown *milliseconds*

no ipx default-triggered-rip-holddown *milliseconds*

Syntax Description	<i>milliseconds</i>	Specifies how many milliseconds (ms) a router will wait before sending the triggered route change information.
---------------------------	---------------------	--

ipx default-triggered-sap-delay

To set the default interpacket delay for triggered SAP updates sent on all interfaces, use the **ipx default-triggered-sap-delay** command in global configuration mode. To return to the system default delay, use the **no** form of this command.

ipx default-triggered-sap-delay *delay*

no ipx default-triggered-sap-delay [*delay*]

Syntax Description	<i>delay</i>	Delay, in milliseconds (ms), between packets in a multiple-packet SAP update. The default delay is 55 ms. Novell recommends a delay of 55 ms.
---------------------------	--------------	---

ipx default-triggered-sap-holddown

To set the global default for the **ipx triggered-sap-holddown** interface configuration command, use the **ipx default-triggered-sap-holddown** command in global configuration mode. To re-establish the default value of 55 milliseconds, use the **no** form of this command.

ipx default-triggered-sap-holddown *milliseconds*

no ipx default-triggered-sap-holddown *milliseconds*

Syntax Description	<i>milliseconds</i>	Specifies how many milliseconds (ms) a router will wait before sending the triggered route change information.
---------------------------	---------------------	--

ipx delay

To set the tick count, use the **ipx delay** command in interface configuration mode. To reset the default increment in the delay field, use the **no** form of this command.

ipx delay *ticks*

no ipx delay

Syntax Description	<i>ticks</i>	Number of IBM clock ticks of delay to use. One clock tick is 1/18 of a second (approximately 55 ms).
---------------------------	--------------	--

ipx down

To administratively shut down an IPX network, use the **ipx down** command in interface configuration mode. To restart the network, use the **no** form of this command.

ipx down *network*

no ipx down

Syntax Description	<i>network</i>	Number of the network to shut down. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
---------------------------	----------------	--

ipx eigrp-sap-split-horizon

To configure Enhanced Interior Gateway Routing Protocol (EIGRP) SAP split horizon, use the **ipx eigrp-sap-split-horizon** command in global configuration mode. To revert to the default, use the **no** form of this command.

ipx eigrp-sap-split-horizon

no ipx eigrp-sap-split-horizon

Syntax Description This command has no argument or keywords.

ipx encapsulation

To set the Ethernet frame type of the interface to that of the local file server, use the **ipx encapsulation** command in interface configuration mode. To reset the frame type to the default, use the **no** form of this command.

ipx encapsulation *encapsulation-type*

no ipx encapsulation *encapsulation-type*

Syntax Description *encapsulation-type* (Required) Type of encapsulation (framing). For a list of possible encapsulation types, see Table 23.

Table 23 describes the types of encapsulation available for specific interfaces.

Table 23 Encapsulation Types

Encapsulation Type	Description
arpa	For Ethernet interfaces only—Uses Novell Ethernet_II encapsulation. This encapsulation is recommended for networks that handle both TCP/IP and IPX traffic.
hdlc	For serial interfaces only—Uses High-Level Data Link Control (HDLC) encapsulation.
novell-ether	For Ethernet interfaces only—Uses Novell Ethernet_802.3 encapsulation. This encapsulation consists of a standard 802.3 MAC header followed directly by the IPX header with a checksum of FFFF. It is the default encapsulation used by all versions of NetWare up to and including Version 3.11.
novell-fddi	For FDDI interfaces only—Uses Novell FDDI_RAW encapsulation. This encapsulation consists of a standard FDDI MAC header followed directly by the IPX header with a checksum of 0xFFFF.

Table 23 Encapsulation Types (continued)

Encapsulation Type	Description
sap	<p>For Ethernet interfaces—Uses Novell Ethernet_802.2 encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 Logical Link Control (LLC) header. This is the default encapsulation used by NetWare Version 3.12 and 4.0.</p> <p>For Token Ring interfaces—This encapsulation consists of a standard 802.5 MAC header followed by an 802.2 LLC header.</p> <p>For FDDI interfaces—This encapsulation consists of a standard FDDI MAC header followed by an 802.2 LLC header.</p>
snap	<p>For Ethernet interfaces—Uses Novell Ethernet_Snap encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 Subnetwork Access Protocol (SNAP) LLC header.</p> <p>For Token Ring and FDDI interfaces—This encapsulation consists of a standard 802.5 or FDDI MAC header followed by an 802.2 SNAP LLC header.</p>

ipx flooding-unthrottled

To control whether a router will throttle NetWare Link Services Protocol (NLSP) packets, use the **ipx flooding-unthrottled** command in global configuration mode. To re-establish the default for unthrottled NLSP packets, use the **no** form of this command.

ipx flooding-unthrottled

no ipx flooding-unthrottled

Syntax Description This command has no arguments or keywords.

ipx gns-reply-disable

To disable the sending of replies to IPX Get Nearest Server (GNS) queries, use the **ipx gns-reply-disable** command in interface configuration mode. To return to the default, use the **no** form of this command.

ipx gns-reply-disable

no ipx gns-reply-disable

Syntax Description This command has no arguments or keywords.

ipx gns-response-delay

To change the delay when responding to Get Nearest Server (GNS) requests, use the **ipx gns-response-delay** command in global or interface configuration mode. To return to the default delay, use the **no** form of this command.

```
ipx gns-response-delay [milliseconds]
```

```
no ipx gns-response-delay
```

Syntax Description	<i>milliseconds</i>	(Optional) Time, in milliseconds (ms), that the Cisco IOS software waits after receiving a GNS request from an IPX client before responding with a server name to that client. The default is zero, which indicates no delay.
---------------------------	---------------------	---

ipx gns-round-robin

To rotate using a round-robin selection method through a set of eligible servers when responding to Get Nearest Server (GNS) requests, use the **ipx gns-round-robin** command in global configuration mode. To use the most recently learned server, use the **no** form of this command.

```
ipx gns-round-robin
```

```
no ipx gns-round-robin
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--

ipx hello-interval eigrp

To configure the interval between Enhanced Interior Gateway Routing Protocol (EIGRP) hello packets, use the **ipx hello-interval eigrp** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

```
ipx hello-interval eigrp autonomous-system-number seconds
```

```
no ipx hello-interval eigrp autonomous-system-number seconds
```

Syntax Description	<i>autonomous-system-number</i>	Enhanced IGRP autonomous system number. It can a number from 1 to 65,535.
	<i>seconds</i>	Interval between hello packets, in seconds. The default interval is 5 seconds, which is one-third of the default hold time.

ipx helper-address

To forward broadcast packets to a specified server, use the **ipx helper-address** command in interface configuration mode. To disable this function, use the **no** form of this command.

ipx helper-address *network.node*

no ipx helper-address *network.node*

Syntax Description		
	<i>network</i>	Network on which the target IPX server resides. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. A network number of -1 indicates all-nets flooding. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
	<i>.node</i>	Node number of the target Novell server. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>). A node number of FFFF.FFFF.FFFF matches all servers.

ipx helper-list

To assign an access list to an interface to control broadcast traffic (including type 20 propagation packets), use the **ipx helper-list** command in interface configuration mode. To remove the access list from an interface, use the **no** form of this command.

ipx helper-list {*access-list-number* | *name*}

no ipx helper-list {*access-list-number* | *name*}

Syntax Description		
	<i>access-list-number</i>	Number of the access list. All outgoing packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, the value for the <i>access-list-number</i> argument is a number from 800 to 899. For extended access lists, it is a number from 900 to 999.
	<i>name</i>	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.

ipx hold-down eigrp

To specify the length of time a lost Enhanced Interior Gateway Routing Protocol (EIGRP) route is placed in the hold-down state, use the **ipx hold-down eigrp** command in interface configuration mode. To restore the default time, use the **no** form of this command.

ipx hold-down eigrp *autonomous-system-number seconds*

no ipx hold-down eigrp *autonomous-system-number seconds*

Syntax Description	
<i>autonomous-system-number</i>	Enhanced IGRP autonomous system number. It can be a number from 1 to 65,535.
<i>seconds</i>	Hold-down time, in seconds. The default hold time is 5 seconds.

ipx hold-time eigrp

To specify the length of time for which a neighbor should consider Enhanced IGRP hello packets valid, use the **ipx hold-time eigrp** command in interface configuration mode. To restore the default time, use the **no** form of this command.

ipx hold-time eigrp *autonomous-system-number seconds*

no ipx hold-time eigrp *autonomous-system-number seconds*

Syntax Description	
<i>autonomous-system-number</i>	Enhanced IGRP autonomous system number. It can be a number from 1 to 65,535.
<i>seconds</i>	Hold time, in seconds. The hold time is advertised in hello packets and indicates to neighbors the length of time they should consider the sender valid. The default hold time is 15 seconds, which is three times the hello interval.

ipx input-network-filter

To control which networks are added to the Cisco IOS software routing table, use the **ipx input-network-filter** command in interface configuration mode. To remove the filter from the interface, use the **no** form of this command.

ipx input-network-filter {*access-list-number* | *name*}

no ipx input-network-filter {*access-list-number* | *name*}

Syntax Description	<i>access-list-number</i>	Number of the access list. All incoming packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, the value for the <i>access-list-number</i> argument is a number from 800 to 899. For extended access lists, it is a number from 900 to 999.
	<i>name</i>	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.

ipx input-sap-filter

To control which services are added to the Cisco IOS software SAP table, use the **ipx input-sap-filter** command in interface configuration mode. To remove the filter, use the **no** form of this command.

ipx input-sap-filter {*access-list-number* | *name*}

no ipx input-sap-filter {*access-list-number* | *name*}

Syntax Description	<i>access-list-number</i>	Number of the SAP access list. All incoming packets are filtered by the entries in this access list. The argument <i>access-list-number</i> is a number from 1000 to 1099.
	<i>name</i>	Name of the access list. Names cannot contain a space or quotation mark, and they must begin with an alphabetic character to prevent ambiguity with numbered access lists.

ipx internal-network

To set an internal network number for use by NetWare Link Services Protocol (NLSP) and IPXWAN, use the **ipx internal-network** command in global configuration mode. To remove an internal network number, use the **no** form of this command.

ipx internal-network *network-number*

no ipx internal-network [*network-number*]

Syntax Description	<i>network-number</i>	Number of the internal network.
---------------------------	-----------------------	---------------------------------

ipx ipxwan

To enable the IPX wide-area network (IPXWAN) protocol on a serial interface, use the **ipx ipxwan** command in interface configuration mode. To disable the IPXWAN protocol, use the **no** form of this command.

```
ipx ipxwan [local-node {network-number | unnumbered} local-server-name retry-interval
retry-limit]
```

```
no ipx ipxwan
```

Syntax Description	
<i>local-node</i>	(Optional) Primary network number of the router. This is an IPX network number that is unique across the entire internetwork. On NetWare 3.x servers, the primary network number is called the internal network number. The device with the higher number is determined to be the link master. A value of 0 causes the Cisco IOS software to use the configured internal network number.
<i>network-number</i>	(Optional) IPX network number to be used for the link if this router is the one determined to be the link master. The number is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 0 to FFFFFFFD. A value 0 is equivalent to specifying the keyword unnumbered . You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
unnumbered	(Optional) Specifies that no IPX network number is defined for the link. This is equivalent to specifying a value of 0 for the <i>network-number</i> argument.
<i>local-server-name</i>	(Optional) Name of the local router. It can be up to 47 characters long, and can contain uppercase letters, digits, underscores (_), hyphens (-), and at signs (@). On NetWare 3.x servers, this is the router name. For our routers, this is the name of the router as configured via the hostname command; that is, the name that precedes the standard prompt, which is an angle bracket (>) for EXEC mode or a pound sign (#) for privileged EXEC mode.
<i>retry-interval</i>	(Optional) Retry interval, in seconds. This interval defines how often the software will retry the IPXWAN start-up negotiation if a startup failure occurs. Retries will occur until the retry limit defined by the <i>retry-limit</i> argument is reached. It can be a value from 1 to 600. The default is 20 seconds.
<i>retry-limit</i>	(Optional) Maximum number of times the software retries the IPXWAN startup negotiation before taking the action defined by the ipx ipxwan error command. It can be a value from 1 through 100. The default is 3.

ipx ipxwan error

To define how to handle IPX wide-area network (IPXWAN) when IPX fails to negotiate properly at link startup, use the **ipx ipxwan error** command in interface configuration mode. To restore the default, use the **no** form of this command.

ipx ipxwan error [**reset** | **resume** | **shutdown**]

no ipx ipxwan error [**reset** | **resume** | **shutdown**]

Syntax Description		
	reset	(Optional) Resets the link when negotiations fail. This is the default action.
	resume	(Optional) When negotiations fail, IPXWAN ignores the failure, takes no special action, and resumes the start-up negotiation attempt.
	shutdown	(Optional) Shuts down the link when negotiations fail.

ipx ipxwan static

To negotiate static routes on a link configured for IPX wide-area network (IPXWAN), use the **ipx ipxwan static** command in interface configuration mode. To disable static route negotiation, use the **no** form of this command.

ipx ipxwan static

no ipx ipxwan static

Syntax Description This command has no arguments or keywords.

ipx link-delay

To specify the link delay, use the **ipx link-delay** command in interface configuration mode. To return to the default link delay, use the **no** form of this command.

ipx link-delay *microseconds*

no ipx link-delay *microseconds*

Syntax Description	<i>microseconds</i>	Delay, in microseconds.

ipx linkup-request

To enable the sending of a general RIP and/or SAP query when an interface comes up, use the **ipx linkup-request** command in interface configuration mode. To disable the sending of a general RIP and/or SAP query when an interface comes up, use the **no** form of this command.

```
ipx linkup-request {rip | sap}
```

```
no ipx linkup-request {rip | sap}
```

Syntax Description

rip	Enables the sending of a general RIP query when an interface comes up.
sap	Enables the sending of a general SAP query when an interface comes up.

ipx maximum-hops

To set the maximum hop count allowed for IPX packets, use the **ipx maximum-hops** command in global configuration mode. To return to the default number of hops, use the **no** form of this command.

```
ipx maximum-hops hops
```

```
no ipx maximum-hops hops
```

Syntax Description

<i>hops</i>	Maximum number of hops considered to be reachable by non-RIP routing protocols. Also, maximum number of routers that an IPX packet can traverse before being dropped. It can be a value from 16 to 254. The default is 16 hops.
-------------	---

ipx maximum-paths

To set the maximum number of equal-cost paths that the Cisco IOS software uses when forwarding packets, use the **ipx maximum-paths** command in global configuration mode. To restore the default value, use the **no** form of this command.

```
ipx maximum-paths paths
```

```
no ipx maximum-paths
```

Syntax Description

<i>paths</i>	Maximum number of equal-cost paths which the Cisco IOS software will use. It can be a number from 1 to 512. The default value is 1.
--------------	---

ipx netbios input-access-filter

To control incoming IPX NetBIOS FindName messages, use the **ipx netbios input-access-filter** command in interface configuration mode. To remove the filter, use the **no** form of this command.

ipx netbios input-access-filter {**host** | **bytes**} *name*

no ipx netbios input-access-filter {**host** | **bytes**} *name*

Syntax Description	host	bytes	name
	Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more netbios access-list host commands.	Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more netbios access-list bytes commands.	Name of a NetBIOS access list.

ipx netbios output-access-filter

To control outgoing NetBIOS FindName messages, use the **ipx netbios output-access-filter** command in interface configuration mode. To remove the filter, use the **no** form of this command.

ipx netbios output-access-filter {**host** | **bytes**} *name*

no ipx netbios output-access-filter {**host** | **bytes**} *name*

Syntax Description	host	bytes	name
	Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more netbios access-list host commands.	Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more netbios access-list bytes commands.	Name of a previously defined NetBIOS access list.

ipx netbios-socket-input-checks

To enable additional checks that are performed on Network Basic Input/Output System (NetBIOS) packets that do not conform fully to Novell Type20 NetBIOS packets, use the **ipx netbios-socket-input-checks** command in global configuration mode. To disable the additional checking, use the **no** form of this command.

ipx netbios-socket-input-checks

no ipx netbios-socket-input-checks

Syntax Description This command has no arguments or keywords.

ipx network

To enable IPX routing on a particular interface and to optionally select the type of encapsulation (framing), use the **ipx network** command in interface configuration mode. To disable IPX routing, use the **no** form of this command.

ipx network *network* [**encapsulation** *encapsulation-type* [**secondary**]]

no ipx network *network* [**encapsulation** *encapsulation-type*]

Syntax Description		
<i>network</i>	Network number. This is an 8-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD.	You do not need to specify leading zeros in the network number. For example, for the network number 000000AA you can enter AA.
encapsulation <i>encapsulation-type</i>	(Optional) Type of encapsulation (framing). For a list of possible encapsulation types, see Table 24.	
secondary	(Optional) Indicates an additional (secondary) network configured after the first (primary) network.	

Table 24 describes the types of encapsulation available for specific interfaces.

Table 24 Encapsulation Types

Encapsulation Type	Description
arpa	For Ethernet interfaces only—Uses Novell Ethernet_II encapsulation. This encapsulation is recommended for networks that handle both TCP/IP and IPX traffic.
hdlc	For serial interfaces only—Uses High-Level Data Link Control (HDLC) encapsulation.
novell-ether	For Ethernet interfaces only—Uses Novell Ethernet_802.3 encapsulation. This encapsulation consists of a standard 802.3 MAC header followed directly by the IPX header with a checksum of FFFF. It is the default encapsulation used by all versions of NetWare up to and including Version 3.11.
novell-fddi	For FDDI interfaces only—Uses Novell FDDI_RAW encapsulation. This encapsulation consists of a standard FDDI MAC header followed directly by the IPX header with a checksum of 0xFFFF.

Table 24 Encapsulation Types (continued)

Encapsulation Type	Description
sap	<p>For Ethernet interfaces—Uses Novell Ethernet_802.2 encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 Logical Link Control (LLC) header. This is the default encapsulation used by NetWare Version 3.12 and 4.0.</p> <p>For Token Ring interfaces—This encapsulation consists of a standard 802.5 MAC header followed by an 802.2 LLC header.</p> <p>For FDDI interfaces—This encapsulation consists of a standard FDDI MAC header followed by an 802.2 LLC header.</p>
snap	<p>For Ethernet interfaces—Uses Novell Ethernet_Snap encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 Subnetwork Access Protocol (SNAP) LLC header.</p> <p>For Token Ring and FDDI interfaces—This encapsulation consists of a standard 802.5 or FDDI MAC header followed by an 802.2 SNAP LLC header.</p>

ipx nhrp authentication

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

ipx nhrp authentication *string*

no ipx nhrp authentication [*string*]

Syntax Description

<i>string</i>	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.
---------------	---

ipx nhrp holdtime

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

ipx nhrp holdtime *seconds-positive* [*seconds-negative*]

no ipx nhrp holdtime [*seconds-positive* [*seconds-negative*]]

Syntax Description	<i>seconds-positive</i>	Time in seconds for which NBMA addresses are advertised as valid in positive authoritative NHRP responses.
	<i>seconds-negative</i>	(Optional) Time in seconds for which NBMA addresses are advertised as valid in negative authoritative NHRP responses.

ipx nhrp interest

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

```
ipx nhrp interest access-list-number
```

```
no ipx nhrp interest [access-list-number]
```

Syntax Description	<i>access-list-number</i>	Standard or extended IPX access list number from 800 through 999.
---------------------------	---------------------------	---

ipx nhrp map

To statically configure the IPX-to-NBMA address mapping of IPX destinations connected to a nonbroadcast multiaccess (NBMA) network, use the **ipx nhrp map** command in interface configuration mode. To remove the static entry from NHRP cache, use the **no** form of this command.

```
ipx nhrp map ipx-address nbma-address
```

```
no ipx nhrp map ipx-address nbma-address
```

Syntax Description	<i>ipx-address</i>	IPX address of the destinations reachable through the NBMA network. This address is mapped to the NBMA address.
	<i>nbma-address</i>	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, and SMDS has an E.164 address. This address is mapped to the IPX address.

ipx nhrp max-send

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

```
ipx nhrp max-send pkt-count every interval
```

```
no ipx nhrp max-send
```

Syntax Description

<i>pkt-count</i>	Number of packets for which can be transmitted in the range 1 to 65,535.
<i>every interval</i>	Time (in seconds) in the range 10 to 65,535. Default is 10 seconds.

ipx nhrp network-id

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

ipx nhrp network-id *number*

no ipx nhrp network-id

Syntax Description

<i>number</i>	Globally unique, 32-bit network identifier for a nonbroadcast multiaccess (NBMA) network. The range is 1 to 4,294,967,295.
---------------	--

ipx nhrp nhs

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

ipx nhrp nhs *nhs-address* [*net-address*]

no ipx nhrp nhs *nhs-address* [*net-address*]

Syntax Description

<i>nhs-address</i>	Address of the Next Hop Server being specified.
<i>net-address</i>	(Optional) IPX address of a network served by the Next Hop Server.

ipx nhrp record

To re-enable the use of forward record and reverse record options in Next Hop Resolution Protocol (NHRP) Request and Reply packets, use the **ipx nhrp record** command in interface configuration mode. To suppress the use of such options, use the **no** form of this command.

ipx nhrp record

no ipx nhrp record

Syntax Description

This command has no arguments or keywords.

ipx nhrp responder

To designate which interface's primary IPX address that the Next Hop Server uses in Next Hop Resolution Protocol (NHRP) Reply packets when the NHRP requestor uses the Responder Address option, use the **ipx nhrp responder** command in interface configuration mode. To remove the designation, use the **no** form of this command.

ipx nhrp responder *type number*

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

Syntax Description		
	<i>type</i>	Interface type whose primary IPX address is used when a Next Hop Server complies with a Responder Address option. Valid options are atm , serial , and tunnel .
	<i>number</i>	Interface number whose primary IPX address is used when a Next Hop Server complies with a Responder Address option.

ipx 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 **ipx nhrp use** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipx nhrp use *usage-count*

no ipx nhrp use *usage-count*

Syntax Description		
	<i>usage-count</i>	Packet count in the range 1 to 65,535.

ipx nlsnp csnp-interval

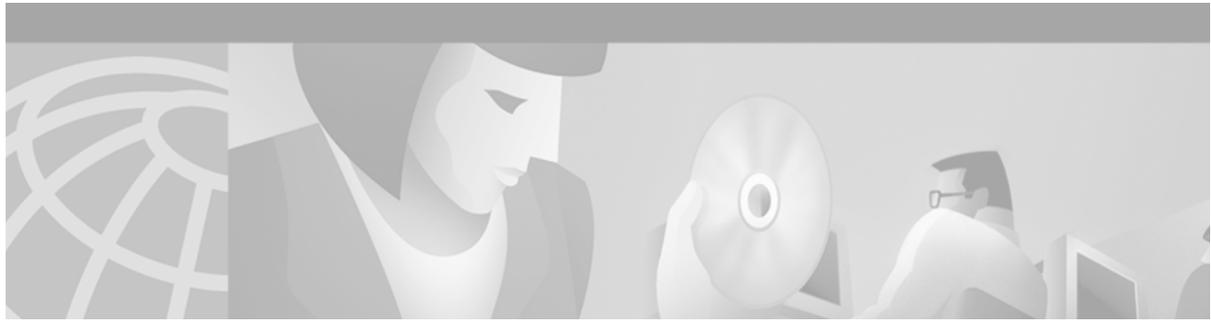
To configure the NetWare Link-Services Protocol (NLSP) complete sequence number PDU (CSNP) interval, use the **ipx nlsnp csnp-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipx nlsnp [*tag*] **csnp-interval** *seconds*

no ipx nlsnp [*tag*] **csnp-interval** *seconds*

Syntax Description		
	<i>tag</i>	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
	<i>seconds</i>	Time, in seconds, between the transmission of CSNPs on multiaccess networks. This interval applies to the designated router only. The interval can be a number in the range 1 to 600. The default is 30 seconds.

■ ipx nlsnp-interval



Novell IPX Commands: `ipx nlsf enable` Through `spf-interval`

This chapter describes the function and syntax of the Novell IPX commands: **`ipx nlsf enable`** through **`spf-interval`**. For more information about these commands, refer to the corresponding chapter in the *Cisco IOS AppleTalk and Novell IPX Command Reference*.

`ipx nlsf enable`

To enable NetWare Link-Services Protocol (NLSP) routing on the primary network configured on this interface or subinterface, use the **`ipx nlsf enable`** command in interface configuration mode. To disable NLSP routing on the primary network configured on this interface or subinterface, use the **`no`** form of this command.

`ipx nlsf [tag] enable`

`no ipx nlsf [tag] enable`

Syntax Description	<i>tag</i>	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
---------------------------	------------	--

`ipx nlsf hello-interval`

To configure the interval between the transmission of hello packets, use the **`ipx nlsf hello-interval`** command in interface configuration mode. To restore the default value, use the **`no`** form of this command.

`ipx nlsf [tag] hello-interval seconds`

`no ipx nlsf [tag] hello-interval seconds`

Syntax Description	<i>tag</i>	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
	<i>seconds</i>	Time, in seconds, between the transmission of hello packets on the interface. It can be a number in the range 1 to 1600. The default is 10 seconds for the designated router and 20 seconds for nondesignated routers.

ipx nlsip hello-multiplier

To specify the hello multiplier used on an interface, use the **ipx nlsip hello-multiplier** command in interface configuration mode. To restore the default value, use the **no** form of this command.

```
ipx nlsip [tag] hello-multiplier multiplier
```

```
no ipx nlsip [tag] hello-multiplier
```

Syntax Description	<i>tag</i>	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
	<i>multiplier</i>	Value by which to multiply the hello interval. It can be a number in the range 3 to 1000. The default is 3.

ipx nlsip lsp-interval

To configure the time delay between successive NetWare Link-Services Protocol (NLSP) link-state packet (LSP) transmissions, use the **ipx nlsip lsp-interval** command in interface configuration mode. To restore the default time delay, use the **no** form of this command.

```
ipx nlsip [tag] lsp-interval interval
```

```
no ipx nlsip [tag] lsp-interval
```

Syntax Description	<i>tag</i>	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
	<i>interval</i>	Time, in milliseconds, between successive LSP transmissions. The interval can be a number in the range 55 and 5000. The default interval is 55 milliseconds (ms).

ipx nlsip metric

To configure the NetWare Link-Services Protocol (NLSP) cost for an interface, use the **ipx nlsip metric** command in interface configuration mode. To restore the default cost, use the **no** form of this command.

```
ipx nlsip [tag] metric metric-number
```

```
no ipx nlsip [tag] metric metric-number
```

Syntax Description	<i>tag</i>	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
	<i>metric-number</i>	Metric value for the interface. It can be a number from 0 to 63.

ipx nlspl multicast

To configure an interface to use multicast addressing, use the **ipx nlspl multicast** command in interface configuration mode. To configure the interface to use broadcast addressing, use the **no** form of this command.

ipx nlspl [*tag*] **multicast**

no ipx nlspl [*tag*] **multicast**

Syntax Description	<i>tag</i>	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
---------------------------	------------	--

ipx nlspl priority

To configure the election priority of the specified interface for designated router election, use the **ipx nlspl priority** command in interface configuration mode. To restore the default priority, use the **no** form of this command.

ipx nlspl [*tag*] **priority** *priority-number*

no ipx nlspl [*tag*] **priority** *priority-number*

Syntax Description	<i>tag</i>	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
	<i>priority-number</i>	Election priority of the designated router for the specified interface. This can be a number in the range 0 to 127. This value is unitless. The default is 44.

ipx nlspl retransmit-interval

To configure the link-state packet (LSP) retransmission interval on WAN links, use the **ipx nlspl retransmit-interval** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

ipx nlspl [*tag*] **retransmit-interval** *seconds*

no ipx nlspl [*tag*] **retransmit-interval** *seconds*

Syntax Description	<i>tag</i>	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
	<i>seconds</i>	LSP retransmission interval, in seconds. This can be a number in the range 1 to 30. The default is 5 seconds.

ipx nlsip rip

To configure RIP compatibility when NetWare Link-Services Protocol (NLSP) is enabled, use the **ipx nlsip rip** command in interface configuration mode. To restore the default, use the **no** form of this command.

ipx nlsip [*tag*] **rip** [**on** | **off** | **auto**]

no ipx nlsip [*tag*] **rip** [**on** | **off** | **auto**]

Syntax Description	<i>tag</i>	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
	on	(Optional) Always generates and sends RIP periodic traffic.
	off	(Optional) Never generates and sends RIP periodic traffic.
	auto	(Optional) Sends RIP periodic traffic only if another RIP router in sending periodic RIP traffic. This is the default.

ipx nlsip sap

To configure SAP compatibility when NetWare Link-Services Protocol (NLSP) is enabled, use the **ipx nlsip sap** command in interface configuration mode. To restore the default, use the **no** form of this command.

ipx nlsip [*tag*] **sap** [**on** | **off** | **auto**]

no ipx nlsip [*tag*] **sap** [**on** | **off** | **auto**]

Syntax Description	<i>tag</i>	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
	on	(Optional) Always generates and sends SAP periodic traffic.
	off	(Optional) Never generates and sends SAP periodic traffic.
	auto	(Optional) Sends SAP periodic traffic only if another SAP router in sending periodic SAP traffic. This is the default.

ipx output-ggs-filter

To control which servers are included in the Get General Service (GGS) responses sent by Cisco IOS software, use the **ipx output-ggs-filter** command in interface configuration mode. To remove the filter from the interface, use the **no** form of this command.

ipx output-ggs-filter {*access-list-number* | *name*}

no ipx output-ggs-filter {*access-list-number* | *name*}

Syntax Description

<i>access-list-number</i>	Number of the Service Advertising Protocol (SAP) access list. All outgoing GGS packets are filtered by the entries in this list. The <i>access-list number</i> is a number from 1000 to 1099.
<i>name</i>	Name of the access list. Names cannot contain a space or quotation mark, and they must begin with an alphabetic character to prevent their being confused with numbered access lists.

ipx output-gns-filter

To control which servers are included in the Get Nearest Server (GNS) responses sent by Cisco IOS software, use the **ipx output-gns-filter** command in interface configuration mode. To remove the filter from the interface, use the **no** form of this command.

ipx output-gns-filter {*access-list-number* | *name*}

no ipx output-gns-filter {*access-list-number* | *name*}

Syntax Description

<i>access-list-number</i>	Number of the SAP access list. All outgoing GNS packets are filtered by the entries in this access list. The argument <i>access-list-number</i> is a number from 1000 to 1099.
<i>name</i>	Name of the access list. Names cannot contain a space or quotation mark, and they must begin with an alphabetic character to prevent ambiguity with numbered access lists.

ipx output-network-filter

To control the list of networks included in routing updates sent out an interface, use the **ipx output-network-filter** command in interface configuration mode. To remove the filter from the interface, use the **no** form of this command.

ipx output-network-filter {*access-list-number* | *name*}

no ipx output-network-filter {*access-list-number* | *name*}

Syntax Description	<i>access-list-number</i>	Number of the access list. All outgoing packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, <i>access-list-number</i> is a number from 800 to 899. For extended access lists, it is a number from 900 to 999.
	<i>name</i>	Name of the access list. Names cannot contain a space or quotation mark, and they must begin with an alphabetic character to prevent ambiguity with numbered access lists.

ipx output-rip-delay

To set the interpacket delay for RIP updates sent on a single interface, use the **ipx output-rip-delay** command in interface configuration mode. To return to the default value, use the **no** form of this command.

```
ipx output-rip-delay delay
```

```
no ipx output-rip-delay [delay]
```

Syntax Description	<i>delay</i>	Delay, in milliseconds (ms), between packets in a multiple-packet RIP update. The default delay is 55 ms. Novell recommends a delay of 55 ms.
---------------------------	--------------	---

ipx output-sap-delay

To set the interpacket delay for Service Advertising Protocol (SAP) updates sent on a single interface, use the **ipx output-sap-delay** command in interface configuration mode. To return to the default delay value, use the **no** form of this command.

```
ipx output-sap-delay delay
```

```
no ipx output-sap-delay
```

Syntax Description	<i>delay</i>	Delay, in milliseconds, between packets in a multiple-packet SAP update. The default delay is 55 ms. Novell recommends a delay of 55 ms.
---------------------------	--------------	--

ipx output-sap-filter

To control which services are included in Service Advertising Protocol (SAP) updates sent by Cisco IOS software, use the **ipx output-sap-filter** command in interface configuration mode. To remove the filter, use the **no** form of this command.

```
ipx output-sap-filter {access-list-number | name}
```

```
no ipx output-sap-filter {access-list-number | name}
```

Syntax Description		
	<i>access-list-number</i>	Number of the SAP access list. All outgoing service advertisements are filtered by the entries in this access list. The argument <i>access-list-number</i> is a number from 1000 to 1099.
	<i>name</i>	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.

ipx pad-process-switched-packets

To control whether odd-length packets are padded so as to be sent as even-length packets on an interface, use the **ipx pad-process-switched-packets** command in interface configuration mode. To disable padding, use the **no** form of this command.

```
ipx pad-process-switched-packets
```

```
no ipx pad-process-switched-packets
```

Syntax Description This command has no arguments or keywords.

ipx per-host-load-share

To enable per-host load sharing, use the **ipx per-host-load-share** command in global configuration mode. To disable per-host load sharing, use the **no** form of this command.

```
ipx per-host-load-share
```

```
no ipx per-host-load-share
```

Syntax Description This command has no arguments or keywords.

ipx ping-default

To select the ping type that Cisco IOS software transmits, use the **ipx ping-default** command in global configuration mode. To return to the default ping type, use the **no** form of this command.

```
ipx ping-default { cisco | novell | diagnostic }
```

```
no ipx ping-default { cisco | novell | diagnostic }
```

Syntax Description		
	cisco	Transmits Cisco pings.
	novell	Transmits standard Novell pings.
	diagnostic	Transmits diagnostic request/response for IPX pings.

ipx potential-pseudonode

To enable NetWare Link Services Protocol (NLSP) to keep backup router and service information for potential pseudonode, use the **ipx potential-pseudonode** command in global configuration mode. To disable the feature so that NLSP does not keep backup router and service information for potential pseudonode, use the **no** form of this command.

ipx potential-pseudonode

no ipx potential-pseudonode

Syntax Description This command has no arguments or keywords.

ipx rip-max-packetsize

To configure the maximum packet size of RIP updates sent out the interface, use the **ipx rip-max-packetsize** command in interface configuration mode. To restore the default packet size, use the **no** form of this command.

ipx rip-max-packetsize *bytes*

no ipx rip-max-packetsize *bytes*

Syntax Description	<i>bytes</i>	Maximum packet size in bytes. The default is 432 bytes, which allows for 50 routes at 8 bytes each, plus 32 bytes of IPX network and RIP header information.
---------------------------	--------------	--

ipx rip-multiplier

To configure the interval at which a network's RIP entry ages out, use the **ipx rip-multiplier** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

ipx rip-multiplier *multiplier*

no ipx rip-multiplier *multiplier*

Syntax Description	<i>multiplier</i>	Multiplier used to calculate the interval at which to age out RIP routing table entries. This can be any positive number. The value you specify is multiplied by the RIP update interval to determine the aging-out interval. The default is three times the RIP update interval.
---------------------------	-------------------	---

ipx rip-queue-maximum

To set an IPX Routing Information Protocol (RIP) queue maximum to control how many RIP packets can be waiting to be processed at any given time, use the **ipx rip-queue-maximum** command in global configuration mode. To clear a set RIP queue maximum, use the **no** form of this command.

ipx rip-queue-maximum *milliseconds*

no ipx rip-queue-maximum *milliseconds*

Syntax Description	<i>milliseconds</i>	Specifies the queue limit as a number from 0 to the maximum unassigned integer.
---------------------------	---------------------	---

ipx rip-update-queue-maximum

To set an IPX Routing Information Protocol (RIP) queue maximum to control how many incoming RIP update packets can be waiting to be processed at any given time, use the **ipx rip-update-queue-maximum** command in global configuration mode. To clear a set RIP queue maximum, use the **no** form of this command.

ipx rip-update-queue-maximum *queue-maximum*

no ipx rip-update-queue-maximum *queue-maximum*

Syntax Description	<i>queue-maximum</i>	Specifies the queue limit as a number from 0 to the maximum unassigned integer.
---------------------------	----------------------	---

ipx rip-response-delay

To change the delay when responding to Routing Information Protocol (RIP) requests, use the **ipx rip-response-delay** command in interface configuration mode. To return to the default delay, use the **no** form of this command.

ipx rip-response-delay *ms*

no ipx rip-response-delay

Syntax Description	<i>ms</i>	Delay time, in milliseconds, for RIP responses.
---------------------------	-----------	---

ipx route

To add a static route or static NetWare Link Services Protocol (NLSP) route summary to the routing table, use the **ipx route** command in global configuration mode. To remove a route from the routing table, use the **no** form of this command.

```
ipx route {network [network-mask] | default} {network.node | interface} [ticks] [hops]
[floating-static]
```

```
no ipx route
```

Syntax Description

<i>network</i>	<p>Network to which you want to establish a static route.</p> <p>This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.</p>
<i>network-mask</i>	<p>(Optional) Specifies the portion of the network address that is common to all addresses in an NLSP route summary. When used with the <i>network</i> argument, it specifies the static route summary.</p> <p>The high-order bits of <i>network-mask</i> must be contiguous Fs, while the low-order bits must be contiguous zeros (0). An arbitrary mix of Fs and 0s is not permitted.</p>
default	<p>Creates a static entry for the “default route.” The router forwards all nonlocal packets for which no explicit route is known via the specified next hop address (<i>network.node</i>) or interface.</p>
<i>network.node</i>	<p>Router to which to forward packets destined for the specified network.</p> <p>The argument <i>network</i> is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.</p> <p>The argument <i>node</i> is the node number of the target router. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxx.xxxx.xxx</i>).</p>
<i>interface</i>	<p>Network interface to which to forward packets destined for the specified network. Interface is serial 0 or serial 0.2. Specifying an interface instead of a network node is intended for use on IPXWAN unnumbered interfaces. The specified interface can be a null interface.</p>
<i>ticks</i>	<p>(Optional) Number of IBM clock ticks of delay to the network for which you are establishing a static route. One clock tick is 1/18 of a second (approximately 55 ms). Valid values are 1 through 65,534.</p>
<i>hops</i>	<p>(Optional) Number of hops to the network for which you are establishing a static route. Valid values are 1 through 254.</p>
floating-static	<p>(Optional) Specifies that this route is a floating static route, which is a static route that can be overridden by a dynamically learned route.</p>

ipx route-cache

To enable IPX fast switching, use the **ipx route-cache** command in interface configuration mode. To disable fast switching, use the **no** form of this command.

ipx route-cache

no ipx route-cache

Syntax Description This command has no arguments or keywords.

ipx route-cache inactivity-timeout

To adjust the period and rate of route cache invalidation because of inactivity, use the **ipx route-cache inactivity-timeout** command in global configuration mode. To return to the default values, use the **no** form of this command.

ipx route-cache inactivity-timeout *period* [*rate*]

no ipx route-cache inactivity-timeout

Syntax Description	<i>period</i>	Number of minutes that a valid cache entry may be inactive before it is invalidated. Valid values are 0 through 65,535. A value of zero disables this feature.
	<i>rate</i>	(Optional) Maximum number of inactive entries that may be invalidated per minute. Valid values are 0 through 65,535. A value of zero means no limit.

ipx route-cache max-size

To set a maximum limit on the number of entries in the IPX route cache, use the **ipx route-cache max-size** command in global configuration mode. To return to the default setting, use the **no** form of this command.

ipx route-cache max-size *size*

no ipx route-cache max-size

Syntax Description	<i>size</i>	Maximum number of entries allowed in the IPX route cache.
---------------------------	-------------	---

ipx route-cache update-timeout

To adjust the period and rate of route cache invalidation because of aging, use the **ipx route-cache update-timeout** command in global configuration mode. To return to the default values, use the **no** form of this command.

ipx route-cache update-timeout *period* [*rate*]

no ipx route-cache update-timeout

Syntax Description		
<i>period</i>		Number of minutes since a valid cache entry was created before it may be invalidated. A value of zero disables this feature.
<i>rate</i>		(Optional) Maximum number of aged entries that may be invalidated per minute. A value of zero means no limit.

ipx router

To specify the routing protocol to use, use the **ipx router** command in global configuration mode. To disable a particular routing protocol on the router, use the **no** form of this command.

ipx router { **eigrp** *autonomous-system-number* | **nlspp** [*tag*] | **rip** }

no ipx router { **eigrp** *autonomous-system-number* | **nlspp** [*tag*] | **rip** }

Syntax Description		
eigrp <i>autonomous-system-number</i>		Enables the Enhanced Interior Gateway Routing Protocol (EIGRP) routing protocol. The argument <i>autonomous-system-number</i> is the Enhanced IGRP autonomous system number. It can be a number from 1 to 65,535.
nlspp [<i>tag</i>]		Enables the NetWare Link Services Protocol (NLSP) routing protocol. The optional argument <i>tag</i> names the NLSP process to which you are assigning the NLSP protocol. If the router has only one process, defining a <i>tag</i> is optional. A maximum of three NLSP processes may be configured on the router at the same time. The <i>tag</i> can be any combination of printable characters.
rip		Enables the Routing Information Protocol (RIP) routing protocol. It is on by default.

ipx router-filter

To filter the routers from which packets are accepted, use the **ipx router-filter** command in interface configuration mode. To remove the filter from the interface, use the **no** form of this command.

ipx router-filter { *access-list-number* | *name* }

no ipx router-filter

Syntax Description	<i>access-list-number</i>	Number of the access list. All incoming packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, <i>access-list-number</i> is a number from 800 to 899. For extended access lists, it is a number from 900 to 999.
	<i>name</i>	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.

ipx router-sap-filter

To filter Service Advertising Protocol (SAP) messages received from a particular router, use the **ipx router-sap-filter** command in interface configuration mode. To remove the filter, use the **no** form of this command.

```
ipx router-sap-filter {access-list-number | name}
```

```
no ipx router-sap-filter {access-list-number | name}
```

Syntax Description	<i>access-list-number</i>	Number of the access list. All incoming service advertisements are filtered by the entries in this access list. The argument <i>access-list-number</i> is a number from 1000 to 1099.
	<i>name</i>	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.

ipx routing

To enable IPX routing, use the **ipx routing** command in global configuration mode. To disable IPX routing, use the **no** form of this command.

```
ipx routing [node]
```

```
no ipx routing
```

Syntax Description	<i>node</i>	(Optional) Node number of the router. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>). It must not be a multicast address. If you omit the <i>node</i> argument, the Cisco IOS software uses the hardware MAC address currently assigned to it as its node address. This is the MAC address of the first Ethernet, Token Ring, or FDDI interface card. If no satisfactory interfaces are present in the router (such as only serial interfaces), you must specify a value for the <i>node</i> argument.
---------------------------	-------------	---

ipx sap

To specify static Service Advertising Protocol (SAP) entries, use the **ipx sap** command in global configuration mode. To remove static SAP entries, use the **no** form of this command.

ipx sap *service-type name network.node socket hop-count*

no ipx sap *service-type name network.node socket hop-count*

Syntax Description	
<i>service-type</i>	SAP service-type number. See the access-list (SAP filtering) command earlier in this chapter for a table of some IPX SAP services.
<i>name</i>	Name of the server that provides the service.
<i>network.node</i>	Network number and node address of the server. The argument <i>network</i> is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA you can enter AA. The argument <i>node</i> is the node number of the target Novell server. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>).
<i>socket</i>	Socket number for this service. See access-list (IPX extended) command earlier in this chapter for a table of some IPX socket numbers.
<i>hop-count</i>	Number of hops to the server.

ipx sap follow-route-path

To enable a router to accept IPX Service Advertising Protocol (SAP) entries from SAP updates received on an interface only if that interface is one of the best paths to reach the destination networks of those SAPs, use the **ipx sap follow-route-path** command in global configuration mode. To disable this router function, use **no** form of this command.

ipx sap follow-route-path

no ipx sap follow-route-path

Syntax Description This command has no arguments or keywords.

ipx sap-helper

To set an address, which should be another Cisco router that is adjacent to the router being configured, to which all Service Advertising Protocol (SAP) request packets are received, use the **ipx sap-helper** command in interface configuration mode. To remove the address and stop forwarding SAP request packets, use the **no** form of this command.

ipx sap-helper *network.node*

no ipx sap-helper *network.node*

Syntax Description	<i>network.node</i>	<p>The argument <i>network</i> is the network on which the SAP helper router resides. This eight-digit hexadecimal number uniquely identifies a network cable segment. It can be a number in the range from 1 to FFFFFFFD. You do not need to specify the leading zeros in the network number. For example, for the network number 00000AA, you can enter AA.</p> <p>The argument <i>node</i> is the node number of the SAP helper router. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxx.xxxx.xxx</i>).</p>
---------------------------	---------------------	--

ipx sap-incremental

To send Service Advertising Protocol (SAP) updates only when a change occurs in the SAP table, use the **ipx sap-incremental** command in interface configuration mode. To send periodic SAP updates, use the **no** form of this command.

ipx sap-incremental eigrp *autonomous-system-number* [**rsup-only**]

no ipx sap-incremental eigrp *autonomous-system-number* [**rsup-only**]

Syntax Description	eigrp <i>autonomous-system-number</i>	IPX Enhanced IGRP autonomous system number. It can be a number from 1 to 65,535.
	rsup-only	(Optional) Indicates that the system uses Enhanced IGRP on this interface to carry reliable SAP update information only. RIP routing updates are used, and Enhanced IGRP routing updates are ignored.

ipx sap-incremental split-horizon

To configure incremental SAP split horizon, use the **ipx sap-incremental split-horizon** command in interface configuration mode. To disable split horizon, use the **no** form of this command.

ipx sap-incremental split-horizon

no ipx sap-incremental split-horizon

Syntax Description This command has no argument or keywords.

ipx sap-max-packetsize

To configure the maximum packet size of Service Advertising Protocol (SAP) updates sent out the interface, use the **ipx sap-max-packetsize** command in interface configuration mode. To restore the default packet size, use the **no** form of this command.

ipx sap-max-packetsize *bytes*

no ipx sap-max-packetsize *bytes*

Syntax Description	<i>bytes</i>	Maximum packet size, in bytes. The default is 480 bytes, which allows for 7 servers (64 bytes each), plus 32 bytes of IPX network and SAP header information.
---------------------------	--------------	---

ipx sap-multiplier

To configure the interval at which a Service Advertising Protocol (SAP) entry for a network or server ages out, use the **ipx sap-multiplier** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

ipx sap-multiplier *multiplier*

no ipx sap-multiplier *multiplier*

Syntax Description	<i>multiplier</i>	Multiplier used to calculate the interval at which to age out SAP routing table entries. This can be any positive number. The value you specify is multiplied by the SAP update interval to determine the aging-out interval. The default is three times the SAP update interval.
---------------------------	-------------------	---

ipx sap-queue-maximum

To set an IPX Service Advertising Protocol (SAP) queue maximum to control how many SAP packets can be waiting to be processed at any given time, use the **ipx sap-queue-maximum** command in global configuration mode. To clear a set SAP queue maximum, use the **no** form of this command.

```
ipx sap-queue-maximum queue-maximum
```

```
no ipx sap-queue-maximum queue-maximum
```

Syntax Description

<i>queue-maximum</i>	Specifies the queue limit as a number from 0 to the maximum unassigned integer.
----------------------	---

ipx sap-update-queue-maximum

To set an IPX Service Advertising Protocol (SAP) queue maximum to control how many incoming SAP update packets can be waiting to be processed at any given time, use the **ipx sap-update-queue-maximum** command in global configuration mode. To clear a set SAP queue maximum, use the **no** form of this command.

```
ipx sap-update-queue-maximum queue-maximum
```

```
no ipx sap-update-queue-maximum queue-maximum
```

Syntax Description

<i>queue-maximum</i>	Specifies the queue limit as a number from 0 to the maximum unassigned integer.
----------------------	---

ipx server-split-horizon-on-server-paths

To control whether Service Information split horizon checking should be based on Router Information Protocol (RIP) paths or Service Advertising Protocol (SAP) paths, use the **ipx server-split-horizon-on-server-paths** command in global configuration mode. To return to the normal mode of following route paths, use the **no** form of this command.

```
ipx server-split-horizon-on-server-paths
```

```
no ipx server-split-horizon-on-server-paths
```

Syntax Description

This command has no arguments or keywords.

ipx split-horizon eigrp

To configure split horizon, use the **ipx split-horizon eigrp** command in interface configuration mode. To disable split horizon, use the **no** form of this command.

ipx split-horizon eigrp *autonomous-system-number*

no ipx split-horizon eigrp *autonomous-system-number*

Syntax Description	<i>autonomous-system-number</i>	Enhanced Interior Gateway Routing Protocol (EIGRP) autonomous system number. It can be a number from 1 to 65,535.
---------------------------	---------------------------------	---

ipx spx-idle-time

To set the amount of time to wait before starting the spoofing of Sequenced Packet Exchange (SPX) keepalive packets following inactive data transfer, use the **ipx spx-idle-time** command in interface configuration mode. To disable the current delay time set by this command, use the **no** form of this command.

ipx spx-idle-time *delay-in-seconds*

no ipx spx-idle-time

Syntax Description	<i>delay-in-seconds</i>	The amount of time, in seconds, to wait before spoofing SPX keepalives after data transfer has stopped.
---------------------------	-------------------------	---

ipx spx-spoof

To configure Cisco IOS software to respond to a client or server's Sequenced Packet Exchange (SPX) keepalive packets on behalf of a remote system so that a dial-on-demand (DDR) link will go idle when data has stopped being transferred, use the **ipx spx-spoof** command in interface configuration mode. To disable spoofing, use the **no** form of this command.

ipx spx-spoof [**session-clear** *session-clear-minutes* | **table-clear** *table-clear-hours*]

no ipx spx-spoof [**session-clear** | **table-clear**]

Syntax Description	session-clear	(Optional) Sets the time to clear inactive entries. Values are 0 through 4,294,967,295.
	table-clear	(Optional) Sets the time to clear the SPX table.
	<i>session-clear-minutes</i>	(Optional) Number of minutes before inactive entries are cleared from the session. Values are 0 through 4,294,967,295.
	<i>table-clear-hours</i>	(Optional) Number of hours before the IPX table is cleared. Values are 0 through 4,294,967,295.

ipx throughput

To configure the throughput, use the **ipx throughput** command in interface configuration mode. To revert to the current bandwidth setting for the interface, use the **no** form of this command.

ipx throughput *bits-per-second*

no ipx throughput *bits-per-second*

Syntax Description	<i>bits-per-second</i>	Throughput, in bits per second.
---------------------------	------------------------	---------------------------------

ipx triggered-rip-delay

To set the interpacket delay for triggered Routing Information Protocol (RIP) updates sent on a single interface, use the **ipx triggered-rip-delay** command in interface configuration mode. To return to the default delay, use the **no** form of this command.

ipx triggered-rip-delay *delay*

no ipx triggered-rip-delay [*delay*]

Syntax Description	<i>delay</i>	Delay, in milliseconds, between packets in a multiple-packet RIP update. The default delay is 55 ms. Novell recommends a delay of 55 ms.
---------------------------	--------------	--

ipx triggered-rip-holddown

To set the amount of time for which an IPX Routing Information Protocol (RIP) process will wait before sending flashes about RIP changes, use the **ipx triggered-rip-holddown** command in interface configuration mode. To remove the RIP hold-down, use the **no** form of this command.

ipx triggered-rip-holddown *milliseconds*

no ipx triggered-rip-holddown *milliseconds*

Syntax Description	<i>milliseconds</i>	Amount of time, in milliseconds, for which the router will wait before sending flashes about RIP changes.
---------------------------	---------------------	---

ipx triggered-sap-delay

To set the interpacket delay for triggered Service Advertising Protocol (SAP) updates sent on a single interface, use the **ipx triggered-sap-delay** command in interface configuration mode. To return to the default delay, use the **no** form of this command.

ipx triggered-sap-delay *delay*

no ipx triggered-sap-delay [*delay*]

Syntax Description

delay

Delay, in milliseconds, between packets in a multiple-packet SAP update. The default delay is 55 ms. Novell recommends a delay of 55 ms.

ipx triggered-sap-holddown

To set the amount of time for which a Service Advertising Protocol (SAP) process will wait before sending flashes about SAP changes, use the **ipx triggered-sap-holddown** command in interface configuration mode. To remove the SAP hold-down, use the **no** form of this command.

ipx triggered-sap-holddown *milliseconds*

no ipx triggered-sap-holddown *milliseconds*

Syntax Description

milliseconds

Amount of time, in milliseconds, for which the router will wait before sending flashes about RIP changes.

ipx type-20-helpered

To forward IPX type 20 propagation packet broadcasts to specific network segments, use the **ipx type-20-helpered** command in global configuration mode. To disable this function, use the **no** form of this command.

ipx type-20-helpered

no ipx type-20-helpered

Syntax Description

This command has no arguments or keywords.

ipx type-20-input-checks

To restrict the acceptance of IPX type 20 propagation packet broadcasts, use the **ipx type-20-input-checks** command in global configuration mode. To remove these restrictions, use the **no** form of this command.

ipx type-20-input-checks

no ipx type-20-input-checks

Syntax Description This command has no arguments or keywords.

ipx type-20-output-checks

To restrict the forwarding of IPX type 20 propagation packet broadcasts, use the **ipx type-20-output-checks** command in global configuration mode. To remove these restrictions, use the **no** form of this command.

ipx type-20-output-checks

no ipx type-20-output-checks

Syntax Description This command has no arguments or keywords.

ipx type-20-propagation

To forward IPX type 20 propagation packet broadcasts to other network segments, use the **ipx type-20-propagation** command in interface configuration mode. To disable both the reception and forwarding of type 20 broadcasts on an interface, use the **no** form of this command.

ipx type-20-propagation

no ipx type-20-propagation

Syntax Description This command has no arguments or keywords.

ipx update interval

To adjust the Routing Information Protocol (RIP) or Service Advertising Protocol (SAP) update interval, use the **ipx update interval** command in interface configuration mode. To restore the default values, use the **no** form of this command.

```
ipx update interval {rip | sap} {value | changes-only}
```

```
no ipx update interval {rip | sap}
```

Syntax Description		
rip		Adjusts the interval at which RIP updates are sent. The minimum interval is 10 seconds.
sap		Adjusts the interval at which SAP updates are sent. The minimum interval is 10 seconds.
<i>value</i>		The interval specified in seconds.
changes-only		Specifies the sending of a SAP update only when the link comes up, when the link is downed administratively, or when service information changes. This parameter is supported for SAP updates only.

ipx update sap-after-rip

To configure the router to send a Service Advertising Protocol (SAP) update immediately following a Routing Information Protocol (RIP) broadcast, use the **ipx update sap-after-rip** command in interface configuration mode. To restore the default value, use the **no** form of this command.

```
ipx update sap-after-rip
```

```
no ipx update sap-after-rip
```

Syntax Description This command has no arguments or keywords.

ipx watchdog

To enable watchdog, use the **ipx watchdog** command in interface configuration mode. To specify filtering, spoofing, or how long spoofing is to be enabled or disabled, use arguments and keywords. To disable filtering or spoofing, use the **no** form of this command.

```
ipx watchdog {filter | spoof} [enable-time-hours disable-time-minutes]
```

```
no ipx watchdog {filter | spoof}
```

Syntax Description		
filter		Discards IPX server watchdog packets when a DDR link is not connected.
spoof		Answers IPX server watchdog packets when a DDR link is not connected.

<i>enable-time-hours</i>	(Optional) Number of consecutive hours spoofing is to stay enabled. Values are 1 through 24.
<i>disable-time-minutes</i>	(Optional) Number of consecutive minutes spoofing is to stay disabled. Values are 18 through 1440.

ipx watchdog-spoof

The `ipx watchdog-spoof` command is replaced by the `ipx watchdog` command. See the description of the `ipx watchdog` command in this chapter for more information.

log-adjacency-changes (IPX)

To generate a log message when an NetWare Link-Services Protocol (NLSP) adjacency changes state (up or down), use the `log-adjacency-changes` command in IPX-router configuration mode. To disable this function, use the `no` form of this command.

`log-adjacency-changes`

`no log-adjacency-changes`

Syntax Description This command has no arguments or keywords.

log-neighbor-changes

To enable the logging of changes in Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor adjacencies, use the `log-neighbor-changes` command in IPX-router configuration mode. To disable this function, use the `no` form of this command.

`log-neighbor-changes`

`no log-neighbor-changes`

Syntax Description This command has no arguments or keywords.

lsp-gen-interval

To set the minimum interval at which link-state packets (LSPs) are generated, use the **lsp-gen-interval** command in router configuration mode. To restore the default interval, use the **no** form of this command.

lsp-gen-interval *seconds*

no lsp-gen-interval *seconds*

Syntax Description	<i>seconds</i>	Minimum interval, in seconds. It can be a number in the range 0 to 120. The default is 5 seconds.
---------------------------	----------------	---

lsp-mtu (IPX)

To set the maximum size of a link-state packet (LSP) generated by Cisco IOS software, use the **lsp-mtu** command in router configuration mode. To restore the default Maximum Transmission Unit (MTU) size, use the **no** form of this command.

lsp-mtu *bytes*

no lsp-mtu *bytes*

Syntax Description	<i>bytes</i>	MTU size, in bytes. It can be a number in the range 512 to 4096. The default is 512 bytes.
---------------------------	--------------	--

lsp-refresh-interval

To set the link-state packet (LSP) refresh interval, use the **lsp-refresh-interval** command in router configuration mode. To restore the default refresh interval, use the **no** form of this command.

lsp-refresh-interval *seconds*

no lsp-refresh-interval *seconds*

Syntax Description	<i>seconds</i>	Refresh interval, in seconds. It can be a value in the range 1 to 50,000 seconds. The default is 7200 seconds (2 hours).
---------------------------	----------------	--

max-lsp-lifetime

To set the maximum time for which link-state packets (LSPs) persist without being refreshed, use the **max-lsp-lifetime** command in router configuration mode. To restore the default time, use the **no** form of this command.

max-lsp-lifetime [**hours**] *value*

no max-lsp-lifetime

Syntax Description	hours	(Optional) If specified, the lifetime of the LSP is set in hours. If not specified, the lifetime is set in seconds.
	<i>value</i>	Lifetime of LSP, in hours or seconds. It can be a number in the range 1 to 32,767. The default is 7500 seconds.

multicast

To configure the router to use multicast addressing, use the **multicast** command in router configuration mode. To configure the router to use broadcast addressing, use the **no** form of this command.

multicast

no multicast

Syntax Description This command has no arguments or keywords.

netbios access-list

To define an IPX NetBIOS FindName access list filter, use the **netbios access-list** command in global configuration mode. To remove a filter, use the **no** form of this command.

netbios access-list host *name* {**deny** | **permit**} *string*

no netbios access-list host *name* {**deny** | **permit**} *string*

netbios access-list bytes *name* {**deny** | **permit**} *offset byte-pattern*

no netbios access-list bytes *name* {**deny** | **permit**} *offset byte-pattern*

Syntax Description	host	Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more netbios access-list host commands.
	<i>name</i>	Name of the access list being defined. The name can be an alphanumeric string.
	deny	Denies access if the conditions are matched.
	permit	Permits access if the conditions are matched.

<i>string</i>	Character string that identifies one or more NetBIOS host names. It can be up to 14 characters long. The argument <i>string</i> can include the following wildcard characters: <ul style="list-style-type: none"> *—Matches one or more characters. You can use this wildcard character only at the end of a string. ?—Matches any single character.
bytes	Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more netbios access-list bytes commands.
<i>offset</i>	Decimal number that indicates the number of bytes into the packet at which the byte comparison should begin. An offset of 0 indicates the beginning of the NetBIOS packet header, which is at the end of the IPX header.
<i>byte-pattern</i>	Hexadecimal pattern that represents the byte pattern to match. It can be up to 16 bytes (32 digits) long and must be an even number of digits. The argument <i>byte-pattern</i> can include the double asterisk (**) wildcard character to match any digits for that byte.

network (IPX Enhanced IGRP)

To enable Enhanced Interior Gateway Routing Protocol (EIGRP), use the **network** (IPX Enhanced IGRP) command in router configuration mode. To disable Enhanced IGRP, use the **no** form of this command.

network {*network-number* | **all**}

no network {*network-number* | **all**}

Syntax Description

<i>network-number</i>	IPX network number.
all	Enables the routing protocol for all IPX networks configured on the router.

permit (IPX extended)

To set conditions for a named IPX extended access list, use the **permit** command in access-list configuration mode. To remove a permit condition from an access list, use the **no** form of this command.

permit *protocol* [*source-network*][[*.source-node*] *source-node-mask*] | [*.source-node* *source-network-mask*.*source-node-mask*] [*source-socket*]
 [*destination-network*][[*.destination-node*] *destination-node-mask*] | [*.destination-node* *destination-network-mask*.*destination-node-mask*] [*destination-socket*] [**log**] [**time-range** *time-range-name*]

no permit *protocol* [*source-network*][[*.source-node*] *source-node-mask*] | [*.source-node* *source-network-mask*.*source-node-mask*] [*source-socket*]
 [*destination-network*][[*.destination-node*] *destination-node-mask*] | [*.destination-node* *destination-network-mask*.*destination-nodemask*] [*destination-socket*] [**log**] [**time-range** *time-range-name*]

Syntax Description

<i>protocol</i>	Name or number of an IPX protocol type. This is sometimes referred to as the packet type. You can also use the keyword any to match all protocol types.
<i>source-network</i>	(Optional) Number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You can also use the keyword any to match all networks. You do not need to specify leading zeros in the network number; for example, for the network number 000000AA, you can enter AA.
<i>.source-node</i>	(Optional) Node on the source-network from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>).
<i>source-node-mask</i>	(Optional) Mask to be applied to the <i>source-node</i> argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>). Place ones in the bit positions you want to mask.
<i>source-network-mask.</i>	(Optional) Mask to be applied to the <i>source-network</i> argument. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask. The mask must immediately be followed by a period, which must in turn immediately be followed by the <i>source-node-mask</i> argument.
<i>source-socket</i>	Socket name or number (hexadecimal) from which the packet is being sent. You can also use the word all to match all sockets.
<i>destination-network</i>	(Optional) Number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You can also use the keyword any to match all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
<i>.destination-node</i>	(Optional) Node on destination-network to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>).
<i>destination-node-mask</i>	(Optional) Mask to be applied to the <i>destination-node</i> argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>). Place ones in the bit positions you want to mask.
<i>destination-network-mask.</i>	(Optional) Mask to be applied to the <i>destination-network</i> argument. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask. The mask must immediately be followed by a period, which must in turn immediately be followed by the <i>destination-node-mask</i> argument.
<i>destination-socket</i>	(Optional) Socket name or number (hexadecimal) to which the packet is being sent.

log	(Optional) Logs IPX access control list violations whenever a packet matches a particular access list entry. The information logged includes source address, destination address, source socket, destination socket, protocol type, and action taken (permit/deny).
time-range <i>time-range-name</i>	(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.

permit (IPX standard)

To set conditions for a named IPX access list, use the **permit** command in access-list configuration mode. To remove a permit condition from an access list, use the **no** form of this command.

```
permit source-network [.source-node [source-node-mask]]
           [destination-network [.destination-node [destination-node-mask]]]
```

```
no permit source-network [.source-node [source-node-mask]]
           [destination-network [.destination-node [destination-node-mask]]]
```

Syntax Description

<i>source-network</i>	Number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
<i>.source-node</i>	(Optional) Node on the <i>source-network</i> from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>).
<i>source-node-mask</i>	(Optional) Mask to be applied to the <i>source-node</i> argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>). Place ones in the bit positions you want to mask.
<i>destination-network</i>	(Optional) Number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
<i>.destination-node</i>	(Optional) Node on the <i>destination-network</i> to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>).
<i>destination-node-mask</i>	(Optional) Mask to be applied to the <i>destination-node</i> argument. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>). Place ones in the bit positions you want to mask.

permit (NLSP)

To allow explicit route redistribution in a named NetWare Link-Services Protocol (NLSP) route aggregation access list, use the **permit** command in access-list configuration mode. To remove a permit condition, use the **no** form of this command.

permit *network network-mask* [**ticks** *ticks*] [**area-count** *area-count*]

no permit *network network-mask* [**ticks** *ticks*] [**area-count** *area-count*]

Syntax Description	
<i>network</i>	Network number to summarize. An IPX network number is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 00000AA, you can enter AA.
<i>network-mask</i>	Specifies the portion of the network address that is common to all addresses in the route summary, expressed as an eight-digit hexadecimal number. The high-order bits specified for the <i>network-mask</i> argument must be contiguous 1s, while the low-order bits must be contiguous zeros (0). An arbitrary mix of 1s and 0s is not permitted.
ticks <i>ticks</i>	(Optional) Metric assigned to the route summary. The default is 1 tick.
area-count <i>area-count</i>	(Optional) Maximum number of NLSP areas to which the route summary can be redistributed. The default is 6 areas.

permit (SAP filtering)

To set conditions for a named IPX Service Advertising Protocol (SAP) filtering access list, use the **permit** command in access-list configuration mode. To remove a permit condition from an access list, use the **no** form of this command.

permit *network[.node]* [*network-mask.node-mask*] [*service-type* [*server-name*]]

no permit *network[.node]* [*network-mask.node-mask*] [*service-type* [*server-name*]]

Syntax Description	
<i>network</i>	Network number. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. A network number of 0 matches the local network. A network number of -1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 00000AA, you can enter AA.
<i>.node</i>	(Optional) Node on the network. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxx.xxxx.xxxx</i>).

<i>network-mask,node-mask</i>	(Optional) Mask to be applied to the <i>network</i> and <i>node</i> arguments. Place ones in the bit positions to be masked.
<i>service-type</i>	(Optional) Service type on which to filter. This is a hexadecimal number. A value of 0 means all services.
<i>server-name</i>	(Optional) Name of the server providing the specified service type. This can be any contiguous string of printable ASCII characters. Use double quotation marks (“ ”) to enclose strings containing embedded spaces. You can use an asterisk (*) at the end of the name as a wildcard to match one or more trailing characters.

prc-interval

To control the hold-down period between partial route calculations, use the **prc-interval** command in router configuration mode. To restore the default interval, use the **no** form of this command.

prc-interval *seconds*

no prc-interval *seconds*

Syntax Description

<i>seconds</i>	Minimum amount of time between partial route calculations, in seconds. It can be a number in the range 1 to 120. The default is 5 seconds.
----------------	--

redistribute (IPX)

To redistribute from one routing domain into another, and vice versa, use one of the following **redistribute** commands in router configuration mode. To disable this feature, use the **no** form of these commands.

For Enhanced Interior Gateway Routing Protocol (EIGRP) or Routing Information Protocol (RIP) environments, use the following command to redistribute from one routing domain into another, and vice versa:

redistribute { **connected** | **eigrp** *autonomous-system-number* | **floating-static** | **nlspl** [*tag*] | **rip** | **static** }

no redistribute { **connected** | **eigrp** *autonomous-system-number* | **floating-static** | **nlspl** [*tag*] | **rip** | **static** }

For NetWare Link-Services Protocol (NLSP) environments, use the following command to redistribute from one routing domain into another, and vice versa:

redistribute { **eigrp** *autonomous-system-number* | **nlspl** [*tag*] | **rip** | **static** }
[**access-list** { *access-list-number* | *name* }]

no redistribute { **eigrp** *autonomous-system-number* | **nlspl** [*tag*] | **rip** | **static** }
[**access-list** { *access-list-number* | *name* }]

Syntax Description	connected	Specifies connected routes.
	eigrp <i>autonomous-system-number</i>	Specifies the Enhanced IGRP protocol and the Enhanced IGRP autonomous system number. It can be a number from 1 to 65,535.
	floating-static	Specifies a floating static route. This is a static route that can be overridden by a dynamically learned route.
	nlsr [<i>tag</i>]	Specifies the NLSP protocol and, optionally, names the NLSP process (<i>tag</i>). The <i>tag</i> can be any combination of printable characters.
	rip	Specifies the RIP protocol. You can configure only one RIP process on the router. Thus, you cannot redistribute RIP into RIP.
	static	Specifies static routes.
	access-list <i>access-list-number</i>	(Optional) Specifies an NLSP route summary access list. The <i>access-list-number</i> is a number from 1200 to 1299.
	access-list <i>name</i>	(Optional) 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.

route-aggregation

To enable the generation of aggregated routes in a NetWare Link-Services Protocol (NLSP) area, use the **route-aggregation** command in router configuration mode. To disable generation, use the **no** form of this command.

route-aggregation

no route-aggregation

Syntax Description This command has no arguments or keywords.

show ipx access-list

To display the contents of all current IPX access lists, use the **show ipx access-list** command in EXEC mode.

show ipx access-list [*access-list-number* | *name*]

Syntax Description	<i>access-list-number</i>	(Optional) Number of the IPX access list to display. This is a number from 800 to 899, 900 to 999, 1000 to 1099, or 1200 to 1299.
	<i>name</i>	(Optional) Name of the IPX access list to display.

show ipx accounting

To display the active or checkpoint accounting database, use the **show ipx accounting** command in EXEC mode.

```
show ipx accounting [checkpoint]
```

Syntax Description	checkpoint	(Optional) Displays entries in the checkpoint database.
--------------------	------------	---

show ipx cache

To display the contents of the IPX fast-switching cache, use the **show ipx cache** command in EXEC mode.

```
show ipx cache
```

Syntax Description	This command has no arguments or keywords.
--------------------	--

show ipx eigrp interfaces

To display information about interfaces configured for Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show ipx eigrp interfaces** command in EXEC mode.

```
show ipx eigrp interfaces [type number] [as-number]
```

Syntax Description	<i>type</i>	(Optional) Interface type.
	<i>number</i>	(Optional) Interface number.
	<i>as-number</i>	(Optional) Autonomous system number.

show ipx eigrp neighbors

To display the neighbors discovered by Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show ipx eigrp neighbors** command in EXEC mode.

```
show ipx eigrp neighbors [servers] [autonomous-system-number | interface] [regex name]
```

Syntax Description	servers	(Optional) Displays the server list advertised by each neighbor. This is displayed only if the ipx sap incremental command is enabled on the interface on which the neighbor resides.
	<i>autonomous-system-number</i>	(Optional) Autonomous system number. It can be a number from 1 to 65,535.

<i>interface</i>	(Optional) Interface type and number.
regex <i>name</i>	(Optional) Displays the IPX servers whose names match the regular expression.

show ipx eigrp topology

To display the Enhanced Interior Gateway Routing Protocol (EIGRP) topology table, use the **show ipx eigrp topology** command in EXEC mode.

```
show ipx eigrp topology [network-number]
```

Syntax Description	<i>network-number</i>	(Optional) IPX network number whose topology table entry is to be displayed.
---------------------------	-----------------------	--

show ipx interface

To display the status of the IPX interfaces configured in Cisco IOS software and the parameters configured on each interface, use the **show ipx interface** command in EXEC mode.

```
show ipx interface [type number]
```

Syntax Description	<i>type</i>	(Optional) Interface type. It can be one of the following types: asynchronous, dialer, Ethernet (IEEE 802.3), FDDI, loopback, null, serial, Token Ring, or tunnel.
	<i>number</i>	(Optional) Interface number.

show ipx nhrp

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

```
show ipx nhrp [dynamic | static] [type number]
```

Syntax Description	dynamic	(Optional) Displays only the dynamic (learned) IPX-to-NBMA address cache entries.
	static	(Optional) Displays only the static IPX-to-NBMA address entries in the cache (configured through the ipx nhrp map command).
	<i>type</i>	(Optional) Interface type for which to display the NHRP cache. Valid options are atm , serial , and tunnel .
	<i>number</i>	(Optional) Interface number for which to display the NHRP cache.

show ipx nhrp traffic

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

```
show ipx nhrp traffic
```

Syntax Description This command has no arguments or keywords.

show ipx nlsr database

To display the entries in the link-state packet (LSP) database, use the **show ipx nlsr database** command in EXEC mode.

```
show ipx nlsr [tag] database [lspid] [detail]
```

Syntax Description	<i>tag</i>	(Optional) Names the NLSP process. The <i>tag</i> can be any combination of printable characters.
	<i>lspid</i>	(Optional) Link-state protocol ID (LSPID). You must specify this in the format <i>xxx.xxx.xxx.yy-zz</i> . The components of this argument have the following meaning: <ul style="list-style-type: none"> <i>xxx.xxx.xxx</i> is the system identifier. <i>yy</i> is the pseudo identifier. <i>zz</i> is the LSP number.
	detail	(Optional) Displays the contents of the LSP database entries. If you omit this keyword, only a summary display is shown.

show ipx nlsr neighbors

To display NetWare Link Services Protocol (NLSP) neighbors and their states, use the **show ipx nlsr neighbors** command in EXEC mode.

```
show ipx nlsr [tag] neighbors [interface] [detail]
```

Syntax Description	<i>tag</i>	(Optional) Names the NLSP process. The value of the <i>tag</i> argument can be any combination of printable characters.
	<i>interface</i>	(Optional) Interface type and number.
	detail	(Optional) Displays detailed information about the neighbor. If you omit this keyword, only a summary display is shown.

show ipx nlspl spf-log

To display a history of the shortest path first (SPF) calculations for NetWare Link Services Protocol (NLSP), use the **show ipx nlspl spf-log** command in EXEC mode.

```
show ipx nlspl [tag] spf-log
```

Syntax Description	tag	(Optional) Names the NLSP process. The tag can be any combination of printable characters.
--------------------	-----	--

show ipx route

To display the contents of the IPX routing table, use the **show ipx route** command in EXEC mode.

```
show ipx route [network] [default] [detailed]
```

Syntax Description	network	(Optional) Number of the network whose routing table entry you want to display. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.
	default	(Optional) Displays the default route. This is equivalent to specifying a value of FFFFFFFE for the argument <i>network</i> .
	detailed	(Optional) Displays detailed route information.

show ipx servers

To list the IPX servers discovered through Service Advertising Protocol (SAP) advertisements, use the **show ipx servers** command in EXEC mode.

```
show ipx servers [detailed] [network network-number] [type service-type-number]
[unsorted | [sorted [name | network | type]]] [regex name]
```

Syntax Description	detailed	(Optional) Displays comprehensive information including path details.
	network	(Optional) Displays IPX SAP services on a specified network.
	network-number	(Optional) IPX network number. 1 to FFFFFFFF.
	type	(Optional) Displays the IPX servers numerically by SAP service type. This is the default.
	service-type-number	(Optional) IPX service type number. 1 to FFFF. When used with the network keyword, displays a list of all SAPs known to a particular network number.
	unsorted	(Optional) Does not sort entries when displaying IPX servers.

sorted	(Optional) Sorts the display of IPX servers according to the keyword that follows.
name	(Optional) Displays the IPX servers alphabetically by server name.
network	(Optional) Displays the IPX servers numerically by network number.
regex <i>name</i>	(Optional) Displays the IPX servers whose names match the regular expression.

show ipx spx-spoof

To display the table of Sequenced Packet Exchange (SPX) connections through interfaces for which SPX spoofing is enabled, use the **show ipx spx-spoof** command in EXEC mode.

show ipx spx-spoof

Syntax Description This command has no arguments or keywords.

show ipx traffic

To display information about the number and type of IPX packets sent and received, use the **show ipx traffic** command in EXEC mode.

show ipx [nlspl] traffic [since {bootup | show}]

Syntax Description	nlspl	(Optional) Displays only NetWare Link Services Protocol (NLSP) traffic counters.
	since bootup	(Optional) Displays traffic statistics since bootup.
	since show	(Optional) Displays traffic statistics since last show command.

show sse summary

To display a summary of Silicon Switch Processor (SSP) statistics, use the **show sse summary** command in EXEC mode.

show sse summary

Syntax Description This command has no arguments or keywords.

spf-interval

To control how often Cisco IOS software performs the Shortest Path First (SPF) calculation, use the **spf-interval** command in router configuration mode. To restore the default interval, use the **no** form of this command.

spf-interval *seconds*

no spf-interval *seconds*

Syntax Description

seconds

Minimum amount of time between SPF calculations, in seconds. It can be a number from 1 to 120. The default is 5 seconds.



**Apollo Domain, Banyan VINES, DECnet,
ISO CLNS, and XNS**



Apollo Domain Commands

This chapter describes the function and syntax of the Apollo Domain commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference*.



Note

The Apollo Domain networking protocol will no longer be offered after Cisco IOS Release 12.2. Apollo Domain commands will not appear in future releases of the Cisco IOS software documentation set.



Note

Not all Cisco access servers support the Apollo Domain protocol. For more information, refer to the release notes for the current Cisco IOS release.

apollo access-group

To apply an access list to an interface, use the **apollo access-group** command in interface configuration mode. To remove the access list, use the **no** form of this command.

```
apollo access-group access-list-name
```

```
no apollo access-group
```

Syntax Description

<i>access-list-name</i>	Name of an access list to apply to the interface.
-------------------------	---

apollo access-list

To define an Apollo Domain access list, use the **apollo access-list** command in global configuration mode. To remove an access list, use the **no** form of this command.

```
apollo access-list access-list-name {deny | permit} [firstnet-] lastnet.host [wildcard-mask]
```

```
no apollo access-list access-list-name
```

Syntax Description	<i>access-list-name</i>	Name of the access list.
	deny	Denies access if the conditions are matched.
	permit	Permits access if the conditions are matched.
	<i>firstnet-</i>	(Optional) Number that specifies the lower limit of a selected Apollo network range, followed by a hyphen.
	<i>lastnet.host</i>	Number that specifies the upper limit of a selected Apollo network range. This is a 32-bit Apollo address, that consists of a network number and a host number, separated by a period. To specify all networks, use a value of -1.
	<i>wildcard-mask</i>	(Optional) Wildcard mask that uses the one bits to ignore the host part of the network address. Host bits corresponding to wildcard mask bits set to zero are used in comparisons.

apollo maximum-paths

To set the maximum number of paths that Cisco IOS software uses when sending packets, use the **apollo maximum-paths** command in global configuration mode. To restore the default value, use the **no** form of this command.

apollo maximum-paths *paths*

no apollo maximum-paths

Syntax Description	<i>paths</i>	Maximum number of equal-cost paths from which the software chooses. The argument <i>paths</i> can be a value from 1 to 512.
---------------------------	--------------	---

apollo network

To enable Apollo Domain routing on a particular interface, use the **apollo network** command in interface configuration mode. To disable Apollo Domain routing on an interface, use the **no** form of this command.

apollo network *number*

no apollo network *number*

Syntax Description	<i>number</i>	Network number. This is an 8-digit hexadecimal number that consists of the network address followed by the host address.
---------------------------	---------------	--

apollo route

To add a static route to the Apollo Domain routing table, use the **apollo route** command in global configuration mode. To remove a route from the routing table, use the **no** form of this command.

apollo route *destination-network network.host*

no apollo route *destination-network network.host*

Syntax Description		
	<i>destination-network</i>	Network to which you want to establish a static route. This is a 12-bit hexadecimal number. You can omit leading zeros.
	<i>network.host</i>	Network address of the router to which to forward packets destined for <i>destination-network</i> . The argument <i>network</i> is a 12-bit hexadecimal number. You can omit leading zeros. The argument <i>host</i> is the host number of the target router. This is a 20-bit hexadecimal value.

apollo routing

To enable Apollo Domain routing, use the **apollo routing** command in global configuration mode. To disable Apollo Domain routing, use the **no** form of this command.

apollo routing *host*

no apollo routing *host*

Syntax Description		
	<i>host</i>	Host number of the router. This is a 5-digit hexadecimal host address that is unique across the Apollo Domain internetwork.

apollo update-time

To set the interval between Apollo Domain routing updates, use the **apollo update-time** command in interface configuration mode. To restore the default value, use the **no** form of this command.

apollo update-time *interval*

no apollo update-time

Syntax Description		
	<i>interval</i>	Interval, in seconds, at which Apollo Domain routing updates are sent. The minimum interval is 10 seconds, and the maximum is 2,493,644 seconds. The default is 30 seconds.

show apollo arp

To list the entries in the Apollo Domain Address Resolution Protocol (ARP) table, use the **show apollo arp** command in EXEC mode.

```
show apollo arp
```

Syntax Description This command has no arguments or keywords.

show apollo interface

To display the status of the Apollo Domain interfaces configured in the router and the parameters configured on each interface, use the **show apollo interface** command in EXEC mode.

```
show apollo interface [type number]
```

Syntax Description	<i>type</i>	(Optional) Interface type. It can be one of the following types: asynchronous, dialer, Ethernet (IEEE 802.3), loopback, null, serial, or tunnel.
	<i>number</i>	(Optional) Interface number.

show apollo route

To display the contents of the Apollo Domain routing table, use the **show apollo route** command in EXEC mode.

```
show apollo route [network]
```

Syntax Description	<i>network</i>	(Optional) Number of the network that the route is to. This is a 12-bit hexadecimal number.
---------------------------	----------------	---

show apollo traffic

To display information about the number and type of Apollo Domain packets transmitted and received by Cisco IOS software, use the **show apollo traffic** command in EXEC mode.

```
show apollo traffic
```

Syntax Description This command has no arguments or keywords.



Banyan VINES Commands

This chapter describes the function and syntax of the Banyan Virtual Network System (VINES) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference*.



Note

Not all Cisco access servers support Banyan VINES. For more information, refer to the release notes for the release that you are running.

clear vines cache

To delete entries from the VINES fast-switching cache, use the **clear vines cache** command in EXEC mode.

```
clear vines cache [interface interface | neighbor address | server network | counters]
```

Syntax Description

interface <i>interface</i>	(Optional) Deletes from the fast-switching cache table any entry that has one or more paths that go through the specified interface.
neighbor <i>address</i>	(Optional) Deletes from the fast-switching cache table any entry that has one or more paths via the specified neighbor router.
server <i>network</i>	(Optional) Deletes from the fast-switching cache table any entry whose network number part of the destination address matches the specified network address. The argument <i>network</i> can be either a 4-byte hexadecimal number or a 4-byte decimal number (if you have issued a vines decimal command).
counters	(Optional) Deletes the fast-switching cache and counters.

clear vines ipc

To delete VINES Interprocess Communications Protocol (IPC) connection blocks, use the **clear vines ipc** command in EXEC mode.

```
clear vines ipc number
```

Syntax Description

<i>number</i>	Hexadecimal number of the IPC connection to delete.
---------------	---

clear vines neighbor

To delete entries from the neighbor table, use the **clear vines neighbor** command in EXEC mode.

```
clear vines neighbor {address | *}
```

Syntax Description

<i>address</i>	Address of the neighbor entry whose entry should be deleted from the neighbor table. The argument is a 6-byte hexadecimal number in the format <i>network:host</i> where <i>network</i> is 4 bytes and <i>host</i> is 2 bytes.
*	Deletes all entries from the neighbor path table except the entry for the local router.

clear vines route

To delete network addresses from the routing table, use the **clear vines route** command in EXEC mode.

```
clear vines route {network | *}
```

Syntax Description

<i>network</i>	Network number of the entry to delete from the routing table. The argument <i>network</i> can be a 4-byte hexadecimal number, a 4-byte decimal number (if you have issued a vines decimal command), or a host name (if you have issued a vines enhancements command).
*	Deletes all entries from the routing table.

clear vines traffic

To clear all VINES-related statistics that are displayed by the **show vines traffic** command, use the **clear vines traffic** command in EXEC mode.

```
clear vines traffic
```

Syntax Description

This command has no arguments or keywords.

show vines access

To display the VINES access lists currently defined, use the **show vines access** command in EXEC mode.

```
show vines access [access-list-number]
```

Syntax Description	<i>access-list-number</i>	(Optional) Number of the access list to display.
--------------------	---------------------------	--

show vines cache

To display the contents of the VINES fast-switching cache, use the **show vines cache** command in EXEC mode.

```
show vines cache [address | interface type number | neighbor address | server network]
```

Syntax Description	<i>address</i>	(Optional) Displays the entry in the fast-switching cache for the specified station.
	interface <i>type number</i>	(Optional) Displays all neighbors in the fast-switching cache that are accessible via the specified interface type and number.
	neighbor <i>address</i>	(Optional) Displays all routes in the VINES fast-switching cache that have the specified neighbor as their first hop. The argument <i>address</i> is a 6-byte hexadecimal number in the format <i>network:host</i> , where <i>network</i> is 4 bytes and <i>host</i> is 2 bytes, a 4-byte decimal number in the same format (if you have issued a vines decimal command), or a host name (if you have issued a vines enhancements command).
	server <i>network</i>	(Optional) Displays all entries in the VINES fast-switching cache that are in the specified logical network. The argument <i>network</i> can be either a 4-byte hexadecimal number or a 4-byte decimal number (if you have issued a vines decimal command).

show vines host

To display the entries in the VINES host-name table, use the **show vines host** command in EXEC mode.

```
show vines host [name]
```

Syntax Description	<i>name</i>	(Optional) Displays the entry in the VINES name table that has the specified name.
--------------------	-------------	--

show vines interface

To display status of the VINES interfaces configured in Cisco IOS software and the parameters configured on each interface, use the **show vines interface** command in EXEC mode.

```
show vines interface [type number]
```

Syntax Description

<i>type</i>	(Optional) Interface type.
<i>number</i>	(Optional) Interface number.

show vines ipc

To display information about any currently active interprocess communication (IPC) connections, use the **show vines ipc** command in EXEC mode.

```
show vines ipc
```

Syntax Description

This command has no arguments or keywords.

show vines neighbor

To display the entries in the VINES neighbor table, use the **show vines neighbor** command in EXEC mode.

```
show vines neighbor [address | interface type number | server number]
```

Syntax Description

<i>address</i>	(Optional) Displays the entry for the specified neighbor.
interface <i>type number</i>	(Optional) Displays all neighbor paths in the neighbor table that use the specified interface.
server <i>number</i>	(Optional) Displays all entries in the neighbor table that have the specified network number.

show vines route

To display the contents of the VINES routing table, use the **show vines route** command in EXEC mode.

```
show vines route [number | neighbor address | metric]
```

Syntax Description

<i>number</i>	(Optional) Displays the routing table entry for the specified network.
neighbor <i>address</i>	(Optional) Displays all routes in the VINES routing table that have the specified neighbor as their first hop.
metric	(Optional) Display routes by metric.

show vines service

To display information about the application layer support, use the **show vines service** command in EXEC mode.

```
show vines service [fs | nsm | ss | vs]
```

Syntax Description		
	fs	(Optional) Displays file service information.
	nsm	(Optional) Displays network and system management service information.
	ss	(Optional) Displays server service information.
	vs	(Optional) Displays security service information.

show vines traffic

To display the statistics maintained about VINES protocol traffic, use the **show vines traffic** command in EXEC mode.

```
show vines traffic [type number]
```

Syntax Description		
	<i>type</i>	(Optional) Interface type.
	<i>number</i>	(Optional) Interface number.

trace (VINES)

To determine the path that a packet takes when traversing a VINES network, use the **trace** command in EXEC mode.

```
trace [vines | oldvines] [address]
```

Syntax Description		
	vines	(Optional) Specifies the VINES protocol. This trace is compatible with the Banyan VINES traceroute function.
	oldvines	(Optional) Specifies the VINES protocol. This trace is compatible with our trace function prior to Cisco IOS Release 10.2.
	<i>address</i>	(Optional) Address of a node. This is a 6-byte hexadecimal number in the format <i>network:host</i> , where <i>network</i> is 4 bytes and <i>host</i> is 2 bytes.

vines access-group

To apply an access list to an interface, use the **vines access-group** command in interface configuration mode. To remove the access list, use the **no** form of this command.

vines access-group *access-list-number*

no vines access-group *access-list-number*

Syntax Description	<i>access-list-number</i>	Number of the access list. All outgoing packets defined with either standard or extended access lists and forwarded through the interface are filtered by the entries in this access list. For standard access lists, <i>access-list-number</i> is a decimal number from 1 to 100. For extended access lists, <i>access-list-number</i> is a decimal number from 101 to 200.
---------------------------	---------------------------	--

vines access-list (extended)

To create an extended VINES access list, use this version of the **vines access-list** command in global configuration mode. To remove an extended access list, use the **no** form of this command.

vines access-list *access-list-number* {**deny** | **permit**} *protocol source-address source-mask*
 [*source-port source-port-mask*] *destination-address destination-mask* [*destination-port destination-port-mask*]

no vines access-list *access-list-number*

Syntax Description	<i>access-list-number</i>	Number of the access list. This is a decimal number from 101 to 200.
	deny	Denies access if the conditions are matched.
	permit	Allows access if the conditions are matched.
	<i>protocol</i>	VINES protocol ID number or name. The number can be a value from 1 to 255, or one of the following protocol keywords: <ul style="list-style-type: none"> • arp—Address Resolution Protocol (ARP) • icp—Internet Control Protocol (ICP) • ip—VINES Internet Protocol • ipc—Interprocess Communications (IPC) • rtp—Routing Table Protocol (RTP) • spp—Sequence Packet Protocol (SPP)
	<i>source-address</i>	Address of the network from which the packet is being sent. This is a 6-byte hexadecimal number in the format <i>network:host</i> , where <i>network</i> is 4 bytes, and <i>host</i> is 2 bytes.
	<i>source-mask</i>	Mask to be applied to <i>source-address</i> . This is a 6-byte hexadecimal value. Place ones in the bit positions you want to mask. These bits correspond to the bits in the address that should be ignored.

<i>source-port</i>	(Optional) Number of the local port from which the packet is being sent. This argument is required when the protocol specified is IPC or SPP, and is not accepted when any other protocol is specified. It can be a number from 0x0000 to 0xFFFF. Well-known local port numbers have values from 0x0001 to 0x01FF. Transient local port numbers have values from 0x0200 to 0xFFFE.
<i>source-port-mask</i>	(Optional) Mask to be applied to the <i>source-port</i> argument. This argument is required when the protocol specified is IPC or SPP, and is not accepted when any other protocol is specified. It can be a number from 0x0000 to 0xFFFF. These bits correspond to the bits in the port that should be ignored.
<i>destination-address</i>	VINES address of the network to which the packet is being sent. This is a 6-byte hexadecimal number in the format <i>network:host</i> , where <i>network</i> is 4 bytes and <i>host</i> is 2 bytes.
<i>destination-mask</i>	Mask to be applied to <i>destination-address</i> . This is a 6-byte hexadecimal value. Place ones in the bit positions you want to mask. These bits correspond to the bits in the address that should be ignored.
<i>destination-port</i>	(Optional) Number of the local port to which the packet is being sent. This argument is required when the protocol specified is IPC or SPP, and is not accepted when any other protocol is specified. It can be a number from 0x0000 to 0xFFFF. Well-known local port numbers have values from 0x0001 to 0x01FF. Transient local port numbers have values from 0x0200 to 0xFFFE.
<i>destination-port-mask</i>	(Optional) Mask to be applied to <i>destination-port</i> . This argument is required when the protocol specified is IPC or SPP, and is not accepted when any other protocol is specified. It can be a number from 0x0000 to 0xFFFF. These bits correspond to the bits in the port that should be ignored.

vines access-list (simple)

To create a simple VINES access list, use this version of the **vines access-list** command in global configuration mode. To remove a simple access list, use the **no** form of this command.

```
vines access-list access-list-number { deny | permit } source-address source-mask
```

```
no vines access-list access-list-number
```

Syntax Description

<i>access-list-number</i>	Access list number. It is a number from 201 to 300.
deny	Denies access if the conditions are matched.
permit	Allows access if the conditions are matched.
<i>source-address</i>	Address of the network from which the packet is being sent. This is a 6-byte hexadecimal number in the format <i>network:host</i> , where <i>network</i> is 4 bytes and <i>host</i> is 2 bytes.
<i>source-mask</i>	Mask to be applied to <i>source-address</i> . This is a 6-byte hexadecimal value. Place ones in the bit positions you want to mask. These bits correspond to the bits in the address that should be ignored.

vines access-list (standard)

To specify a standard VINES access list, use this version of the **vines access-list** command in global configuration mode. To remove the access list, use the **no** form of this command.

```
vines access-list access-list-number {deny | permit} protocol source-address source-mask
[source-port] destination-address destination-mask [destination-port]
```

```
no vines access-list access-list-number
```

Syntax Description

<i>access-list-number</i>	Number of the access list. This is a decimal number from 1 to 100.
deny	Denies access if the conditions are matched.
permit	Allows access if the conditions are matched.
<i>protocol</i>	VINES protocol ID number or name. It can be a value from 1 to 255 or one of the following protocol keywords: <ul style="list-style-type: none"> • arp—Address Resolution Protocol (ARP) • icp—Internet Control Protocol (ICP) • ip—VINES Internet Protocol • ipc—Interprocess Communications (IPC) • rtp—Routing Table Protocol (RTP) • spp—Sequence Packet Protocol (SPP)
<i>source-address</i>	Address of the network from which the packet is being sent. This is a 6-byte hexadecimal number in the format <i>network:host</i> , where <i>network</i> is 4 bytes and <i>host</i> is 2 bytes.
<i>source-mask</i>	Mask to be applied to <i>source-address</i> . This is a 6-byte hexadecimal value. Place ones in the bit positions you want to mask. These bits correspond to the bit in the address that should be ignored.
<i>source-port</i>	(Optional) Number of the local port from which the packet is being sent. This argument is required when the protocol specified is IPC or SPP, and is not accepted when any other protocol is specified. It can be a number from 0x0000 to 0xFFFF. Well-known local port numbers have values from 0x0001 to 0x01FF. Transient local port numbers have values from 0x0200 to 0xFFFE.
<i>destination-address</i>	Address of the network to which the packet is being sent. This is a 6-byte hexadecimal number in the format <i>network:host</i> , where <i>network</i> is 4 bytes and <i>host</i> is 2 bytes.
<i>destination-mask</i>	Mask to be applied to <i>destination-address</i> . This is a 6-byte hexadecimal value. Place ones in the bit positions you want to mask. These bits correspond to the bits in the address that should be ignored.
<i>destination-port</i>	(Optional) Number of the local port to which the packet is being sent. This argument is required when the protocol specified is IPC or SPP, and is not accepted when any other protocol is specified. It can be a number from 0x0000 to 0xFFFF. Well-known local port numbers have values from 0x0001 to 0x01FF. Transient local port numbers have values from 0x0200 to 0xFFFE.

vines arp-enable

To enable the processing of Address Resolution Protocol (ARP) packets, use the **vines arp-enable** command in interface configuration mode. To disable the processing of ARP packets, use the **no** form of this command.

vines arp-enable [dynamic]

no vines arp-enable [dynamic]

Syntax Description	dynamic	(Optional) Responds to ARP and SARP requests on this interface only if there are no other VINES servers present.
---------------------------	----------------	--

vines decimal

To display VINES addresses in decimal notation, use the **vines decimal** command in global configuration mode. To return to displaying the addresses in hexadecimal, use the **no** form of this command.

vines decimal

no vines decimal

Syntax Description	This command has no arguments or keywords.
---------------------------	--

vines encapsulation

To set the MAC-level encapsulation used for VINES broadcast packets, use the **vines encapsulation** command in interface configuration mode. To disable encapsulation, use the **no** form of this command.

vines encapsulation [arpa | snap | vines-tr]

no vines encapsulation

Syntax Description	arpa	(Optional) Advanced Research Projects Agency (ARPA) encapsulation. This is the default encapsulation for Ethernet interfaces.
	snap	(Optional) Subnetwork Access Protocol (SNAP) encapsulation. This encapsulation uses an IEEE 802.2 SNAP header. It is the default encapsulation for all media except Ethernet and Token Ring.
	vines-tr	(Optional) Our VINES Token Ring encapsulation. This is the default encapsulation for Token Ring interfaces.

vines enhancements

To enable split-horizon for routing updates and to generate flash updates, use the **vines enhancements** command in global configuration mode. To turn VINES enhancement off, use the **no** form of this command.

vines enhancements

no vines enhancements

Syntax Description This command has no arguments or keywords.

vines host

To associate a host name with a VINES address, use the **vines host** command in global configuration mode. To delete the association, use the **no** form of this command.

vines host *name address*

no vines host *name*

Syntax Description	<i>name</i>	VINES host name. It can be any length and sequence of characters separated by white space.
	<i>address</i>	Number of a VINES network. You enter it in the current VINES radix, in the format <i>network:host</i> , where <i>network</i> is 4 bytes and <i>host</i> is 2 bytes.

vines input-network-filter

To filter the information contained in routing messages received from other stations, use the **vines input-network-filter** command in interface configuration mode. To disable this filtering, use the **no** form of this command.

vines input-network-filter *access-list-number*

no vines input-network-filter

Syntax Description	<i>access-list-number</i>	Number of the access list. It is a decimal number from 201 to 300.
---------------------------	---------------------------	--

vines input-router-filter

To filter received routing messages based upon the address of the sending station, use the **vines input-router-filter** command in interface configuration mode. To disable this filtering, use the **no** form of this command.

vines input-router-filter *access-list-number*

no vines input-router-filter

Syntax Description	<i>access-list-number</i>	Number of the access list. It is a decimal number from 201 to 300.
---------------------------	---------------------------	--

vines metric

To enable VINES routing on an interface, use the **vines metric** command in interface configuration mode. To disable VINES routing, use the **no** form of this command.

vines metric [*whole* [*fractional*]]

no vines metric

Syntax Description	<i>whole</i>	(Optional) Integer cost value associated with the interface. It is optional for all interface types. If you omit <i>whole</i> , the Cisco IOS software automatically chooses a reasonable value.
	<i>fractional</i>	(Optional) Fractional cost value associated with the interface expressed in 10,000ths. It is optional for all interface types, but may only be present if a whole number portion is specified. This number is rounded to the nearest 1/16. If you omit both whole and fractional numbers, the software automatically chooses a reasonable value.

vines neighbor

To specify a static path to a neighbor station, use the **vines neighbor** command in interface configuration mode. To remove a static path from the neighbor table, use the **no** form of this command.

vines neighbor *address mac-address encapsulation* [*whole* [*fractional*]]

no vines neighbor *address mac-address*

Syntax Description	<i>address</i>	VINES IP address of the station to which to add or remove a static path.
	<i>mac-address</i>	MAC-level address used to reach the neighbor station.

<i>encapsulation</i>	Encapsulation type to use on the media. It can be one of the following values: <ul style="list-style-type: none"> • arpa—Uses ARPA encapsulation. This is recommended for Ethernet interfaces. • snap—Uses an IEEE 802.2 SNAP header. This is recommended for FDDI interfaces. • vines-tr—Uses our VINES Token Ring encapsulation. This is recommended for Token Ring interfaces.
<i>whole</i>	(Optional) Delay metric to use on the neighbor. If you omit this argument, the metric used is that specified with the vines metric command for the selected interface.
<i>fractional</i>	(Optional) Fractional metric value associated with this neighbor. This number is rounded to the nearest 1/16. If you omit both whole and fractional numbers, the interface metric is used.

vines output-network-filter

To filter the information contained in routing updates transmitted to other stations, use the **vines output-network-filter** command in interface configuration mode. To disable this filtering, use the **no** form of this command.

vines output-network-filter *access-list-number*

no vines output-network-filter

Syntax Description	<i>access-list-number</i>	Number of the access list. It is a decimal number from 201 to 300.
---------------------------	---------------------------	--

vines propagate

To modify how Cisco IOS software forwards a broadcast packet, use the **vines propagate** command in interface configuration mode. To return to the default forwarding scheme, use the **no** form of this command.

vines propagate [**dynamic**]

no vines propagate [**dynamic**]

Syntax Description	dynamic	(Optional) Propagates broadcasts on this interface only if there are no servers on any local network.
---------------------------	----------------	---

vines redirect

To determine how frequently Cisco IOS software sends an Routing Table Protocol (RTP) redirect message on an interface, use the **vines redirect** command in interface configuration mode. To restore the default, use the **no** form of this command.

vines redirect [*seconds*]

no vines redirect

Syntax Description	<i>seconds</i>	(Optional) Interval, in seconds, that the software waits after sending a redirect message on an interface before it sends another redirect message on that same interface. If you specify a value of 0, the software never sends redirect messages on that interface.
---------------------------	----------------	---

vines route

To specify a static route to a server, use the **vines route** command in global configuration mode. To remove a static route from the routing table, use the **no** form of this command.

vines route *number address* [*whole* [*fractional*]]

no vines route *number address* [*whole* [*fractional*]]

Syntax Description	<i>number</i>	Number of the server to which to add or remove the static route.
	<i>address</i>	VINES IP address of the neighbor station to use to reach the server.
	<i>whole</i>	(Optional) Metric value assigned to this route.
	<i>fractional</i>	(Optional) Fractional cost value associated with this route.

vines route-cache

To enable fast switching, use the **vines route-cache** command in interface configuration mode. To disable fast switching, use the **no** form of this command.

vines route-cache

no vines route-cache

Syntax Description	This command has no arguments or keywords.
---------------------------	--

vines routing

To enable VINES routing, use the **vines routing** command in global configuration mode. To disable VINES routing, use the **no** form of this command.

vines routing [*address* | **recompute**]

no vines routing

Syntax Description	<i>address</i>	(Optional) Network address of the router. You should specify an address on a router that does not have any Ethernet or FDDI interfaces. You can also specify an address in the unlikely event that two routers map themselves to the same address.
	recompute	(Optional) Dynamically redetermines the network address of the router.

vines serverless

To configure a Banyan VINES network that does not have a server, use the **vines serverless** command in interface configuration mode. To disable this feature, use the **no** form of this command.

vines serverless [**dynamic** | **broadcast**]

no vines serverless [**dynamic** | **broadcast**]

Syntax Description	dynamic	(Optional) Forwards broadcasts toward one server only if there are no servers present on this interface.
	broadcast	(Optional) Always floods broadcasts out all other router interfaces to reach all servers.

vines single-route

To maintain only one route per server, use the **vines single-route** command in global configuration mode. To allow multiple routes per server, use the **no** form of this command.

vines single-route

no vines single route

Syntax Description	This command has no arguments or keywords.
---------------------------	--

vines split-horizon

To use split horizon when sending routing updates, use the **vines split-horizon** command in interface configuration mode. To disable split horizon, use the **no** form of this command.

vines split-horizon

no vines split-horizon

Syntax Description This command has no arguments or keywords.

vines srtp-enabled

To enable Sequenced Routing Update Protocol (SRTP), use the **vines srtp-enabled** command in global configuration mode. To disable SRTP, use the **no** form of this command.

vines srtp-enabled

no vines srtp-enabled

Syntax Description This command has no arguments or keywords.

vines time access-group

To control the servers from which the router will accept VINES network time, use the **vines time access-group** command in global configuration mode. To accept VINES network time messages from any server, use the **no** form of this command.

vines time access-group *access-list-number*

no vines time access-group

Syntax Description *access-list-number* Number of the access list. It is a decimal number from 201 to 300.

vines time destination

To control the servers to which Cisco IOS software sends VINES network time, use the **vines time destination** command in global configuration mode. To send VINES network time messages to all servers, use the **no** form of this command.

vines time destination *address*

no vines time destination

Syntax Description

<i>address</i>	Destination VINES address for the network time messages.
----------------	--

vines time participate

To enable participation in synchronizing time across a VINES network, use the **vines time participate** command in global configuration mode. To disable this participation, use the **no** form of this command.

vines time participate

no vines time participate

Syntax Description

This command has no arguments or keywords.

vines time services

To enable Cisco IOS software to provide time services for VINES clients and to enable participation in the synchronization of time across a VINES network, use the **vines time services** command in global configuration mode. To disable participation in time synchronization and services, use the **no** form of this command.

vines time services

no vines time services

Syntax Description

This command has no arguments or keywords.

vines time set-system

To set the internal time based upon the received VINES network time, use the **vines time set-system** command in global configuration mode. To uncouple the time from VINES network time, use the **no** form of this command.

vines time set-system

no vines time set-system

Syntax Description This command has no arguments or keywords.

vines time use-system

To set VINES network time based on the internal time, use the **vines time use-system** command in global configuration mode. To uncouple VINES network time from the time, use the **no** form of this command.

vines time use-system

no vines time use-system

Syntax Description This command has no arguments or keywords.

vines update deltas

To modify the manner in which routing updates are sent, use the **vines update deltas** command in interface configuration mode. To return to the default method, use the **no** form of this command.

vines update deltas

no vines update deltas

Syntax Description This command has no arguments or keywords.

vines update interval

To modify the frequency at which routing updates are sent, use the **vines update interval** command in interface configuration mode. To return to the default frequency, use the **no** form of this command.

vines update interval [*seconds*]

no vines update interval [*seconds*]

Syntax Description

seconds

(Optional) Interval, in seconds, between the sending of periodic VINES routing updates. This can be a number in the range 0 to 2³² and is rounded up to the nearest 5 seconds. The default value is 90 seconds. If you omit *seconds* or specify a value of 0, the default value of 90 seconds is used.



DECnet Commands

This chapter describes the function and syntax of the DECnet commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference*.



Note

Not all Cisco access servers support DECnet. For more information, refer to the release notes for the current Cisco IOS release.

access-list (DECnet extended)

To create an extended access list, use the **access-list** command in global configuration mode. To delete the entire access list, use the **no** form of this command.

```
access-list access-list-number {permit | deny} source source-mask [destination destination-mask]
```

```
no access-list
```

Syntax Description

<i>access-list-number</i>	Integer you choose between 300 and 399 that uniquely identifies the access list.
permit	Permits access when there is an address match.
deny	Denies access when there is an address match.
<i>source</i>	Source address. DECnet addresses are written in the form <i>area.node</i> . For example, 50.4 is node 4 in area 50. All addresses are in decimal.
<i>source-mask</i>	Mask to be applied to the address of the source node. All masks are in decimal.
<i>destination</i>	(Optional) Destination node's DECnet address in decimal format. DECnet addresses are written in the form <i>area.node</i> . For example, 50.4 is node 4 in area 50.
<i>destination-mask</i>	(Optional) Destination mask. DECnet addresses are written in the form <i>area.node</i> . For example, 50.4 is node 4 in area 50. All masks are in decimal.

access-list (connect initiate)

To create an access list that filters *connect initiate* packets, use this version of the **access-list** command in global configuration mode. To disable the access list, use the **no** form of this command.

```
access-list access-list-number {permit | deny} source source-mask [destination destination-mask]
  {eq | neq} [source-object] [destination-object] [identification] any
```

```
no access-list
```

The optional argument *source-object* consists of the following string:

```
src [{eq | neq | gt | lt} object-number] [exp regular-expression] [uic [group, user]]
```

The optional argument *destination-object* consists of the following string:

```
dst [{eq | neq | gt | lt} object-number] [exp regular-expression] [uic [group, user]]
```

The optional argument *identification* consists of the following string:

```
[id regular-expression] [password regular-expression] [account regular-expression]
```

Syntax Description

<i>access-list-number</i>	Integer you choose between 300 and 399 that uniquely identifies the access list.
permit	Permits access when there is an address match.
deny	Denies access when there is an address match.
<i>source</i>	Source address. DECnet addresses are written in the form <i>area.node</i> . For example, 50.4 is node 4 in area 50. All addresses are in decimal.
<i>source-mask</i>	Mask to be applied to the address of the source node. All masks are in decimal.
<i>destination</i>	(Optional) Destination node's DECnet address in decimal format. DECnet addresses are written in the form <i>area.node</i> . For example, 50.4 is node 4 in area 50. All addresses are in decimal.
<i>destination-mask</i>	(Optional) Destination mask. DECnet addresses are written in the form <i>area.node</i> . For example, 50.4 is node 4 in area 50. All masks are in decimal.
eq neq	Use either of these keywords: <ul style="list-style-type: none"> eq—Item matches the packet if <i>all</i> the specified parts of <i>source-object</i>, <i>destination-object</i>, and <i>identification</i> match data in the packet. neq—Item matches the packet if <i>any</i> of the specified parts do <i>not</i> match the corresponding entry in the packet.

<i>source-object</i>	<p>(Optional) Contains the mandatory keyword src and one of the following optional keywords:</p> <ul style="list-style-type: none"> • eq neq lt gt—Equal to, not equal to, less than, or greater than. These keywords must be followed by the argument <i>object-number</i>, a numeric DECnet object number. • exp—Stands for expression; followed by a <i>regular-expression</i> that matches a string. Refer to the “Regular Expressions” appendix in the <i>Cisco IOS Dial Technologies Command Reference</i> for a description of regular expressions. • uic—Stands for user identification code; followed by a numeric user ID (UID) expression. The argument [<i>group, user</i>] is a numeric UID expression. In this case, the bracket symbols are literal; they must be entered. The <i>group</i> and <i>user</i> parts can either be specified in decimal, in octal by prefixing the number with a 0, or in hex by prefixing the number with 0x. The uic expression displays as an octal number.
<i>destination-object</i>	<p>(Optional) Contains the mandatory keyword dst and one of the following optional keywords:</p> <ul style="list-style-type: none"> • eq neq lt gt—Equal to, not equal to, less than, or greater than. These keywords must be followed by the argument <i>object-number</i>, a numeric DECnet object number. • exp—Stands for expression; followed by a <i>regular-expression</i> that matches a string. Refer to the “Regular Expressions” appendix in the <i>Cisco IOS Dial Technologies Command Reference</i> for a description of regular expressions. • uic—Stands for user identification code; followed by a numeric user ID (UID) expression. In this case, the bracket symbols are literal; they must be entered. The <i>group</i> and <i>user</i> parts can either be specified in decimal, in octal by prefixing the number with a 0, or in hex by prefixing the number with 0x. The uic expression displays as an octal number.
<i>identification</i>	<p>(Optional) Uses any of the following three keywords:</p> <ul style="list-style-type: none"> • id—Regular expression; refers to user ID. • password—Regular expression; the password to the account. • account—Regular expression; the account string.
any	<p>(Optional) Item matches if <i>any</i> of the specified parts <i>do</i> match the corresponding entries for <i>source-object</i>, <i>destination-object</i>, or <i>identification</i>.</p>

access-list (DECnet standard)

To create a standard access list, use the standard version of the **access-list** command in global configuration mode. To delete the entire access list, use the **no** form of this command.

```
access-list access-list-number { permit | deny } source source-mask
```

```
no access-list
```

Syntax Description	<i>access-list-number</i>	Integer you choose between 300 and 399 that uniquely identifies the access list.
	permit	Permits access when there is an address match.
	deny	Denies access when there is an address match.
	<i>source</i>	Source address. DECnet addresses are written in the form <i>area.node</i> . For example, 50.4 is node 4 in area 50. All addresses are in decimal.
	<i>source-mask</i>	Mask to be applied to the address of the source node. Bits are set wherever the corresponding bits in the address should be ignored. All masks are in decimal.

clear decnet accounting

To delete all entries in the accounting database when DECnet accounting is enabled, use the **clear decnet accounting** command in EXEC mode.

```
clear decnet accounting [checkpoint]
```

Syntax Description	checkpoint	(Optional) Clears the checkpoint database.
---------------------------	-------------------	--

clear decnet counters

To clear DECnet counters that are shown in the output of the **show decnet traffic** EXEC command, use the **clear decnet counters** command in EXEC mode.

```
clear decnet counters
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--

decnet access-group

To create a DECnet access group, use the **decnet access-group** command in interface configuration mode. To delete a DECnet access-group, use the **no** form of this command.

```
decnet access-group access-list-number
```

```
no decnet access-group
```

Syntax Description	<i>access-list-number</i>	Either a standard or an extended DECnet access list. A standard DECnet access list applies to source addresses. The value (or values in the case of extended lists) can be in the range 300 to 399.
---------------------------	---------------------------	---

decnet accounting

To enable DECnet accounting, use the **decnet accounting** command in interface configuration mode. To disable DECnet accounting, use the **no** form of this command.

decnet accounting

no decnet accounting

Syntax Description This command has no arguments or keywords.

decnet accounting list

To specify the source and destination address pairs for which DECnet accounting information is kept, use the **decnet accounting list** command in global configuration mode. DECnet accounting tracks all traffic that traverses the router between the source and destination address pairs specified with this command. To remove the accounting filter, use the **no** form of this command.

decnet accounting list *src-dec-address dest-dec-address*

no decnet accounting list {*src-dec-address dest-dec-address* | **all**}

Syntax Description	<i>src-dec-address</i>	DECnet address for the source. The address is in the form <i>area.node</i> , for example, 5.3.
	<i>dest-dec-address</i>	DECnet address for the destination. The address is in the form <i>area.node</i> , for example, 5.3.
	all	Disables DECnet accounting for all source and destination address pairs specified previously with the decnet accounting list command.

decnet accounting threshold

To set the maximum number of accounting database entries, use the **decnet accounting threshold** command in global configuration mode. To restore the default, use the **no** form of this command.

decnet accounting threshold *threshold*

no decnet accounting threshold *threshold*

Syntax Description	<i>threshold</i>	Maximum number of entries (source and destination address pairs) that Cisco IOS software can accumulate.
---------------------------	------------------	--

decnet accounting transits

To set the maximum number of transit entries that will be stored in the DECnet accounting database, use the **decnet accounting transits** command in global configuration mode. To disable this function, use the **no** form of this command.

decnet accounting transits *count*

no decnet accounting transits

Syntax Description	<i>count</i>	Number of transit entries that will be stored in the DECnet accounting database.
---------------------------	--------------	--

decnet advertise

To configure border routers to propagate Phase IV areas through an OSI backbone, use the **decnet advertise** command in global configuration mode. To disable this function, use the **no** form of this command.

decnet advertise [*decnet-area*] *hops cost*

no decnet advertise [*decnet-area*]

Syntax Description	<i>decnet-area</i>	(Optional) Phase IV area that you want propagated.
	<i>hops</i>	Hop count to be associated with the route being advertised. Default is 0.
	<i>cost</i>	Cost to be associated with the route being advertised. Default is 0.

decnet area-max-cost

To set the maximum cost specification value for *interarea* routing, use the **decnet area-max-cost** command in global configuration mode.

decnet [*network-number*] **area-max-cost** *value*

Syntax Description	<i>network-number</i>	(Optional) Network number from 0 to 3. Specified when using Address Translation Gateway (ATG). If not specified, the default is network 0.
	<i>value</i>	Maximum cost for a route to a distant area that Cisco IOS software may consider usable; the software treats as unreachable any route with a cost greater than the value you specify. A valid range for cost is 1 to 1022. This parameter is only valid for area routers. The default is 1022.

decnet area-max-hops

To set the maximum hop count value for *interarea* routing, use the **decnet area-max-hops** command in global configuration mode.

decnet [*network-number*] **area-max-hops** *value*

Syntax Description		
	<i>network-number</i>	(Optional) Network number in the range 0 to 3. Specified when using ATG. If not specified, the default is network 0.
	<i>value</i>	Maximum number of hops for a usable route to a distant area. The Cisco IOS software treats as unreachable any route with a count greater than the value you specify. A valid range for the hop count is 1 to 30.

decnet cluster-alias update

To allow all cluster aliases to be propagated, use the **decnet cluster-alias update** command in interface configuration mode. To prevent cluster aliases from being propagated, use the **no** form of this command.

decnet cluster-alias update

no decnet cluster-alias update

Syntax Description	
	This command has no arguments or keywords.

decnet cluster-holdtime

To set a holdtime for a cluster alias adjacency, use the **decnet cluster-holdtime** command in interface configuration mode. To restore the default, use the **no** form of this command.

decnet cluster-holdtime *seconds*

no decnet cluster-holdtime

Syntax Description		
	<i>seconds</i>	Amount of time, in seconds, before the cluster alias adjacency times out.

decnet congestion-threshold

To set the congestion-experienced bit if the output queue has more than the specified number of packets in it, use the **decnet congestion-threshold** command in interface configuration mode. To remove the parameter setting and set it to 0, use the **no** form of this command.

decnet congestion-threshold *number*

no decnet congestion-threshold

Syntax Description	<i>number</i>	Number of packets that are allowed in the output queue before the system sets the congestion experience bit. This value is an integer between 0 and 0x7fff. The value zero prevents this bit from being set. Only relatively small integers are reasonable. The default is 1 packet.
---------------------------	---------------	--

decnet conversion

To allow Phase IV routers (running Cisco Release 9.1 or higher) to run in a Phase V network and vice versa, enable conversion with the **decnet conversion** command in global configuration mode. To disable conversion, use the **no** form of this command.

decnet conversion *nsap-prefix*

no decnet conversion *nsap-prefix*

Syntax Description	<i>nsap-prefix</i>	Value used for the IDP field when constructing NSAPs from a Phase IV address.
---------------------------	--------------------	---

decnet cost

To set a cost value for an interface, use the **decnet cost** command in interface configuration mode. To disable DECnet routing for an interface, use the **no** form of this command.

decnet cost *cost-value*

no decnet cost

Syntax Description	<i>cost-value</i>	Integer from 1 to 63. There is no default cost for an interface, although a suggested cost for FDDI is 1, for Ethernet is 4, and for serial links is greater than 10.
---------------------------	-------------------	---

decnet encapsulation

To provide DECnet encapsulation over Token Ring, use the **decnet encapsulation** command in interface configuration mode.

decnet encapsulation { **pre-dec** | **dec** }

Syntax Description		
	pre-dec	Configures routers for operation on the same Token Ring with routers running software versions prior to Cisco IOS Release 9.1. In this mode, Cisco routers cannot communicate with non-Cisco equipment. Referred to as Cisco-style encapsulation.
	dec	Provides encapsulation that is compatible with other Digital equipment. All Cisco routers must be running Cisco IOS Release 9.1 or a later release.

decnet hello-timer

To change the interval for sending broadcast hello messages, use the **decnet hello-timer** command in interface configuration mode. To restore the default value, use the **no** form of this command.

decnet hello-timer *seconds*

no decnet hello-timer

Syntax Description		
	<i>seconds</i>	Interval at which Cisco IOS software sends hello messages. It can be a decimal number in the range 1 to 8191 seconds. The default is 15 seconds.

decnet host

To associate a name-to-DECnet address mapping, use the **decnet host** command in global configuration mode. To disable name mapping, use the **no** form of this command.

decnet host *name decnet-address*

no decnet host *name*

Syntax Description		
	<i>name</i>	A name you choose that uniquely identifies this DECnet address.
	<i>decnet-address</i>	Source address. DECnet addresses are written in the form <i>area.node</i> . For example, 50.4 is node 4 in area 50. All addresses are in decimal.

decnet in-routing-filter

To provide access control to hello messages or routing information received on an interface, use the **decnet in-routing-filter** command in interface configuration mode. To remove access control, use the **no** form of this command.

decnet in-routing-filter *access-list-number*

no decnet in-routing-filter

Syntax Description	<i>access-list-number</i>	Standard DECnet access list. This list applies to source addresses. The value can be in the range 300 to 399.
---------------------------	---------------------------	---

decnet map

To establish an address translation for selected nodes, use the **decnet map** command in global configuration mode.

decnet *first-network* **map** *virtual-address* *second-network* *real-address*

Syntax Description	<i>first-network</i>	DECnet network numbers in the range 0 to 3.
	<i>virtual-address</i>	Numeric DECnet address (10.5, for example).
	<i>second-network</i>	DECnet network number you map to; DECnet numbers range 0 to 3.
	<i>real-address</i>	Numeric DECnet address (10.5, for example).

decnet max-address

To configure Cisco IOS software with a maximum number of node addresses, use the **decnet max-address** command in global configuration mode.

decnet [*network-number*] **max-address** *value*

Syntax Description	<i>network-number</i>	(Optional) Network number in the range 0 to 3. Specified when using ATG.
	<i>value</i>	A number less than or equal to 1023 that represents the maximum address possible on the network. In general, all routers on the network should use the same value for this argument. The default is 1023.

decnet max-area

To set the largest number of areas that Cisco IOS software can handle in its routing table, use the **decnet max-area** command in global configuration mode.

```
decnet [network-number] max-area area-number
```

Syntax Description		
	<i>network-number</i>	(Optional) Network number in the range 0 to 3. Specified when using ATG.
	<i>area-number</i>	Area number from 1 to 63. Like the decnet max-address global configuration command value, this argument controls the sizes of internal routing tables and of messages sent to other nodes. All routers on the network should use the same maximum address value. The default is 63.

decnet max-cost

To set the maximum cost specification for *intra-area* routing, use the **decnet max-cost** command in global configuration mode.

```
decnet [network-number] max-cost cost
```

Syntax Description		
	<i>network-number</i>	(Optional) Network number in the range 0 to 3. Specified when using ATG.
	<i>cost</i>	Cost from 1 to 1022. The default is 1022.

decnet max-hops

To set the maximum hop count specification value for *intra-area* routing, use the **decnet max-hops** command in global configuration mode.

```
decnet [network-number] max-hops hop-count
```

Syntax Description		
	<i>network-number</i>	(Optional) Network number in the range 0 to 3. Specified when using ATG.
	<i>hop-count</i>	Hop count from 1 to 30. Cisco IOS software ignores routes that have a hop count greater than the corresponding value of this parameter. The default is 30 hops.

decnet max-paths

To define the maximum number of equal-cost paths to a destination that Cisco IOS software keeps in its routing table, use the **decnet max-paths** command in global configuration mode.

```
decnet [network-number] max-paths value
```

Syntax Description	<i>network-number</i>	(Optional) Network number in the range 0 to 3. Specified when using ATG.
	<i>value</i>	Decimal number equal to the maximum number of equal-cost paths the software will save. The valid range is 1 to 31. The default is 1.

decnet max-visits

To set the limit on the number of times a packet can pass through a router, use the **decnet max-visits** command in global configuration mode.

decnet [*network-number*] **max-visits** *value*

Syntax Description	<i>network-number</i>	(Optional) Network number in the range 0 to 3. Specified when using ATG.
	<i>value</i>	Number of times a packet can pass through a router. It can be a decimal number in the range 1 to 63. If a packet exceeds <i>value</i> , Cisco IOS software discards the packet. Digital recommends that the value of the max-visits parameter be at least twice that of the max-hops parameter, to allow packets to still reach their destinations when routes are changing. The default is 63 times.

decnet multicast-map

To specify a mapping between DECnet multicast addresses and Token Ring functional addresses, other than the default mapping, use the **decnet multicast-map** command in interface configuration mode. To delete the specified information, use the **no** form of this command.

decnet multicast-map *multicast-address-type functional-address*

no decnet multicast-map *multicast-address-type functional-address*

Syntax Description	<i>multicast-address-type</i>	Type of multicast address that is used. The following are valid values for the argument: <ul style="list-style-type: none"> • iv-all-routers (all Phase-IV routers) • iv-all-endnodes (all Phase-IV end nodes) • iv-prime-all-routers (all Phase IV Prime routers)
	<i>functional-address</i>	Functional MAC address to which this multicast ID maps; in the form of "c000.xxxx.yyyy."

decnet node-type

To specify the node type, use the **decnet node-type** command in global configuration mode.

```
decnet [network-number] node-type {area | routing-iv}
```

Syntax Description		
	<i>network-number</i>	(Optional) Network number in the range 0 to 3. Specified when using ATG. If not specified, the default is network 0.
	area	Router participates in the DECnet routing protocol with other area routers, as described in the Digital documentation, and routes packets from and to routers in other areas. This is sometimes referred to as Level 2 (or interarea) routing. An area router does not just handle interarea routing, it also acts as an intra-area or Level 1 router in its own area.
	routing-iv	Router acts as an intra-area (standard DECnet Phase IV, Level 1 router) and ignores Level 2 routing packets. In this mode, it routes packets destined for other areas to a designated interarea router, exchanging packets with other end nodes and routers in the same area.

decnet out-routing-filter

To provide access control to routing information being sent out on an interface, use the **decnet out-routing-filter** command in interface configuration mode. To remove access control, use the **no** form of this command.

```
decnet out-routing-filter access-list-number
```

```
no decnet out-routing-filter
```

Syntax Description		
	<i>access-list-number</i>	Standard DECnet access list applying to source addresses. The value can be in the range 300 to 399.

decnet path-split-mode

To specify how Cisco IOS software splits the routable packets between equal-cost paths, use the **decnet path-split-mode** command in global configuration mode.

```
decnet path-split-mode {normal | interim}
```

Syntax Description	normal	Normal mode, where equal-cost paths are selected on a round-robin basis. This is the default.
	interim	Traffic for any particular (higher-layer) session is always routed over the same path. This mode supports older implementations of DECnet (VMS Versions 4.5 and earlier) that do not support out-of-order packet caching. Other sessions may take another path, thus using equal-cost paths that a router may have for a particular destination.

decnet propagate static

To enable static route propagation, use the **decnet propagate static** command in global configuration mode. To disable propagation, use the **no** form of this command.

decnet propagate static

no decnet propagate static

Syntax Description This command has no arguments or keywords.

decnet route (interface static route)

To create an interface static route, use this version of the **decnet route** command in global configuration mode. To remove this route, use the **no** form of this command.

decnet route *decnet-address next-hop-type number [snpa-address] [hops [cost]]*

no decnet route *decnet-address next-hop-type number*

Syntax Description	<i>decnet-address</i>	DECnet address. This value is entered into a static routing table and used to match a destination DECnet address. Use a node address value of 0 to specify an area static route.
	<i>next-hop-type</i>	Interface type.
	<i>number</i>	Interface number.
	<i>snpa-address</i>	(Optional) Optional for serial links; required for multiaccess networks.
	<i>hops</i>	(Optional) Hop count to be associated with the route being advertised.
	<i>cost</i>	(Optional) Cost to be associated with the route being advertised.

decnet route (specific static route)

To enter a specific static route, use this version of the **decnet route** command in global configuration mode. DECnet addresses that match are forwarded to the *next-hop-address*. To remove this route, use the **no** form of this command.

decnet route *decnet-address next-hop-address [hops [cost]]*

no decnet route *decnet-address next-hop-address*

Syntax Description		
<i>decnet-address</i>	DECnet address. This value is entered into a static routing table and used to match a destination DECnet address. Use a node address value of 0 to specify an area static route.	
<i>next-hop-address</i>	This value is used to establish the next hop of the route for forwarding packets.	
<i>hops</i>	(Optional) Hop count to be associated with the route being advertised. Default is 0.	
<i>cost</i>	(Optional) Cost to be associated with the route being advertised. Default is 0.	

decnet route default (interface default route)

To create an interface default route, use this version of the **decnet route default** command in global configuration mode. To remove this route, use the **no** form of this command.

decnet route default *next-hop-type number [snpa-address] [hops [cost]]*

no decnet route default *next-hop-type number*

Syntax Description		
<i>next-hop-type</i>	Interface type.	
<i>number</i>	Interface number.	
<i>snpa-address</i>	(Optional) Optional for serial links; required for multiaccess networks.	
<i>hops</i>	(Optional) Hop count to be associated with the route being advertised. Default is 0.	
<i>cost</i>	(Optional) Cost to be associated with the route being advertised. Default is 0.	

decnet route default (specific default route)

To enter a specific default route, use this version of the **decnet route default** command in global configuration mode. To remove this route, use the **no** form of this command.

decnet route default *next-hop-address [hops [cost]]*

no decnet route default *next-hop-address*

Syntax Description	<i>next-hop-address</i>	This value is used to establish the next hop of the route for forwarding packets.
	<i>hops</i>	(Optional) Hop count to be associated with the route being advertised. Default is 0.
	<i>cost</i>	(Optional) Cost to be associated with the route being advertised. Default is 0.

decnet route-cache

To enable fast switching, use the **decnet route-cache** command in interface configuration mode. To disable fast switching, use the **no** form of this command.

decnet route-cache

no decnet route-cache

Syntax Description This command has no arguments or keywords.

decnet router-priority

To elect a designated router to which packets are sent when no destination is specified, use the **decnet router-priority** command in interface configuration mode.

decnet router-priority *value*

Syntax Description *value* Priority of the router. This can be a number in the range 0 to 127. The larger the number the higher the priority.

decnet routing

To enable DECnet routing, use the **decnet routing** command in global configuration mode. To disable DECnet routing, use the **no** form of this command.

decnet [*network-number*] **routing** [**iv-prime**] *decnet-address*

no decnet routing

Syntax Description

<i>network-number</i>	(Optional) Network number in the range 0 to 3. Specified when using ATG. If not specified, the default is network 0.
iv-prime	(Optional) Enables DECnet Phase IV Prime routing.
<i>decnet-address</i>	Address in DECnet format X.Y, where X is the area number and Y is the node number.

decnet routing-timer

To specify how often Cisco IOS software sends routing updates that list the hosts that the router can reach, use the **decnet routing-timer** command in interface configuration mode. To disable the routing update timer, use the **no** form of this command.

decnet routing-timer *seconds*

no decnet routing-timer

Syntax Description

seconds Time, in seconds, from 1 to 65,535. The default is 40 seconds.

decnet split-horizon

To use split horizon when sending routing updates, use the **decnet split-horizon** command in interface configuration mode. To disable split horizon, use the **no** form of this command.

decnet split-horizon

no decnet split-horizon

Syntax Description

This command has no arguments or keywords.

lat host-delay

To set the delayed acknowledgment for incoming local-area transport (LAT) slave connections, use the **lat host-delay** command in global configuration mode. To restore the default, use the **no** form of this command.

lat host-delay *number*

no host-delay

Syntax Description

number Delay, in milliseconds.

lat service autocommand

To associate a command with a service, use the **lat service autocommand** command in global configuration mode. To remove the specified autocommand, use the **no** form of this command.

lat service *service-name* **autocommand** *command*

no lat service *service-name* **autocommand** *command*

Syntax Description

<i>service-name</i>	Name of the service.
<i>command</i>	Command to be associated with the service.

show decnet

To display the global DECnet parameters, use the **show decnet** command in privileged EXEC mode.

```
show decnet
```

Syntax Description

This command has no arguments or keywords.

show decnet accounting

To display the active accounting or checkpointed database, use the **show decnet accounting** command in EXEC mode.

```
show decnet accounting [checkpoint]
```

Syntax Description

checkpoint	(Optional) Displays entries in the checkpoint database.
-------------------	---

show decnet interface

To display the global DECnet status and configuration for all interfaces, or the status and configuration for a specified interface, use the **show decnet interface** command in EXEC mode.

```
show decnet interface [type number]
```

Syntax Description

<i>type</i>	(Optional) Interface type.
<i>number</i>	(Optional) Interface number.

show decnet map

To display the address mapping information used by the DECnet Address Translation Gateway, use the **show decnet map** command in EXEC mode.

```
show decnet map
```

Syntax Description

This command has no arguments or keywords.

show decnet neighbors

To display all Phase IV and Phase IV Prime adjacencies and the MAC address associated with each neighbor, use the **show decnet neighbors** command in privileged EXEC mode.

```
show decnet neighbors
```

Syntax Description This command has no arguments or keywords.

show decnet route

To display the DECnet routing table, use the **show decnet route** command in EXEC mode.

```
show decnet route [decnet-address]
```

Syntax Description *decnet-address* (Optional) Displays the DECnet address and, when specified, the first hop route to that address.

show decnet static

To display all statically configured DECnet routes, use the **show decnet static** command in privileged EXEC mode.

```
show decnet static
```

Syntax Description This command has no arguments or keywords.

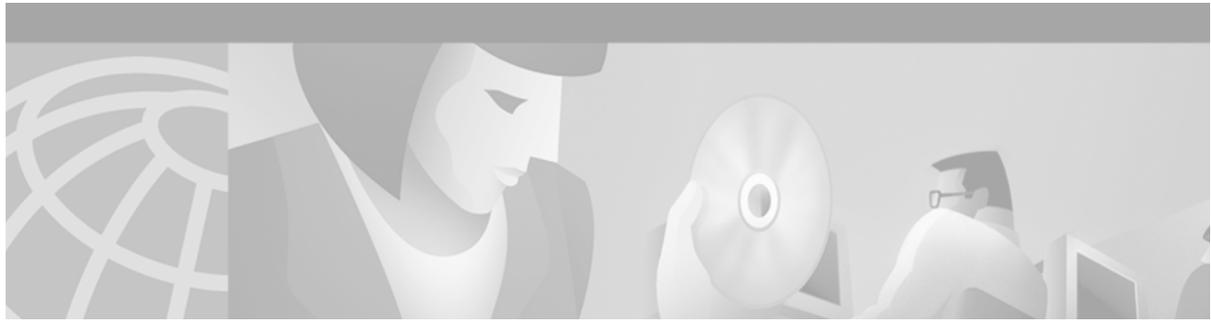
show decnet traffic

To show the DECnet traffic statistics (including datagrams sent, received, and forwarded), use the **show decnet traffic** command in EXEC mode.

```
show decnet traffic
```

Syntax Description This command has no arguments or keywords.

■ show decnet traffic



ISO CLNS Commands

This chapter describes the function and syntax of the International Organization for Standardization (ISO) Connectionless Network Service (CLNS) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference*.

clear clns cache

To clear and reinitialize the CLNS routing cache, use the **clear clns cache** command in EXEC mode.

```
clear clns cache
```

Syntax Description

This command has no arguments or keywords.

clear clns es-neighbors

To remove end system (ES) neighbor information from the adjacency database, use the **clear clns es-neighbors** command in EXEC mode.

```
clear clns [tag] es-neighbors
```

Syntax Description

<i>tag</i>	(Optional) Meaningful name for a routing process. For example, you could define a routing process named <i>Finance</i> for the Finance department, and another routing process named <i>Marketing</i> for the Marketing department. If not specified, a null tag is assumed. The <i>tag</i> argument must be unique among all CLNS router processes for a given router.
------------	---

clear clns is-neighbors

To remove intermediate system (IS) neighbor information from the adjacency database, use the **clear clns is-neighbors** command in EXEC mode.

```
clear clns [tag] is-neighbors
```

Syntax Description	<i>tag</i>	(Optional) Meaningful name for a routing process. For example, you could define a routing process named <i>Finance</i> for the Finance department, and another routing process named <i>Marketing</i> for the Marketing department. If not specified, a null tag is assumed. The <i>tag</i> argument must be unique among all CLNS router processes for a given router.
---------------------------	------------	---

clear clns neighbors

To remove CLNS neighbor information from the adjacency database, use the **clear clns neighbors** command in EXEC mode.

clear clns [*tag*] **neighbors**

Syntax Description	<i>tag</i>	(Optional) Meaningful name for a routing process. For example, you could define a routing process named <i>Finance</i> for the Finance department, and another routing process named <i>Marketing</i> for the Marketing department. If not specified, a null tag is assumed. The <i>tag</i> argument must be unique among all CLNS router processes for a given router.
---------------------------	------------	---

clear clns route

To remove all of the dynamically derived CLNS routing information, use the **clear clns route** command in EXEC mode.

clear clns route

Syntax Description	This command has no arguments or keywords.
---------------------------	--

clear clns traffic

To clear all ISO CLNS statistics that are displayed when you use the **show clns traffic** command, use the **clear clns traffic** command in EXEC mode.

clear clns [*tag*] **traffic**

Syntax Description	<i>tag</i>	(Optional) Meaningful name for a routing process. For example, you could define a routing process named <i>Finance</i> for the Finance department, and another routing process named <i>Marketing</i> for the Marketing department. If not specified, a null tag is assumed. The <i>tag</i> argument must be unique among all CLNS router processes for a given router.
---------------------------	------------	---

clear tarp counters

To clear all Target Identifier Address Resolution Protocol (TARP) counters that are shown with the **show tarp traffic** command, use the **clear tarp counters** command in EXEC mode.

```
clear tarp counters
```

Syntax Description This command has no arguments or keywords.

clear tarp ldb-table

To clear the system ID-to-sequence number mapping entries stored in the TARP loop-detection buffer table, use the **clear tarp ldb-table** command in EXEC mode.

```
clear tarp ldb-table
```

Syntax Description This command has no arguments or keywords.

clear tarp tid-table

To clear the dynamically created TARP target identifier (TID)-to-NSAP address mapping entries stored in TID cache, use the **clear tarp tid-table** command in EXEC mode.

```
clear tarp tid-table
```

Syntax Description This command has no arguments or keywords.

clns access-group

To filter transit CLNS traffic going either into or out of the router or both on a per-interface basis, use the **clns access-group** command in interface configuration mode. To disable filtering of transit CLNS packets, use the **no** form of this command.

```
clns access-group name [in | out]
```

```
no clns access-group name [in | out]
```

Syntax Description	<i>name</i>	Name of the filter set or expression to apply.
	in	(Optional) Filter should be applied to CLNS packets entering the router.
	out	(Optional) Filter should be applied to CLNS packets leaving the router. If you do not specify an in or out keyword, out is assumed.

clns adjacency-filter

To filter the establishment of ES-IS adjacencies, use the **clns adjacency-filter** command in interface configuration mode. To disable this filtering, use the **no** form of this command.

clns adjacency-filter {es | is} *name*

no clns adjacency-filter {es | is} *name*

Syntax Description		
	es	ES adjacencies are to be filtered.
	is	IS adjacencies are to be filtered.
	<i>name</i>	Name of the filter set or expression to apply.

clns cache-invalidate-delay

To control the invalidation rate of the CLNS route cache, use the **clns cache-invalidate-delay** command in global configuration mode. To allow the CLNS route cache to be immediately invalidated, use the **no** form of this command.

clns cache-invalidate-delay [*minimum maximum quiet threshold*]

no clns cache-invalidate-delay

Syntax Description		
	<i>minimum</i>	(Optional) Minimum time (in seconds) between invalidation request and actual invalidation. The default is 2 seconds.
	<i>maximum</i>	(Optional) Maximum time (in seconds) between invalidation request and actual invalidation. The default is 5 seconds.
	<i>quiet</i>	(Optional) Length of time (in seconds) before invalidation.
	<i>threshold</i>	(Optional) Maximum number of invalidations considered to be quiet.

clns checksum

To enable checksum generation when ISO CLNS routing software sources a CLNS packet, use the **clns checksum** command in interface configuration mode. To disable checksum generation, use the **no** form of this command.

clns checksum

no clns checksum

Syntax Description	
	This command has no arguments or keywords.

clns cluster-alias

To allow multiple end systems to advertise the same NSAP address but with different system IDs in ES hello messages, use the **clns cluster-alias** command in interface configuration mode. To disable cluster aliasing, use the **no** form of this command.

clns cluster-alias

no clns cluster-alias

Syntax Description This command has no arguments or keywords.

clns configuration-time

To specify the rate at which ES hellos and IS hellos are sent, use the **clns configuration-time** command in global configuration mode. To restore the default value, use the **no** form of this command.

clns configuration-time *seconds*

no clns configuration-time

Syntax Description *seconds* Rate, in seconds, at which ES and IS hello packets are sent.

clns congestion-threshold

To set the congestion experienced bit if the output queue has more than the specified number of packets in it, use the **clns congestion-threshold** command in interface configuration mode. A *number* value of zero or the **no** form of this command prevents this bit from being set. To remove the parameter setting and set it to 0, use the **no** form of this command.

clns congestion-threshold *number*

no clns congestion-threshold

Syntax Description *number* Number of packets that are allowed in the output queue before the system sets the congestion-experienced bit. The value zero (0) prevents this bit from being set.

clns dec-compatible

To allow IS hellos sent and received to ignore the N-selector byte, use the **clns dec-compatible** command in interface configuration mode. To disable this feature, use the **no** form of this command.

clns dec-compatible

no clns dec-compatible

Syntax Description This command has no arguments or keywords.

clns enable

If you do not intend to perform any dynamic routing on an interface, but intend to pass ISO CLNS packet traffic to end systems, use the **clns enable** command in interface configuration mode. To disable ISO CLNS on a particular interface, use the **no** form of this command.

clns enable

no clns enable

Syntax Description This command has no arguments or keywords.

clns erpdu-interval

To determine the minimum interval time, in milliseconds, between error ERPDUs, use the **clns erpdu-interval** command in interface configuration mode. A *milliseconds* value of zero or the **no** form of this command turns off the interval and effectively sets no limit between ERPDUs.

clns erpdu-interval *milliseconds*

no clns erpdu-interval *milliseconds*

Syntax Description *milliseconds* Minimum interval time (in milliseconds) between ERPDUs.

clns esct-time

To supply an ES configuration timer option in a transmitted IS hello packet that tells the ES how often it should transmit ES hello packet PDUs, use the **clns esct-time** command in interface configuration mode. To restore the default value and disable this function, use the **no** form of this command.

clns esct-time *seconds*

no clns esct-time *seconds*

Syntax Description	<i>seconds</i>	Time, in seconds, between ES hello PDUs. Range is from 0 to 65,535.
---------------------------	----------------	---

clns es-neighbor

To manually define adjacencies for end systems that do not support the ES-IS routing protocol, use the **clns es-neighbor** command in interface configuration mode. To delete the ES neighbor, use the **no** form of this command.

clns es-neighbor *nsap snpa*

no clns es-neighbor *nsap*

Syntax Description	<i>nsap</i>	Specific NSAP to map to a specific data link address.
	<i>snpa</i>	Data link address.

clns filter-expr

To combine CLNS filter sets and CLNS address templates to create complex logical NSAP pattern-matching expressions, use one or more **clns filter-expr** commands in global configuration mode. To delete the expression, use the **no** form of this command.

clns filter-expr *ename* [*term* | **not** *term* | *term* {**and** | **or** | **xor**} *term*]

no clns filter-expr *ename*

Syntax Description	<i>ename</i>	Alphanumeric name to apply to this filter expression.
	not	(Optional) Defines a filter expression that is pattern matched only if the pattern given by <i>term</i> is not matched.
	and	(Optional) Defines a filter expression that is pattern matched only if both of the patterns given by the two terms are matched.
	or	(Optional) Defines a filter expression that is pattern matched if either of the patterns given by the two terms is matched.

xor	(Optional) Defines a filter expression that is pattern matched only if one of the patterns, but not both, given by the two terms are matched.
<i>term</i>	(Optional) Filter expression term. A term can be any of the following: <i>ename</i> —Another, previously defined, filter expression. <i>sname</i> (or destination sname)—A previously defined filter set name, with the filter set applied to the destination NSAP address. source sname —A previously defined filter set name, with the filter set applied to the source NSAP address.

clns filter-set

To build a list of CLNS address templates with associated permit and deny conditions for use in CLNS filter expressions, use the **clns filter-set** command in global configuration mode. CLNS filter expressions are used in the creation and use of CLNS access lists. To delete the entire filter set, use the **no** form of this command.

clns filter-set *name* [**permit** | **deny**] *template*

no clns filter-set *name*

Syntax Description	<i>name</i>	Alphanumeric name to apply to this filter set.
	permit deny	(Optional) Addresses matching the pattern specified by <i>template</i> are to be permitted or denied. If neither permit nor deny is specified, permit is assumed.
	<i>template</i>	Address template, template alias name, or the keyword default . Address templates and alias names are described under the description of the clns template-alias global configuration command. The default keyword denotes a zero-length prefix and matches any address.

clns holding-time

To allow the sender of an ES hello or IS hello to specify the length of time for which you consider the information in the hello packets to be valid, use the **clns holding-time** command in global configuration mode. To restore the default value (300 seconds, or 5 minutes), use the **no** form of this command.

clns holding-time *seconds*

no clns holding-time

Syntax Description	<i>seconds</i>	Length of time, in seconds, during which the information in the hello packets is considered valid.
---------------------------	----------------	--

clns host

To define a name-to-NSAP mapping that can then be used with commands that require NSAPs, use the **clns host** command in global configuration mode.

clns host *name nsap*

Syntax Description		
	<i>name</i>	Desired name for the NSAP. The first character can be either a letter or a number, but if you use a number, the operations you can perform are limited.
	<i>nsap</i>	NSAP to which that the name maps.

clns is-neighbor

To manually define adjacencies for intermediate systems, use the **clns is-neighbor** command in interface configuration mode. To delete the specified IS neighbor, use the **no** form of this command.

clns is-neighbor *nsap snpa*

no clns is-neighbor *nsap*

Syntax Description		
	<i>nsap</i>	NSAP of a specific intermediate system to enter as neighbor to a specific data link address.
	<i>snpa</i>	Data link address.

clns mtu

To set the maximum transmission unit (MTU) packet size for the interface, use the **clns mtu** command in interface configuration mode. To restore the default and maximum packet size, use the **no** form of this command.

clns mtu *bytes*

no clns mtu

Syntax Description		
	<i>bytes</i>	Maximum packet size in bytes. The minimum value is 512; the default and maximum packet size depend on the interface type.

clns net (global)

To assign a static address for a router, use the **clns net** command in global configuration mode. If the Cisco IOS software is configured to support ISO CLNS, but is not configured to dynamically route CLNS packets using ISO IGRP or IS-IS, use this command to assign an address to the router. To remove any previously configured NET or NSAP address, use the **no** form of this command.

```
clns net {net-address | name}
```

```
no clns net {net-address | name}
```

Syntax Description

<i>net-address</i>	NET address.
<i>name</i>	CLNS host name to be associated with this interface.

clns net (interface)

To assign an NSAP address or name to a router interface, use the **clns net** command in interface configuration mode. If Cisco IOS software is configured to support ISO CLNS, but is not configured to dynamically route CLNS packets using an ISO IGRP or IS-IS, use this command to assign an address to the router. To remove any previously configured NSAP address, use the **no** form of this command.

```
clns net {nsap-address | name}
```

```
no clns net {nsap-address | name}
```

Syntax Description

<i>nsap-address</i>	Specific NSAP address.
<i>name</i>	Name to be associated with this interface.

clns packet-lifetime

To specify the initial lifetime for locally generated packets, use the **clns packet-lifetime** command in global configuration mode. To remove the parameter's settings, use the **no** form of this command.

```
clns packet-lifetime seconds
```

```
no clns packet-lifetime
```

Syntax Description

<i>seconds</i>	Packet lifetime in seconds.
----------------	-----------------------------

clns rdpdu-interval

To determine the minimum interval time between redirect PDUs (RDPDUs), use the **clns rdpdu-interval** command in interface configuration mode. To turn off the interval rate and effectively set no limit between RDPDUs, use the **no** form of this command or a *milliseconds* value of zero.

clns rdpdu-interval *milliseconds*

no clns rdpdu-interval *milliseconds*

Syntax Description	<i>milliseconds</i>	Minimum interval time in milliseconds between RDPDUs.
---------------------------	---------------------	---

clns route (create)

To create an interface static route, use this form of the **clns route** command in global configuration mode. To remove this route, use the **no** form of this command.

clns route *nsap-prefix type number [snpa-address]*

no clns route *nsap-prefix*

Syntax Description	<i>nsap-prefix</i>	Network service access point prefix. This value is entered into a static routing table and used to match the beginning of a destination NSAP. The longest NSAP-prefix entry that matches is used.
	<i>type</i>	Interface type.
	<i>number</i>	Interface number.
	<i>snpa-address</i>	(Optional) Specific subnetwork point of attachment (SNPA) address. Optional for serial links; required for multiaccess networks.

clns route (enter)

To enter a specific static route, use this form of the **clns route** command in global configuration mode. NSAPs that start with *nsap-prefix* are forwarded to *next-hop-net* or the *name* of the next hop. To remove this route, use the **no** form of this command.

clns route *nsap-prefix {next-hop-net | name}*

no clns route *nsap-prefix*

Syntax Description	<i>nsap-prefix</i>	Network service access point prefix. This value is entered into a static routing table and used to match the beginning of a destination NSAP. The longest NSAP-prefix entry that matches is used.
	<i>next-hop-net</i>	Next-hop NET. This value is used to establish the next hop of the route for forwarding packets.
	<i>name</i>	Name of the next hop node. This value can be used instead of the next-hop NET to establish the next hop of the route for forwarding packets.

clns route-cache

To allow fast switching through the cache, use the **clns route-cache** command in interface configuration mode. To disable fast switching, use the **no** form of this command.

clns route-cache

no clns route-cache

Syntax Description This command has no arguments or keywords.

clns route default

To configure a default zero-length prefix rather than type an NSAP prefix, use the **clns route default** command in global configuration mode. To remove this route, use the **no** form of this command.

clns route default *type number*

no clns route default

Syntax Description	<i>type</i>	Interface type. Specify the interface type immediately followed by the interface number; there is no space between the two.
	<i>number</i>	Interface number.

clns route default discard

To assign a default discard route and automatically discard packets with NSAP addresses that do not match any existing routes, use the **clns route default discard** command in global configuration mode. To remove the default discard route, use the **no** form of this command.

clns route default discard

no clns route default discard

Syntax Description This command has no arguments or keywords.

clns route discard

To explicitly tell a router to discard packets with NSAP addresses that match the specified *nsap-prefix*, use the **clns route discard** command in global configuration mode. To remove this route, use the **no** form of this command.

clns route *nsap-prefix* **discard**

no clns route *nsap-prefix*

Syntax Description	<i>nsap-prefix</i>	Network service access point prefix. This value is entered into a static routing table and used to match the beginning of a destination NSAP. The longest NSAP-prefix entry that matches is used.
	discard	The router discards packets with NSAPs that match the specified value for the <i>nsap-prefix</i> argument.

clns router isis

To configure an Intermediate System-to-Intermediate System (IS-IS) routing process for ISO Connectionless Network Service Protocol (CLNS) on a specified interface and to attach an area designator to the routing process, use the **clns router isis** command in interface configuration mode. To disable IS-IS for ISO CLNS, use the **no** form of the command.

clns router isis *area-tag*

no clns router isis *area-tag*

Syntax Description	<i>area-tag</i>	Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration.
		Defines a meaningful name for an area routing process. If not specified, a null tag is assumed. It must be unique among all CLNS router processes for a given router. The <i>area-tag</i> argument is used later as a reference to this area routing process.
		Each area in a multiarea configuration should have a non-null area tag to facilitate identification of the area.

clns router iso-igrp

To specify ISO IGRP routing on a specified interface, use the **clns router iso-igrp** command in interface configuration mode. To disable ISO IGRP routing for the system, use the **no** form of the global configuration command with the appropriate tag.

clns router iso-igrp *tag* [**level 2**]

no clns router iso-igrp *tag*

Syntax Description	<i>tag</i>	Meaningful name for routing process. It must be unique among all CLNS router processes for a given router. This tag should be the same as defined for the routing process in the router iso-igrp global configuration command.
	level 2	(Optional) Allows the interface to advertise Level 2 information.

clns routing

To enable routing of CLNS packets, use the **clns routing** command in global configuration mode. To disable CLNS routing, use the **no** form of this command.

clns routing

no clns routing

Syntax Description This command has no arguments or keywords.

clns security pass-through

To allow Cisco IOS software to pass packets that have security options set, use the **clns security pass-through** command in global configuration mode. To disable this function, use the **no** form of this command.

clns security pass-through

no clns security pass-through

Syntax Description This command has no arguments or keywords.

clns send-erpdu

To allow CLNS to send an error PDU when the routing software detects an error in a data PDU, use the **clns send-erpdu** command in interface configuration mode. To disable this function, use the **no** form of this command.

clns send-erpdu

no clns send-erpdu

Syntax Description This command has no arguments or keywords.

clns send-rdpdu

To allow CLNS to redirect PDUs (RDPDUs) when a better route for a given host is known, use the **clns send-rdpdu** command in interface configuration mode. To disable this function, use the **no** form of this command.

clns send-rdpdu

no clns send-rdpdu

Syntax Description This command has no arguments or keywords.

clns split-horizon

To implement split horizon for ISO IGRP updates, use the **clns split-horizon** command in interface configuration mode. To disable this function, use the **no** form of this command.

clns split-horizon

no clns split-horizon

Syntax Description This command has no arguments or keywords.

clns template-alias

To build a list of alphanumeric aliases of CLNS address templates for use in the definition of CLNS filter sets, use one or more **clns template-alias** commands in global configuration mode. To delete the alias, use the **no** form of this command.

clns template-alias *name* *template*

no clns template-alias *name*

Syntax Description	<i>name</i>	Alphanumeric name to apply as an alias for the template.
	<i>template</i>	Address template.

clns want-erpdu

To specify whether to request ERPDUs on packets sourced by the router, use the **clns want-erpdu** command in global configuration mode. To remove the parameter's settings, use the **no** form of this command.

clns want-erpdu

no clns want-erpdu

Syntax Description This command has no arguments or keywords.

ctunnel destination

To configure the destination parameter for an IP over CLNS tunnel (CTunnel), use the **ctunnel destination** command in interface configuration mode. To remove the destination parameter, use the **no** form of this command.

ctunnel destination *nsap-address*

no ctunnel destination *nsap-address*

Syntax Description *nsap-address* NSAP address for the CTunnel destination.

distance (ISO CLNS)

To configure the administrative distance for CLNS routes learned, use the **distance** command in router configuration mode. To restore the administrative distance to the default, use the **no** form of this command.

distance *value* [**clns**]

no distance *value* [**clns**]

Syntax Description

<i>value</i>	Administrative distance, indicating the trustworthiness of a routing information source. This argument has a numerical value between 0 and 255. A higher relative value indicates a lower trustworthiness rating. Preference is given to routes with smaller values.
clns	(Optional) CLNS-derived routes for IS-IS.

ignore-lsp-errors

To allow the router to ignore Intermediate System-to-Intermediate System (IS-IS) link-state packets that are received with internal checksum errors rather than purging the link-state packets, use the **ignore-lsp-errors** command in router configuration mode. To disable this function, use the **no** form of this command.

ignore-lsp-errors

no ignore-lsp-errors

Syntax Description This command has no arguments or keywords.

interface ctunnel

To create a virtual interface to transport IP over a CLNS tunnel (CTunnel), use the **interface ctunnel** command in global configuration mode. To remove the virtual interface, use the **no** form of this command.

interface ctunnel *interface-number*

no interface ctunnel *interface-number*

Syntax Description *interface-number* CTunnel interface number (a number from 0 through 2,147,483,647).

ip domain-lookup nsap

To allow Domain Name System (DNS) queries for CLNS addresses, use the **ip domain-lookup nsap** command in global configuration mode. To disable this function, use the **no** form of this command.

ip domain-lookup nsap

no ip domain-lookup nsap

Syntax Description This command has no arguments or keywords.

isis adjacency-filter

To filter the establishment of Intermediate System-to-Intermediate System (IS-IS) adjacencies, use the **isis adjacency-filter** command in interface configuration mode. To disable filtering of the establishment of IS-IS adjacencies, use the **no** form of this command.

isis adjacency-filter *name* [**match-all**]

no isis adjacency-filter *name* [**match-all**]

Syntax Description

<i>name</i>	Name of the filter set or expression to apply.
match-all	(Optional) All NSAP addresses must match the filter in order to accept the adjacency. If not specified (the default), only one address need match the filter in order for the adjacency to be accepted.

iso-igrp adjacency-filter

To filter the establishment of ISO IGRP adjacencies, use the **iso-igrp adjacency-filter** command in interface configuration mode. To disable filtering of the establishment of ISO IGRP adjacencies, use the **no** form of this command.

iso-igrp adjacency-filter *name*

no iso-igrp adjacency-filter *name*

Syntax Description

<i>name</i>	Name of the filter set or expression to apply.
-------------	--

log-adjacency-changes (ISO CLNS)

To cause Intermediate System-to-Intermediate System (IS-IS) to generate a log message when an Netware Link Services Protocol (NLSP) IS-IS adjacency changes state (up or down), use the **log-adjacency-changes** command in router configuration mode. To disable this function, use the **no** form of this command.

log-adjacency-changes

no log-adjacency-changes

Syntax Description

This command has no arguments or keywords.

lsp-mtu (ISO CLNS)

To set the maximum transmission unit (MTU) size of Intermediate System-to-Intermediate System (IS-IS) link-state packets (LSPs), use the **lsp-mtu** command in router configuration mode. To disable this function, use the **no** form of this command.

lsp-mtu *size*

no lsp-mtu

Syntax Description	<i>size</i>	Maximum packet size in bytes. The size must be less than or equal to the smallest MTU of any link in the network. The default size is 1497 bytes.
---------------------------	-------------	---

match clns address

To define the match criterion, use the **match clns address** command in route-map configuration mode. Routes that have a network address matching one or more of the names—and that satisfy all other defined match criteria—will be redistributed. To remove the match criterion, use the **no** form of this command.

match clns address *name* [*name...name*]

no match clns address *name* [*name...name*]

Syntax Description	<i>name</i>	Name of a standard access list, filter set, or expression.
---------------------------	-------------	--

match clns next-hop

To define the next-hop match criterion, use the **match clns next-hop** command in route-map configuration mode. Routes that have a next-hop router address matching one of the names—and that satisfy all other defined match criteria—will be redistributed. To remove the match criterion, use the **no** form of this command.

match clns next-hop *name* [*name...name*]

no match clns next-hop *name* [*name...name*]

Syntax Description	<i>name</i>	Name of an access list, filter set, or expression.
---------------------------	-------------	--

match clns route-source

To define the route-source match criterion, use the **match clns route-source** command in route-map configuration mode. Routes that have been advertised by routers at the address specified by the name—and that satisfy all other defined match criteria—will be redistributed. To remove the specified match criterion, use the **no** form of this command.

match clns route-source *name* [*name...name*]

no match clns route-source *name* [*name...name*]

Syntax Description	<i>name</i>	Name of access list, filter set, or expression.
---------------------------	-------------	---

match interface (ISO CLNS)

To define the interface match criterion, use the **match interface** command in route-map configuration mode. Routes that have the next hop out one of the interfaces specified—and that satisfy all other defined match criteria—will be redistributed. To remove the specified match criterion, use the **no** form of this command.

match interface *type number* [*type number...type number*]

no match interface *type number* [*type number...type number*]

Syntax Description	<i>type</i>	Interface type.
	<i>number</i>	Interface number.

match metric (ISO CLNS)

To define the metric match criterion, use the **match metric** command in route-map configuration mode. Routes that have the specified metric—and satisfy all other defined match criteria—will be redistributed. To remove the specified match criterion, use the **no** form of this command.

match metric *metric-value*

no match metric *metric-value*

Syntax Description	<i>metric-value</i>	Route metric. This can be an Interior Gateway Routing Protocol (IGRP) five-part metric.
---------------------------	---------------------	---

match route-type (ISO CLNS)

To define the route-type match criterion, use the **match route-type** command in route-map configuration mode. Routes that have the specified route type—and satisfy all other defined match criteria—will be redistributed. To remove the specified match criterion, use the **no** form of this command.

```
match route-type {level-1 | level-2}
```

```
no match route-type {level-1 | level-2}
```

Syntax Description	level-1	IS-IS Level 1 routes.
	level-2	IS-IS Level 2 routes.

metric weights (ISO CLNS)

To specify different metrics for the ISO IGRP routing protocol on CLNS, use the **metric weights** command in router configuration mode. This command allows you to configure the metric constants used in the ISO IGRP composite metric calculation of reliability and load. To return the five *k* arguments to their default values, use the **no** form of this command.

```
metric weights qos k1 k2 k3 k4 k5
```

```
no metric weights
```

Syntax Description	qos	QoS defines transmission quality and availability of service. The argument must be 0, the default metric.
	k1, k2, k3, k4, k5	Values that apply to ISO IGRP for the default metric QoS. The <i>k</i> values are metric constants used in the ISO IGRP equation that converts an IGRP metric vector into a scalar quantity. They are numbers from 0 to 127; higher numbers mean a greater multiplier effect.

redistribute (ISO CLNS)

To redistribute routes from one routing domain into another routing domain, use the **redistribute** command in router configuration mode. To disable redistribution, or to disable any of the specified keywords, use the **no** form of this command.

```
redistribute protocol [tag] [route-map map-tag]
```

```
no redistribute protocol [tag] [route-map map-tag] static [clns | ip]
```

Syntax Description	<i>protocol</i>	Type of other routing protocol that is to be redistributed as a source of routes into the current routing protocol being configured. The keywords supported are iso-igrp , isis , and static .
	<i>tag</i>	(Optional) Meaningful name for a routing process.
	route-map <i>map-tag</i>	(Optional) Route map should be interrogated to filter the importation of routes from this source routing protocol to the current routing protocol. If not specified, all routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes will be imported. The argument <i>map-tag</i> is the identifier of a configured route map.
	static	Keyword static is used to redistribute static routes. When used without the optional keywords, Cisco IOS software injects any OSI static routes into an OSI domain.
	clns	(Optional) Keyword clns is used when redistributing OSI static routes into an IS-IS domain.
	ip	(Optional) Keyword ip is used when redistributing IP into an IS-IS domain.

route-map (ISO CLNS)

To define the conditions for redistributing routes from one routing protocol into another, use the **route-map** command in global configuration mode. To delete the route map, use the **no** form of this command.

```
route-map map-tag {permit | deny} sequence-number
```

```
no route-map map-tag {permit | deny} sequence-number
```

Syntax Description	<i>map-tag</i>	Meaningful name for the route map. The redistribute command uses this name to reference this route map. Multiple route-maps can share the same map tag name. Can either be an expression or a filter set.
	permit	If the match criteria are met for this route map, and permit is specified, the route is redistributed as controlled by the set actions. If the match criteria are not met, and permit is specified, the next route map with the same map-tag is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it is not redistributed by that set.
	deny	If the match criteria are met for the route map, and deny is specified, the route is not redistributed, and no further route maps sharing the same map tag name will be examined.
	<i>sequence-number</i>	Number that indicates the position a new route map is to have in the list of route maps already configured with the same name. If given with the no form of this command, it specifies the position of the route map that should be deleted.

router iso-igrp

To identify the area that the router will work in and let it know that it will be routing dynamically using the ISO IGRP protocol, use the **router iso-igrp** command in global configuration mode. To disable ISO IGRP routing for the system, use the **no** form of this command with the appropriate tag.

```
router iso-igrp [tag]
```

```
no router iso-igrp [tag]
```

Syntax Description	<i>tag</i>	(Optional) Meaningful name for a routing process. For example, you could define a routing process named <i>Finance</i> for the Finance department, and another routing process named <i>Marketing</i> for the Marketing department. If not specified, a null tag is assumed. The <i>tag</i> argument must be unique among all CLNS router processes for a given router.
---------------------------	------------	---

set level (ISO CLNS)

To specify the routing level of routes to be advertised into a specified area of the routing domain, use the **set level** command in route-map configuration mode. To disable advertising the specified routing level into a specified area, use the **no** form of this command.

```
set level {level-1 | level-2 | level-1-2}
```

```
no set level {level-1 | level-2 | level-1-2}
```

Syntax Description	level-1	Inserted in IS-IS Level 1 link-state PDUs.
	level-2	Inserted in IS-IS Level 2 link-state PDUs. For IS-IS destinations, level-2 is the default.
	level-1-2	Inserted into both Level 1 and Level 2 IS-IS link-state PDUs.

set metric (ISO CLNS)

To change the metric value used to redistribute routes, use the **set metric** command in route-map configuration mode. To reinstate the original metric values, use the **no** form of this command.

```
set metric metric-value
```

```
no set metric metric-value
```

Syntax Description	<i>metric-value</i>	Route metric. This can be an IGRP five-part metric.
---------------------------	---------------------	---

set metric-type (ISO CLNS)

To set the metric type for redistributed routes, use the **set metric-type** command in route-map configuration mode. To reinstate the original metric type, use the **no** form of this command.

```
set metric-type {internal | external}
```

```
no set metric-type {internal | external}
```

Syntax Description	internal	IS-IS internal metric.
	external	IS-IS external metric.

set tag (ISO CLNS)

To set a tag value to associate with the redistributed routes, use the **set tag** command in route-map configuration mode. To revert to redistributing routes without associating a specific tag with them, use the **no** form of this command.

```
set tag tag-value
```

```
no set tag tag-value
```

Syntax Description	tag-value	Name for the tag. The tag value to associate with the redistributed route. If not specified, the default action is to <i>forward</i> the tag in the source routing protocol onto the new destination protocol.
--------------------	-----------	--

show clns

To display information about the CLNS network, use the **show clns** command in EXEC mode.

```
show clns
```

Syntax Description	This command has no arguments or keywords.
--------------------	--

show clns cache

To display the CLNS route cache, use the **show clns cache** command in EXEC mode. The cache contains an entry for each destination that recently has been fast-switched. The output of this command includes entries showing each destination for which the router has switched a packet in the recent past. This includes the router itself.

```
show clns cache [delay-parameters | invalidations]
```

Syntax Description	delay-parameters	(Optional) Current settings for delays when entries are invalidated in the CLNS route cache.
	invalidations	(Optional) When specified, shows the last time each function purged the CLNS route cache.

show clns es-neighbors

To list the ES neighbors that this router knows about, use the **show clns es-neighbors** command in EXEC mode.

```
show clns area-tag es-neighbors [type number] [detail]
```

Syntax Description	<i>area-tag</i>	Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration. Meaningful name for a routing process. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router. If an area tag is not specified, a null tag is assumed and the process is referenced with a null tag. If an area tag is specified, output is limited to the specified area.
	<i>type</i>	(Optional) Interface type.
	<i>number</i>	(Optional) Interface number.
	detail	(Optional) When specified, the areas associated with the end systems are displayed. Otherwise, a summary display is provided.

show clns filter-expr

To display one or all currently defined CLNS filter expressions, use the **show clns filter-expr** command in EXEC mode.

```
show clns filter-expr [name] [detail]
```

Syntax Description	<i>name</i>	(Optional) Name of the filter expression to display. If none is specified, all are displayed.
	detail	(Optional) When specified, expressions are evaluated down to their most primitive filter set terms before being displayed.

show clns filter-set

To display one or all currently defined CLNS filter sets, use the **show clns filter-set** command in EXEC mode.

```
show clns filter-set [name]
```

Syntax Description	<i>name</i>	(Optional) Name of the filter set to display. If none is specified, all are displayed.
---------------------------	-------------	--

show clns interface

To list the CLNS-specific information about each interface, use the **show clns interface** command in EXEC mode.

```
show clns interface [type number]
```

Syntax Description	<i>type</i>	(Optional) Interface type.
	<i>number</i>	(Optional) Interface number.

show clns is-neighbors

To display Intermediate System-to-Intermediate System (IS-IS) related information for IS-IS router adjacencies, use the **show clns is-neighbors** command in EXEC mode. Neighbor entries are sorted according to the area in which they are located.

```
show clns area-tag is-neighbors [type number] [detail]
```

Syntax Description	<i>area-tag</i>	Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration. Meaningful name for a routing process. This name must be unique among all IP or CLNS router processes for a given router. If an area tag is not specified, a null tag is assumed and the process is referenced with a null tag. If an area tag is specified, output is limited to the specified area.
	<i>type</i>	(Optional) Interface type.
	<i>number</i>	(Optional) Interface number.
	detail	(Optional) When specified, the areas associated with the intermediate systems are displayed. Otherwise, a summary display is provided.

show clns neighbor areas

To display information about Intermediate System-to-Intermediate System (IS-IS) neighbors and the areas to which they belong, use the **show clns neighbor areas** command in EXEC mode.

```
show clns area-tag neighbor areas
```

Syntax Description	<i>area-tag</i>	
		Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration.
		Meaningful name for a routing process. This name must be unique among all IP or CLNS router processes for a given router. If an area tag is not specified, a null tag is assumed and the process is referenced with a null tag. If an area tag is specified, output is limited to the specified area.

show clns neighbors

To display both ES and IS neighbors, use the **show clns neighbors** command in EXEC mode.

```
show clns area-tag neighbors [type number] [area] [detail]
```

Syntax Description	<i>area-tag</i>	
		Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration.
		Meaningful name for a routing process. This name must be unique among all IP or CLNS router processes for a given router. If an area tag is not specified, a null tag is assumed and the process is referenced with a null tag. If an area tag is specified, output is limited to the specified area.
	<i>type</i>	(Optional) Interface type.
	<i>number</i>	(Optional) Interface number.
	area	(Optional) When specified, the CLNS multiarea adjacencies are displayed.
	detail	(Optional) When specified, the area addresses advertised by the neighbor in the hello messages is displayed. Otherwise, a summary display is provided.

show clns protocol

To list the protocol-specific information for each ISO IGRP or Intermediate System-to-Intermediate System (IS-IS) routing process in the router, use the **show clns protocol** command in EXEC mode. There will always be at least two routing processes, a Level 1 and a Level 2, and there can be more.

```
show clns [domain | area-tag] protocol
```

Syntax Description	domain	(Optional) Particular ISO IGRP routing domain.
	<i>area-tag</i>	Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration. Meaningful name for a routing process. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router. If an area tag is not specified, a null tag is assumed and the process is referenced with a null tag. If an area tag is specified, output is limited to the specified area.

show clns route

To display one or all of the destinations to which this router knows how to route CLNS packets, use the **show clns route** command in EXEC mode.

```
show clns route nsap
```

Syntax Description	<i>nsap</i>	CLNS network service access point (NSAP) address.
--------------------	-------------	---

show clns traffic

To list the CLNS packets that this router has seen, use the **show clns traffic** command in EXEC mode.

```
show clns area-tag traffic
```

Syntax Description	<i>area-tag</i>	Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration. Meaningful name for a routing process. This name must be unique among all IP or CLNS router processes for a given router. If an area tag is not specified, a null tag is assumed and the process is referenced with a null tag. If an area tag is specified, output is limited to the specified area.
--------------------	-----------------	---

show isis routes

To display the Intermediate System-to-Intermediate System (IS-IS) Level 1 forwarding table for IS-IS learned routes, use the **show isis routes** command in EXEC mode.

```
show isis area-tag routes
```

Syntax Description	<i>area-tag</i>	<p>Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration.</p> <p>Meaningful name for a routing process. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router. If an area tag is not specified, a null tag is assumed and the process is referenced with a null tag. If an area tag is specified, output is limited to the specified area.</p>
---------------------------	-----------------	---

show route-map

To display all route maps configured or only the one specified, use the **show route-map** command in EXEC mode.

```
show route-map [map-name]
```

Syntax Description	<i>map-name</i>	(Optional) Name of a specific route map.
---------------------------	-----------------	--

show tarp

To display all global TID Address Resolution Protocol (TARP) parameters, use the **show tarp** command in EXEC mode.

```
show tarp
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--

show tarp blacklisted-adjacencies

To list all adjacencies that have been blacklisted (that is, adjacencies that this router will not propagate TARP PDUs to) by the **tarp blacklist-adjacency** command, use the **show tarp blacklisted-adjacencies** command in EXEC mode.

```
show tarp blacklisted-adjacencies
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--

show tarp host

To display information about a specific TID Address Resolution Protocol (TARP) router stored in the local TID cache, use the **show tarp host** command in EXEC mode.

```
show tarp host tid
```

Syntax Description	<i>tid</i>	Target identifier of the router from which you want information. Alphanumeric string up to 255 characters.
---------------------------	------------	---

show tarp interface

To list all interfaces that have TID Address Resolution Protocol (TARP) enabled, use the **show tarp interface** command in EXEC mode.

```
show tarp interface [type number]
```

Syntax Description	<i>type</i>	(Optional) Interface type.
	<i>number</i>	(Optional) Interface number.

show tarp ldb

To display the contents of the loop-detection buffer table, use the **show tarp ldb** command in EXEC mode.

```
show tarp ldb
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--

show tarp map

To list all static entries in the TID cache that were configured with the **tarp map** command, use the **show tarp map** command in EXEC mode.

```
show tarp map
```

Syntax Description	This command has no arguments or keywords.
---------------------------	--

show tarp static-adjacencies

To list all static TID Address Resolution Protocol (TARP) adjacencies that are configured with the **tarp route-static** command, use the **show tarp static-adjacencies** command in EXEC mode.

```
show tarp static-adjacencies
```

Syntax Description This command has no arguments or keywords.

show tarp tid-cache

To display information about the entries in the TID cache, use the **show tarp tid-cache** command in EXEC mode. Entries are created dynamically, statically, or as a result of assigning a TID to the device by using the **tarp tid** command.

```
show tarp tid-cache [detail]
```

Syntax Description

detail	(Optional) List additional information in the TID/NET cache (such as the expiration time for dynamic entries).
---------------	--

show tarp traffic

To display statistics about TID Address Resolution Protocol (TARP) PDUs since the last time the counters were cleared, use the **show tarp traffic** command in EXEC mode.

```
show tarp traffic
```

Syntax Description This command has no arguments or keywords.

tarp allow-caching

To reenble the storage of TID-to-NSAP address mapping in the TID cache, use the **tarp allow-caching** command in global configuration mode. To disable this function and clear the TID cache, use the **no** form of this command.

```
tarp allow-caching
```

```
no tarp allow-caching
```

Syntax Description This command has no arguments or keywords.

tarp arp-request-timer

To set the timeout for TID Address Resolution Protocol (TARP) Type 5 PDUs, use the **tarp arp-request-timer** command in global configuration mode. To set the timeout to the default value, use the **no** form of this command.

tarp arp-request-timer *seconds*

no tarp arp-request-timer

Syntax Description	<i>seconds</i>	Number of seconds for which the router will wait for a response from a TARP Type 5 PDU. The range is from 0 to 3600 seconds.
---------------------------	----------------	--

tarp blacklist-adjacency

To blacklist the specified router so that the router does not receive TID Address Resolution Protocol (TARP) PDUs propagated by this router, use the **tarp blacklist-adjacency** command in global configuration mode. To remove the specified router from the blacklist so that the router can once again receive propagated TARP PDUs, use the **no** form of this command.

tarp blacklist-adjacency *nsap*

no tarp blacklist-adjacency *nsap*

Syntax Description	<i>nsap</i>	NSAP address that cannot receive TARP PDUs. Use the full NSAP address.
---------------------------	-------------	--

tarp cache-timer

To specify the length of time for which a dynamically created TID Address Resolution Protocol (TARP) entry remains in the TID cache, use the **tarp cache-timer** command in global configuration mode. To set the timer to the default value, use the **no** form of this command.

tarp cache-timer *seconds*

no tarp cache-timer

Syntax Description	<i>seconds</i>	Number of seconds for which an entry remains in the TID cache. The range is 30 to 86,400 seconds.
---------------------------	----------------	---

tarp enable

To enable TID Address Resolution Protocol (TARP) on an interface, use the **tarp enable** command in interface configuration mode. To disable TARP on a particular interface, use the **no** form of this command.

tarp enable

no tarp enable

Syntax Description This command has no arguments or keywords.

tarp global-propagate

To reenable the capability to propagate TID Address Resolution Protocol (TARP) PDUs globally, use the **tarp global-propagate** command in global configuration mode. To disable global propagation of TARP PDUs, use the **no** form of this command.

tarp global-propagate

no tarp global-propagate

Syntax Description This command has no arguments or keywords.

tarp ldb-timer

To specify the length of time for which a system ID-to-sequence number mapping entry remains in the loop-detection buffer table, use the **tarp ldb-timer** command in global configuration mode. To set the timer to the default value, use the **no** form of this command.

tarp ldb-timer *seconds*

no tarp ldb-timer

Syntax Description	<i>seconds</i>	Number of seconds for which a system ID-to-sequence number mapping entry remains in the loop-detection buffer table. The range is 0 to 86,400 seconds. The default is 300 seconds.
---------------------------	----------------	--

tarp lifetime

To specify the lifetime for locally generated TID Address Resolution Protocol (TARP) PDUs based on the number of hops, use the **tarp lifetime** command in global configuration mode. To set the PDU lifetime to the default value, use the **no** form of this command.

tarp lifetime *hops*

no tarp lifetime

Syntax Description	<i>hops</i>	Number of hosts that a PDU can traverse before it is discarded. Each router represents one hop. The range is 0 to 65,535 hops. The default is 100 hops.
---------------------------	-------------	---

tarp map

To enter a TID-to-NSAP static map entry in the TID cache, use the **tarp map** command in global configuration mode. To remove a static map entry from the TID cache, use the **no** form of this command.

tarp map *tid nsap*

no tarp map *tid nsap*

Syntax Description	<i>tid</i>	Target identifier to be mapped to the specified NSAP. Alphanumeric string up to 255 characters.
	<i>nsap</i>	NSAP address to map to the specified TID. Use the full NSAP address.

tarp nselector-type

To specify the N-selector to be used in Connectionless Network Protocol (CLNP) PDUs to indicate that the packet is a TID Address Resolution Protocol (TARP) PDU, use the **tarp nselector-type** command in global configuration mode. To set the N-selector to the default value, use the **no** form of this command.

tarp nselector-type *hex-digit*

no tarp nselector-type

Syntax Description	<i>hex-digit</i>	Two digits in hexadecimal format to be used to identify TARP PDUs.
---------------------------	------------------	--

tarp originate

To reenble the router to originate TID Address Resolution Protocol (TARP) PDUs, use the **tarp originate** command in global configuration mode. To disable the capability to originate TARP PDUs, use the **no** form of this command.

tarp originate

no tarp originate

Syntax Description This command has no arguments or keywords.

tarp post-t2-response-timer

To specify the length of time for which a router waits for a response to a Type 2 PDU after the default timer expires, use the **tarp post-t2-response-timer** command in global configuration mode. To set the timer to the default value, use the **no** form of this command.

tarp post-t2-response-timer *seconds*

no tarp post-t2-response-timer

Syntax Description	<i>seconds</i>	Number of seconds for which the router will wait for a response for a Type 2 PDU after the default timer has expired. The range is 0 to 3600 seconds.
---------------------------	----------------	---

tarp propagate

To reenble propagation of TID Address Resolution Protocol (TARP) PDUs on an interface, use the **tarp propagate** command in interface configuration mode. To disable propagation of TARP PDUs on one or more interfaces, use the **no** form of this command.

tarp propagate [**all** | **message-type** *type-number* [*type-number*] [*type-number*]]

no tarp propagate [**all** | **message-type** *type-number* [*type-number*] [*type-number*]]

Syntax Description	all	(Optional) Specifies all TARP PDUs.
	message-type <i>type-number</i>	(Optional) Specifies only type-number broadcast PDUs. Valid values are 1, 2, and 4. You may enter more than one value for the <i>type-number</i> argument.

tarp protocol-type

To specify the network protocol type to be used in outgoing TID Address Resolution Protocol (TARP) PDUs, use the **tarp protocol-type** command in global configuration mode. To set the protocol type to the default value, use the **no** form of this command.

tarp protocol-type *hex-digit*

no tarp protocol-type

Syntax Description	<i>hex-digit</i>	Two digits in hexadecimal format to be used to identify the protocol used in outgoing TARP PDUs. The default is FE (for CLNP).
---------------------------	------------------	--

tarp query

To determine a corresponding TID entry for a specific NSAP address, use the **tarp query** command in EXEC mode.

tarp query *nsap*

Syntax Description	<i>nsap</i>	NSAP address that you want the TID for. Use the full NSAP address.
---------------------------	-------------	--

tarp resolve

To determine an NSAP address corresponding to a specified TID, use the **tarp resolve** command in EXEC mode.

tarp resolve *tid* [**1** | **2**]

Syntax Description	<i>tid</i>	Target identifier to be mapped to the specified NSAP. Alphanumeric string up to 255 characters.
	1	(Optional) Send a Type 1 PDU. The default is a Type 1 PDU. If a response is not received before the timeout period, a Type 2 PDU is sent.
	2	(Optional) Send only Type 2 PDU.

tarp route-static

To configure a static TID Address Resolution Protocol (TARP) adjacency, use the **tarp route-static** command in global configuration mode. To remove a static TARP adjacency from the TARP queue, use the **no** form of this command.

```
tarp route-static nsap [all | message-type type-number [type-number] [type-number]]
```

```
no tarp route-static nsap [all | message-type type-number [type-number] [type-number]]
```

Syntax Description

<i>nsap</i>	NSAP address to create a static TARP adjacency. Use the full NSAP address.
all	(Optional) Specifies all TARP PDUs.
message-type <i>type-number</i>	(Optional) Specifies only type-number broadcast PDUs. Valid values are 1, 2, and 4. You may enter more than one value for the <i>type-number</i> argument.

tarp run

To start the TID Address Resolution Protocol (TARP) process on the router, use the **tarp run** command in global configuration mode. To stop the TARP process, use the **no** form of this command.

```
tarp run
```

```
no tarp run
```

Syntax Description

This command has no arguments or keywords.

tarp sequence-number

To specify the sequence number to be used in the next originated TID Address Resolution Protocol (TARP) PDU, use the **tarp sequence-number** command in global configuration mode. To return to the default value, use the **no** form of this command.

```
tarp sequence-number number
```

```
no tarp sequence-number number
```

Syntax Description

<i>number</i>	Number from 0 to 65,535 that will be used as the sequence number in the next originated PDU.
---------------	--

tarp t1-response-timer

To specify the length of time for which the router will wait for a response from a Type 1 PDU, use the **tarp t1-response-timer** command in global configuration mode. To set the timer to the default value, use the **no** form of this command.

tarp t1-response-timer *seconds*

no tarp t1-response-timer

Syntax Description	<i>seconds</i>	Number of seconds for which the router will wait to receive a response from a Type 1 PDU. The range is 0 to 3600 seconds.
---------------------------	----------------	---

tarp t2-response-timer

To specify the length of time for which the router will wait for a response from a Type 2 PDU, use the **tarp t2-response-timer** command in global configuration mode. To set the timer to the default value, use the **no** form of this command.

tarp t2-response-timer *seconds*

no tarp t2-response-timer

Syntax Description	<i>seconds</i>	Number of seconds for which the router will wait to receive a response from a Type 2 PDU. The range is 0 to 3600 seconds.
---------------------------	----------------	---

tarp tid

To assign a TID to the router, use the **tarp tid** command in global configuration mode. To remove the TID from the router, use the **no** form of this command.

tarp tid *tid*

no tarp tid *tid*

Syntax Description	<i>tid</i>	Target identifier to be used by this router. Alphanumeric string up to 255 characters.
---------------------------	------------	--

tarp urc

To set the update remote cache bit in all subsequent outgoing PDUs, use the **tarp urc** command in global configuration mode. To set the update remote cache bit to the default value, use the **no** form of this command.

tarp urc {0 | 1}

no tarp urc

Syntax Description	0	1
	Sets the update remote cache bit to 0, which is the default value. When the bit is zero, the receiver's PDU will update its TID cache entry.	Sets the update remote cache bit to 1. When the bit is 1, the receiver's TID cache is not updated.

timers basic (ISO CLNS)

To configure ISO IGRP timers, use the **timers basic** command in router configuration mode. To restore the default values, use the **no** form of this command.

timers basic *update-interval holddown-interval invalid-interval*

no timers basic *update-interval holddown-interval invalid-interval*

Syntax Description	<i>update-interval</i>	<i>holddown-interval</i>	<i>invalid-interval</i>
	Time, in seconds, between the sending of routing updates.	Time, in seconds, a system or area router is kept in holddown state, during which routing information regarding better paths is suppressed. (A router enters into a holddown state when an update packet is received that indicates the route is unreachable. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets.) When the holddown interval expires, routes advertised by other sources are accepted and the route is no longer inaccessible.	Time, in seconds, that a route remains in the routing table after it has been determined that it is not reachable. After that length of time, the route is removed from the routing table.

which-route

To determine which next-hop router will be used or to troubleshoot your configuration if you have multiple processes running, use the **which-route** command in EXEC mode. This command displays the routing table in which the specified CLNS destination is found.

```
which-route {nsap-address | clns-name}
```

Syntax Description

<i>nsap-address</i>	CLNS destination network address.
<i>clns-name</i>	Destination host name.



XNS Commands

This chapter describes the function and syntax of the Xerox Network Systems (XNS) commands. For more information about these commands, refer to the corresponding chapter of the *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference*.



Note

The XNS networking protocol will no longer be offered after Cisco IOS Release 12.2. XNS commands will not appear in future releases of the Cisco IOS software documentation set.



Note

Not all Cisco access servers support XNS. For more information, refer to the release notes for the release you are running.

access-list (XNS extended)

To define an extended XNS access list, use the extended version of the **access-list** command in global configuration mode. To remove an extended access list, use the **no** form of this command.

```
access-list access-list-number { deny | permit } protocol [source-network [.source-host  
[source-network-mask.source-host-mask]]] source-socket [destination-network  
[.destination-host [destination-network-mask.destination-host-mask]  
destination-socket[/pep]]]
```

```
no access-list access-list-number { deny | permit } protocol [source-network[.source-host  
[source-network-mask.source-host-mask]]] source-socket [destination-network  
[.destination-host [destination-network-mask.destination-host-mask]  
destination-socket[/pep]]]
```



Note

If network masks are used, all fields are required, except the destination socket and the destination Packet Exchange Protocol (PEP) type.

Syntax Description

<i>access-list-number</i>	Number of the access list. This is a decimal number from 500 to 599.
deny	Denies access if the conditions are matched.

permit	Permits access if the conditions are matched.
<i>protocol</i>	Number of an XNS protocol, in decimal. See the documentation accompanying your host's XNS implementation for a list of protocol numbers.
<i>source-network</i>	<p>(Optional) Number of the network from which the packet is being sent. This is a 32-bit decimal number. A network number of -1 matches all networks.</p> <p>You can omit leading zeros from the network number.</p> <p>Note that you enter the network number in decimal, and this number is expressed in decimal format in Cisco's configuration files and routing tables. However, Cisco IOS software internally converts the network number into hexadecimal. This means, for instance, that a network analyzer will display the network number in hexadecimal.</p>
<i>.source-host</i>	(Optional) Host on <i>source-network</i> from which the packet is being sent. This is a 48-bit hexadecimal value represented as a dotted triplet of 4-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>).
<i>source-network-mask</i>	(Optional) Mask to be applied to <i>source-network</i> . The mask is a 32-bit decimal number. The mask must immediately be followed by a period, which must in turn immediately be followed by <i>source-host-mask</i> .
<i>.source-host-mask</i>	(Optional) Mask to be applied to <i>source-host</i> . This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>). Place ones in the bit positions you want to mask.
<i>source-socket</i>	Number of the socket from which the packet is being sent. This is a 16-bit decimal value. See the documentation accompanying your host's XNS implementation for a list of socket numbers.
<i>destination-network</i>	<p>(Optional) Number of the network to which the packet is being sent. This is a 32-bit decimal number. A network number of -1 matches all networks.</p> <p>You can omit leading zeros from the network number.</p> <p>Note that you enter the network number in decimal, and this number is expressed in decimal format in Cisco's configuration files and routing tables. However, Cisco IOS software internally converts the network number into hexadecimal. This means, for instance, that a network analyzer will display the network number in hexadecimal.</p>
<i>.destination-host</i>	(Optional) Host on <i>destination-network</i> to which the packet is being sent. This is a 48-bit hexadecimal value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>).
<i>destination-network-mask</i>	(Optional) Mask to be applied to <i>destination-network</i> . The mask is a 32-bit decimal number. The mask must immediately be followed by a period, which must in turn immediately be followed by <i>destination-host-mask</i> .
<i>.destination-host-mask</i>	(Optional) Mask to be applied to <i>destination-host</i> . This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>). Place ones in the bit positions you want to mask.

<i>destination-socket</i>	(Optional) Number of the socket to which the packet is being sent. This is a 16-bit decimal value. See the documentation accompanying your host's XNS implementation for a list of socket numbers.
<i>/pep</i>	(Optional) Packet Exchange Protocol (PEP) type. PEP is a connectionless-oriented protocol that uses XNS Type 4 initial domain part (IDP) frames.

access-list (XNS standard)

To define a standard XNS 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-network [source-address
[source-address-mask]] [destination-network [destination-address
[destination-address-mask]]]
```

```
no access-list access-list-number
```

Syntax Description

<i>access-list-number</i>	Number of the access list. This is a decimal number from 400 to 499.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
<i>source-network</i>	Number of the network from which the packet is being sent. This is a 32-bit decimal number. You can omit leading zeros. A network number of -1 matches all networks. Note that you enter the network number in decimal, and this number is expressed in decimal format in Cisco's configuration files and routing tables. However, Cisco IOS software internally converts the network number into hexadecimal. This means, for instance, that a network analyzer will display the network number in hexadecimal.
<i>.source-address</i>	(Optional) Host on <i>source-network</i> from which the packet is being sent. This is a 48-bit hexadecimal value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>).
<i>source-address-mask</i>	(Optional) Mask to be applied to <i>source-address</i> . This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>). Place ones in the bit positions you want to mask.
<i>destination-network</i>	(Optional) Number of the network to which the packet is being sent. This is a 32-bit decimal number. A network number of -1 matches all networks. You can omit leading zeros from the network number. Note that you enter the network number in decimal, and this number is expressed in decimal format in Cisco's configuration files and routing tables. However, Cisco IOS software internally converts the network number into hexadecimal. This means, for instance, that a network analyzer will display the network number in hexadecimal.

<i>.destination-address</i>	(Optional) Host on <i>destination-network</i> to which the packet is being sent. This is a 48-bit hexadecimal value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>).
<i>destination-address-mask</i>	(Optional) Mask to be applied to <i>destination-address</i> . This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>). Place ones in the bit positions you want to mask.

show xns cache

To display the contents of the XNS fast-switching cache, use the **show xns cache** command in EXEC mode.

```
show xns cache
```

Syntax Description This command has no arguments or keywords.

show xns interface

To display the status of the XNS interfaces configured in Cisco IOS software and the parameters configured on each interface, use the **show xns interface** command in EXEC mode.

```
show xns interface [type number]
```

Syntax Description	<i>type</i>	(Optional) Interface type. It can be one of the following types: asynchronous, dialer, Ethernet (IEEE 802.3), loopback, null, serial, or tunnel.
	<i>number</i>	(Optional) Interface number.

show xns route

To display the contents of the XNS routing table, use the **show xns route** command in EXEC mode.

```
show xns route [network]
```

Syntax Description	<i>network</i>	(Optional) Number of the network that the route is to. This is a 32-bit decimal number. You can omit leading zeros.
---------------------------	----------------	---

show xns traffic

To display information about the number and type of XNS packets transmitted and received by Cisco IOS software, use the **show xns traffic** command in EXEC mode.

```
show xns traffic
```

Syntax Description This command has no arguments or keywords.

xns access-group

To apply a generic filter to an interface, use the **xns access-group** command in interface configuration mode. To remove the access list, use the **no** form of this command.

```
xns access-group access-list-number
```

```
no xns access-group access-list-number
```

Syntax Description	<i>access-list-number</i>	Number of the access list. All outgoing packets defined with either standard or extended access lists and forwarded through the interface are filtered by the entries in this access list. For standard access lists, <i>access-list-number</i> is a decimal number from 400 to 499. For extended access lists, <i>access-list-number</i> is a decimal number from 500 to 599.
---------------------------	---------------------------	--

xns encapsulation

To select the type of encapsulation used on a Token Ring interface, use the **xns encapsulation** command in interface configuration mode. To disable the encapsulation, use the **no** form of this command.

```
xns encapsulation {snap | ub | 3com}
```

```
no xns encapsulation {snap | ub | 3com}
```

Syntax Description	snap	802.2 LLC encapsulation. This is the default encapsulation type. Use this encapsulation type with IBM Token Ring networks.
	ub	Ungermann-Bass encapsulation.
	3com	3Com encapsulation. Use this encapsulation type when older 3Com Corporation products are present on the network.

xns flood broadcast allnets

To flood broadcast packets whose destination address is -1.FFFF.FFFF.FFFF, use the **xns flood broadcast allnets** command in interface configuration mode. To disable this type of flooding, use the **no** form of this command.

xns flood broadcast allnets

no xns flood broadcast allnets

Syntax Description This command has no arguments or keywords.

xns flood broadcast net-zero

To flood packets whose destinations address is 0.FFFF.FFFF.FFFF, use the **xns flood broadcast net-zero** command in interface configuration mode. To disable this type of flooding, use the **no** form of this command.

xns flood broadcast net-zero

no xns flood broadcast net-zero

Syntax Description This command has no arguments or keywords.

xns flood specific allnets

To flood packets whose destination address is -1.*specific-host*, use the **xns flood specific allnets** command in interface configuration mode. To disable this type of flooding, use the **no** form of this command.

xns flood specific allnets

no xns flood specific allnets

Syntax Description This command has no arguments or keywords.

xns forward-protocol

To forward packets of a specific XNS protocol to a helper address, use the **xns forward-protocol** command in global configuration mode. To disable the forwarding of these packets, use the **no** form of this command.

xns forward-protocol *protocol*

no xns forward-protocol *protocol*

Syntax Description

protocol

Number of an XNS protocol, in decimal. See the documentation accompanying your host's XNS implementation for a list of protocol numbers.

xns hear-rip

To receive Routing Information Protocol (RIP) updates, use the **xns hear-rip** command in interface configuration mode. To disable the receipt of RIP updates, use the **no** form of this command.

xns hear-rip [*access-list-number*]

no xns hear-rip

Syntax Description

access-list-number

(Optional) Number of the access list. This list defines the routes Cisco IOS software is to learn through standard RIP. The list is applied to individual routes within the RIP packet, not to the address of the packet's sender. For standard access lists, *access-list-number* is a decimal number from 400 to 499. For extended access lists, *access-list-number* is a decimal number from 500 to 599.

xns helper-address

To forward broadcast packets to a specified server, use the **xns helper-address** command in interface configuration mode. To disable this function, use the **no** form of this command.

xns helper-address *network.host*

no xns helper-address *network.host*

Syntax Description

network

Network on which the target XNS server resides. This is a 32-bit decimal number.

.host

Host number of the target XNS server. This is a 48-bit hexadecimal value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). The host must be directly connected to one of the router's directly attached networks. A number of FFFF.FFFF.FFFF indicates all hosts on the specified network.

xns input-network-filter

To control which networks are added to the routing table, use the **xns input-network-filter** command in interface configuration mode. To remove the filter from the interface, use the **no** form of this command.

xns input-network-filter *access-list-number*

no xns input-network-filter *access-list-number*

Syntax Description	<i>access-list-number</i>	Number of the access list. All incoming packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, <i>access-list-number</i> is a decimal number from 400 to 499. For extended access lists, it is a decimal number from 500 to 599.
---------------------------	---------------------------	---

xns maximum-paths

To set the maximum number of paths that Cisco IOS software uses when sending packets, use the **xns maximum-paths** command in global configuration mode. To restore the default value, use the **no** form of this command.

xns maximum-paths *number*

no xns maximum-paths

Syntax Description	<i>number</i>	Maximum number of equal-cost paths from which the software chooses. It can be a number from 1 to 512. The default is 1.
---------------------------	---------------	---

xns network

To enable XNS routing on a particular interface by assigning a network number to the interface, use the **xns network** command in interface configuration mode. To disable XNS routing on an interface, use the **no** form of this command.

xns network *number*

no xns network

Syntax Description	<i>number</i>	Network number. This is a 32-bit decimal number. You can omit leading zeros.
---------------------------	---------------	--

xns output-network-filter

To control the list of networks included in routing updates sent out an interface, use the **xns output-network-filter** command in interface configuration mode. To remove the filter from the interface, use the **no** form of this command.

xns output-network-filter *access-list-number*

no xns output-network-filter *access-list-number*

Syntax Description	<i>access-list-number</i>	Number of the access list. All outgoing packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, the access-list-number is a decimal number from 400 to 499. For extended access lists, it is a decimal number from 500 to 599.
---------------------------	---------------------------	--

xns route

To add a static route to the XNS routing table, use the **xns route** command in global configuration mode. To remove a route from the routing table, use the **no** form of this command.

xns route *network network.host*

no xns route *network network.host*

Syntax Description	<i>network</i>	Network to which you want to establish a static route. This is a 32-bit decimal number. You can omit leading zeros.
	<i>network.host</i>	Router to which to forward packets destined for the specified network. The argument <i>network</i> is a 32-bit decimal number. You can omit leading zeros. The argument <i>host</i> is the host number of the target router. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxx.xxxx.xxx</i>).

xns route-cache

To enable XNS fast switching, use the **xns route-cache** command in interface configuration mode. To disable fast switching, use the **no** form of this command.

xns route-cache

no xns route-cache

Syntax Description	This command has no arguments or keywords.
---------------------------	--

xns router-filter

To control the routers from which packets are accepted, use the **xns router-filter** command in interface configuration mode. To remove the filters from the interface, use the **no** form of this command.

xns router-filter *access-list-number*

no xns router-filter *access-list-number*

Syntax Description	<i>access-list-number</i>	Number of the access list. All incoming packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, <i>access-list-number</i> is a decimal number from 400 to 499. For extended access lists, it is a decimal number from 500 to 599.
---------------------------	---------------------------	---

xns routing

To enable XNS routing, use the **xns routing** command in global configuration mode. To disable XNS routing, use the **no** form of this command.

xns routing [*address*]

no xns routing

Syntax Description	<i>address</i>	(Optional) Host number of the router. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (<i>xxxx.xxxx.xxxx</i>). It must not be a multicast address. If you omit <i>address</i> , Cisco IOS software uses the address of the first IEEE-compliant (Token Ring, FDDI, or Ethernet) interface MAC address it finds in its interface list. The software uses the address 0123.4567.abcd for non-IEEE-compliant interfaces.
---------------------------	----------------	---

xns ub-emulation

To enable Ungermann-Bass Net/One routing, use the **xns ub-emulation** command in global configuration mode. To disable Net/One routing and restore standard routing mode, use the **no** form of this command.

xns ub-emulation

no xns ub-emulation

Syntax Description	This command has no arguments or keywords.
---------------------------	--

xns update-time

To set the XNS routing update timers, use the **xns update-time** command in interface configuration mode. To restore the default value, use the **no** form of this command.

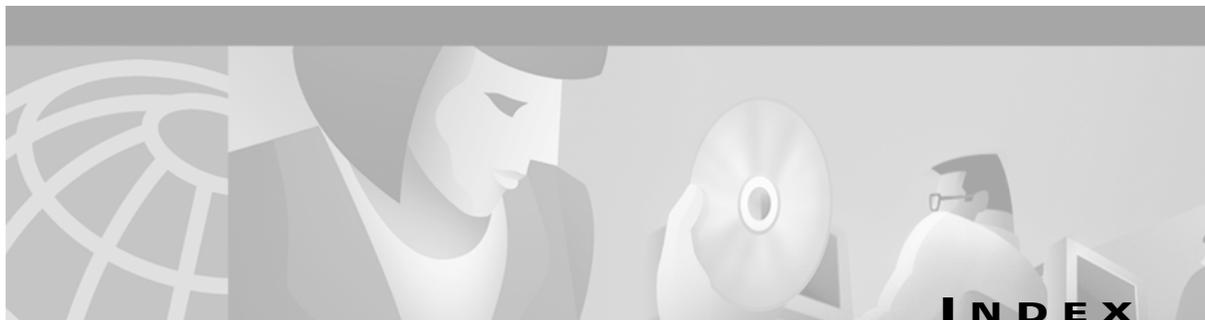
xns update-time *interval*

no xns update-time

Syntax Description	<i>interval</i>	Interval, in seconds, at which XNS routing updates are sent. The minimum interval is 10 seconds, and the maximum is 2493644 seconds, which is about 29 days. The default is 30 seconds.
---------------------------	-----------------	---



Index



BC	Cisco IOS Bridging and IBM Networking Configuration Guide
CS1	Cisco IOS Command Summary, Volume 1 of 3
CS2	Cisco IOS Command Summary, Volume 2 of 3
CS3	Cisco IOS Command Summary, Volume 3 of 3
DC	Cisco IOS Dial Technologies Configuration Guide
FC	Cisco IOS Configuration Fundamentals Configuration Guide
IC	Cisco IOS Interface Configuration Guide
IPC	Cisco IOS IP Routing Configuration Guide
MWC	Cisco IOS Mobile Wireless Configuration Guide
P2C	Cisco IOS AppleTalk and Novell IPX Configuration Guide
P3C	Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide
QC	Cisco IOS Quality of Service Solutions Configuration Guide
SC	Cisco IOS Security Configuration Guide
TC	Cisco IOS Terminal Services Configuration Guide
VC	Cisco IOS Voice, Video, and Fax Configuration Guide
WC	Cisco IOS Wide-Area Networking Configuration Guide
XC	Cisco IOS Switching Services Configuration Guide

Symbols

? command **xviii**

A

aaa authorization ipmobile command **CS1-287**
absolute command **CS1-93**
access-class command **CS1-241**
access-list additional-zones command **CS1-477**
access-list cable-range command **CS1-477**
access-list command
 IP
 extended **CS1-241, CS1-247, CS1-250**
 standard **CS1-245**
access-list compiled command **CS1-246**

access-list (connect initiate) command
 DECnet **CS1-614**
access-list (DECnet extended) command **CS1-613**
access-list (DECnet standard) command **CS1-615**
access-list includes command **CS1-478**
access-list (IPX extended) command **CS1-515**
access-list (IPX standard) command **CS1-517**
access-list nbp command **CS1-478**
access-list network command **CS1-479**
access-list (NLSP) command **CS1-518**
access-list other-access command **CS1-480**
access-list other-nbps command **CS1-480**
access-list remark command **CS1-246**
access-list within command **CS1-480**
access-list (XNS extended) command **CS1-673**
access-list (XNS standard) command **CS1-675**
access-list zone command **CS1-481**
activation-character command **CS1-13, CS1-127**
address-family ipv4 command **CS1-391**
address-family vpnv4 command **CS1-392**
advertise command **CS1-275**
agent command **CS1-275**
aggregate-address command **CS1-357**
alias command **CS1-93**
apollo access-group command **CS1-591**
apollo access-list command **CS1-591**
apollo maximum-paths command **CS1-592**
apollo network command **CS1-592**
apollo route command **CS1-593**
apollo routing command **CS1-593**
apollo update-time command **CS1-593**
appletalk access-group command **CS1-481**
appletalk address command **CS1-482**
appletalk alternate-addressing command **CS1-482**
appletalk arp interval command **CS1-482**

- appletalk arp retransmit-count command **CS1-483**
 appletalk arp-timeout command **CS1-483**
 appletalk aurp tickle-time command **CS1-484**
 appletalk cable-range command **CS1-484**
 appletalk checksum command **CS1-485**
 appletalk client-mode command **CS1-485**
 appletalk discovery command **CS1-485**
 appletalk distribute-list in command **CS1-486**
 appletalk distribute-list out command **CS1-486**
 appletalk domain hop-reduction command **CS1-487**
 appletalk domain name command **CS1-487**
 appletalk domain remap-range command **CS1-487**
 appletalk domain-group command **CS1-486**
 appletalk eigrp active-time command **CS1-488**
 appletalk eigrp log-neighbor-changes command **CS1-489**
 appletalk eigrp split-horizon command **CS1-489**
 appletalk eigrp-bandwidth-percent command **CS1-488**
 appletalk eigrp-timers command **CS1-489**
 appletalk event-logging command **CS1-490**
 appletalk free-trade-zone command **CS1-490**
 appletalk getzonelist-filter command **CS1-490**
 appletalk glean-packets command **CS1-491**
 appletalk ignore-verify-errors command **CS1-491**
 appletalk iptalk command **CS1-491**
 appletalk iptalk-baseport command **CS1-492**
 appletalk lookup-type command **CS1-492**
 appletalk macip server command **CS1-493**
 appletalk macip static command **CS1-494**
 appletalk maximum-paths command **CS1-494**
 appletalk name-lookup interval command **CS1-495**
 appletalk permit-partial-zones command **CS1-495**
 appletalk pre-fdditalk command **CS1-495**
 appletalk protocol command **CS1-496**
 appletalk proxy-npb command **CS1-496**
 appletalk require-route-zones command **CS1-497**
 appletalk route-cache command **CS1-497**
 appletalk route-redistribution command **CS1-497**
 appletalk routing command **CS1-498**
 appletalk rtmp jitter command **CS1-498**
 appletalk rtmp-stub command **CS1-498**
 appletalk send-rtmps command **CS1-499**
 appletalk static cable-range command **CS1-499**
 appletalk static network command **CS1-499**
 appletalk strict-rtmp-checking command **CS1-500**
 appletalk timers command **CS1-500**
 appletalk virtual-net command **CS1-501**
 appletalk zip-reply-filter command **CS1-501**
 appletalk zone command **CS1-502**
 area authentication command **CS1-315**
 area default-cost command **CS1-315**
 area filter-list command **CS1-316**
 area nssa command **CS1-316**
 area range command **CS1-316**
 area stub command **CS1-317**
 area virtual-link command **CS1-317**
 area-address command **CS1-519**
 area-password command **CS1-345**
 arp arpa command **CS1-203**
 arp command **CS1-203**
 arp frame-relay command **CS1-203**
 arp probe command **CS1-203**
 arp snap command **CS1-203**
 arp timeout command **CS1-204**
 async-bootp command **CS1-83**
 attach command **CS1-113**
 autobaud command **CS1-13**
 auto-cost command **CS1-319**
 auto-summary (BGP) command **CS1-358**
 auto-summary (Enhanced IGRP) command **CS1-335**
 auto-summary (RIP) command **CS1-301**
-
- B**
 banner exec command **CS1-33**
 banner incoming command **CS1-34**
 banner login command **CS1-34**
 banner motd command **CS1-34**
 beacon command **CS1-467**

- bgp always-compare-med command **CS1-358**
 - bgp bestpath compare-routerid command **CS1-359**
 - bgp bestpath med confed command **CS1-359**
 - bgp bestpath missing-as-worst command **CS1-359**
 - bgp client-to-client reflection command **CS1-360**
 - bgp cluster-id command **CS1-360**
 - bgp confederation identifier command **CS1-360**
 - bgp confederation peers command **CS1-361**
 - bgp dampening command **CS1-361**
 - bgp default ipv4-unicast command **CS1-362**
 - bgp default local-preference command **CS1-362**
 - bgp deterministic med command **CS1-362**
 - bgp fast-external-fallover command **CS1-363**
 - bgp log-neighbor-changes command **CS1-363**
 - bgp redistribute-internal command **CS1-363**
 - bgp router-id command **CS1-364**
 - bindid command **CS1-276**
 - boot bootldr command **CS1-77**
 - boot bootstrap command **CS1-77**
 - boot buffersize command **CS1-57**
 - boot command **CS1-75**
 - boot config command **CS1-57**
 - boot flash command **CS1-75**
 - boot host command **CS1-58**
 - boot network command **CS1-58**
 - boot registers **CS1-79, CS1-80**
 - boot system command **CS1-77**
 - bootfile command **CS1-227**
 - buckets-of-history-kept command **CS1-169**
 - buffers command **CS1-94**
 - buffers huge size command **CS1-94**
-
- C**
- cd command **CS1-48**
 - cdp advertise-v2 command **CS1-157**
 - cdp enable command **CS1-157**
 - cdp holdtime command **CS1-158**
 - cdp run command **CS1-158**
 - cdp timer command **CS1-158**
 - clear access-list counters command **CS1-246**
 - clear appletalk arp command **CS1-503**
 - clear appletalk neighbor command **CS1-503**
 - clear appletalk route command **CS1-504**
 - clear appletalk traffic command **CS1-504**
 - clear arp-cache command **CS1-204**
 - clear cdp counters command **CS1-158**
 - clear cdp table command **CS1-159**
 - clear clns cache command **CS1-633**
 - clear clns es-neighbors command **CS1-633**
 - clear clns is-neighbors command **CS1-633**
 - clear clns neighbors command **CS1-634**
 - clear clns route command **CS1-634**
 - clear clns traffic command **CS1-634**
 - clear decnet accounting command **CS1-616**
 - clear decnet counters command **CS1-616**
 - clear host command **CS1-204**
 - clear ip accounting command **CS1-246**
 - clear ip bgp command **CS1-364**
 - clear ip bgp dampening command **CS1-364**
 - clear ip bgp external command **CS1-365**
 - clear ip bgp flap-statistics command **CS1-365**
 - clear ip bgp peer-group command **CS1-365**
 - clear ip cgmp command **CS1-415**
 - clear ip dhcp binding command **CS1-227**
 - clear ip dhcp conflict command **CS1-228**
 - clear ip dhcp server statistics command **CS1-228**
 - clear ip drp command **CS1-247**
 - clear ip dvmrp route command **CS1-415**
 - clear ip eigrp neighbors command **CS1-335, CS1-415**
 - clear ip igmp group command **CS1-415**
 - clear ip mobile binding command **CS1-287**
 - clear ip mobile secure command **CS1-288**
 - clear ip mobile traffic command **CS1-288**
 - clear ip mobile visitor command **CS1-288**
 - clear ip mrm status-report command **CS1-467**
 - clear ip msdp peer command **CS1-447**
 - clear ip msdp sa-cache command **CS1-447**

- clear ip msdp statistics command **CS1-448**
- clear ip nat translation command **CS1-205**
- clear ip nhrp command **CS1-205**
- clear ip ospf command **CS1-319**
- clear ip peer-group command **CS1-366**
- clear ip pgm host command **CS1-457**
- clear ip pgm router command **CS1-457**
- clear ip pim auto-rp command **CS1-416**
- clear ip route command **CS1-205**
- clear ip rtp header-compression command **CS1-416**
- clear ip sap command **CS1-417**
- clear ip sdr command **CS1-417**
- clear ip slb command **CS1-276**
- clear ip sse command **CS1-247**
- clear ipx accounting command **CS1-519**
- clear ipx cache command **CS1-520**
- clear ipx nhrp command **CS1-520**
- clear ipx nlsip neighbors command **CS1-520**
- clear ipx route command **CS1-520, CS1-521**
- clear ipx traffic command **CS1-522**
- clear logging command **CS1-113**
- clear parser cache command **CS1-58**
- clear smrp mcache command **CS1-504**
- clear tarp counters command **CS1-635**
- clear tarp ldb-table command **CS1-635**
- clear tarp tid-table command **CS1-635**
- clear tcp command **CS1-35**
- clear tcp statistics command **CS1-247**
- clear vines cache command **CS1-595**
- clear vines ipc command **CS1-596**
- clear vines neighbor command **CS1-596**
- clear vines route command **CS1-596**
- clear vines traffic command **CS1-596**
- client command **CS1-276**
- client-identifier command **CS1-228**
- client-name command **CS1-229**
- clns access-group command **CS1-635**
- clns adjacency-filter command **CS1-636**
- clns cache-invalidate-delay command **CS1-636**
- clns checksum command **CS1-636**
- clns cluster-alias command **CS1-637**
- clns configuration-time command **CS1-637**
- clns congestion-threshold command **CS1-637**
- clns dec-compatible command **CS1-638**
- clns enable command **CS1-638**
- clns erpdu-interval command **CS1-638**
- clns esct-time command **CS1-639**
- clns es-neighbor command **CS1-639**
- clns filter-expr command **CS1-639**
- clns filter-set command **CS1-640**
- clns holding-time command **CS1-640**
- clns host command **CS1-641**
- clns is-neighbor command **CS1-641**
- clns mtu command **CS1-641**
- clns net (global) command **CS1-642**
- clns net (interface) command **CS1-642**
- clns packet-lifetime command **CS1-642**
- clns rdpdu-interval command **CS1-643**
- clns route (create) command **CS1-643**
- clns route default command **CS1-644**
- clns route discard command **CS1-645**
- clns route (enter) command **CS1-643**
- clns route-cache command **CS1-644**
- clns router isis command **CS1-645**
- clns router iso-igrp command **CS1-645**
- clns routing command **CS1-646**
- clns security-passthrough command **CS1-646**
- clns send-erpdu command **CS1-646**
- clns send-rdpdu command **CS1-647**
- clns split-horizon command **CS1-647**
- clns template-alias command **CS1-647**
- clns want-erpdu command **CS1-648**
- clock calendar-valid command **CS1-95**
- clock read-calendar command **CS1-95**
- clock set command **CS1-95**
- clock summer-time command **CS1-96**
- clock ticks, IPX **CS1-534**
- clock timezone command **CS1-96**

clock update-calendar command **CS1-97**
 compatible rfc 1583 command **CS1-319**
 config-register command **CS1-79**
 configure command **CS1-59**
 configure network command **CS1-48**
 configure overwrite-network command **CS1-59**
 confreg command **CS1-80**
 continue command **CS1-80**
 copy command **CS1-49**
 copy erase flash command
 See erase flash command
 copy running-config startup-config command **CS1-49**
 copy startup-config running-config command **CS1-49**
 copy verify bootflash command **CS1-64**
 copy verify command
 See verify command
 copy verify flash command **CS1-65**
 See verify command
 copy xmodem command **CS1-65**
 copy ymodem command **CS1-65**
 ctunnel destination command **CS1-648**

D

databits command **CS1-14**
 data-character-bits command **CS1-14**
 data-pattern command **CS1-169**
 decnet access-group command **CS1-616**
 decnet accounting command **CS1-617**
 decnet accounting list command **CS1-617**
 decnet accounting threshold command **CS1-617**
 decnet accounting transits command **CS1-618**
 decnet advertise command **CS1-618**
 decnet area-max-cost command **CS1-618**
 decnet area-max-hops command **CS1-619**
 decnet congestion-threshold command **CS1-620**
 decnet conversion command **CS1-620**
 decnet cost command **CS1-620**
 decnet encapsulation command **CS1-621**
 decnet hello-timer command **CS1-621**
 decnet host command **CS1-621**
 decnet in-routing-filter command **CS1-622**
 decnet map command **CS1-622**
 decnet max-address command **CS1-622**
 decnet max-area command **CS1-623**
 decnet max-cost command **CS1-623**
 decnet max-hops command **CS1-623**
 decnet max-paths command **CS1-623**
 decnet max-visits command **CS1-624**
 decnet multicast-map command **CS1-624**
 decnet node-type command **CS1-625**
 decnet out-routing-filter command **CS1-625**
 decnet path-split-mode command **CS1-625**
 decnet propagate static command **CS1-626**
 decnet route default (interface default route)
 command **CS1-627**
 decnet route default (specific default route)
 command **CS1-627**
 decnet route (interface static route) command **CS1-626**
 decnet route (specific static route) command **CS1-627**
 decnet route-cache command **CS1-628**
 decnet router-priority command **CS1-628**
 decnet routing command **CS1-628**
 decnet routing-timer command **CS1-629**
 decnet split-horizon command **CS1-629**
 default-information (Enhanced IGRP) command **CS1-336**
 default-information originate (BGP) command **CS1-366,**
 CS1-388
 default-information originate (IS-IS) command **CS1-345**
 default-information originate (OSPF) command **CS1-320**
 default-information originate (RIP) command **CS1-301**
 default-metric (BGP) command **CS1-366**
 default-metric (Enhanced IGRP) command **CS1-336**
 default-metric (OSPF) command **CS1-320**
 default-metric (RIP) command **CS1-302**
 default-router command **CS1-229**
 default-value exec-character-bits command **CS1-14**
 default-value special-character-bits command **CS1-15**
 delay (virtual server) command **CS1-277**

delete command **CS1-49**

deny command

- IPX
 - NLSP **CS1-523**
 - SAP filtering **CS1-524**
 - standard **CS1-525**

deny (extended) command **CS1-522**

deny (IP) command **CS1-247**

deny (NLSP) command **CS1-523**

deny (SAP filtering) command **CS1-524**

deny (standard) command **CS1-525**

diag command **CS1-114**

dir command **CS1-49**

disable command **CS1-3**

disconnect-character command **CS1-15**

dispatch-character command **CS1-15**

dispatch-machine command **CS1-16**

dispatch-timeout command **CS1-16**

distance bgp command **CS1-366**

distance command **CS1-396**

distance eigrp command **CS1-337**

distance (ISO CLNS) command **CS1-648**

distance mbgp command

- See* distance bgp command

distance ospf command **CS1-320**

distribute-list in command **CS1-367, CS1-396**

distribute-list in (IPX) command **CS1-525**

distribute-list out command **CS1-367, CS1-397**

distribute-list out (IPX) command **CS1-526**

distribute-sap-list in command **CS1-527**

distribute-sap-list out command **CS1-527**

distributions-of-statistics-kept command **CS1-170**

dns-server **CS1-229**

dns-server command **CS1-229**

domain-name command **CS1-230**

domain-password command **CS1-346**

downward-compatible-config command **CS1-97**

dynamic command **CS1-250**

E

editing command **CS1-3**

eigrp log-neighbor-changes command **CS1-337**

eigrp log-neighbor-warnings command **CS1-337**

eigrp stub command **CS1-338**

enable command **CS1-4**

end command **CS1-4**

erase bootflash command

- See* erase command

erase command **CS1-50**

erase flash command **CS1-65**

erase start-up config command

- See* erase command

escape-character command **CS1-16**

exception core-file command **CS1-114**

exception dump command **CS1-115**

exception linecard command **CS1-115**

exception memory command **CS1-116**

exception protocol command **CS1-116**

exception spurious-interrupt command **CS1-117**

exec command **CS1-35**

exec-banner command **CS1-33, CS1-34**

exec-character-bits command **CS1-17**

exec-timeout command **CS1-36**

execute-on command **CS1-117**

exit command **CS1-4**

F

faildetect command **CS1-277**

file compression **CS1-59**

file prompt command **CS1-50**

filter-for-history command **CS1-170**

filtering output, show and more commands **xxii**

format command **CS1-50**

forwarding-agent command **CS1-253**

frame-relay ip rtp header-compression command **CS1-417**

frame-relay map ip compress command **CS1-418**

frame-relay map ip nocompress command **CS1-418**
 frame-relay map ip rtp header-compression
 command **CS1-418**
 frequency (RTR) command **CS1-170**
 fsck command **CS1-51**
 full-help command **CS1-5**

H

hardware-address command **CS1-230**
 help command **xviii, CS1-5**
 help, user-level commands **CS1-5**
 history command **CS1-5**
 history size command **CS1-5**
 hold-character command **CS1-17**
 hops-of-statistics-kept command **CS1-171**
 host command **CS1-230**
 hostname command **CS1-97**
 hours-of-statistics-kept command **CS1-171**
 http-raw-request command **CS1-171**

I

idle command **CS1-277**
 ignore lsa mospf command **CS1-321**
 ignore-lsp-errors command **CS1-649**
 import all command **CS1-231**
 input-queue command **CS1-302**
 insecure command **CS1-17**
 inservice (real server) command **CS1-278**
 inservice (virtual server) command **CS1-278**
 interface ctunnel command **CS1-649**
 international command **CS1-43**
 ip access-group command **CS1-253**
 ip access-list command **CS1-253**
 ip accounting command **CS1-254**
 ip accounting-list command **CS1-254**
 ip accounting-threshold command **CS1-254**
 ip accounting-transits command **CS1-255**

ip address command **CS1-206**
 ip address dhcp command **CS1-231**
 ip as-path access-list command **CS1-368**
 ip authentication key-chain eigrp command **CS1-338**
 ip authentication mode eigrp command **CS1-338**
 ip bandwidth-percent eigrp command **CS1-339**
 ip bgp-community new-format command **CS1-368**
 ip bootp server command **CS1-97**
 ip broadcast-address command **CS1-206**
 ip casa command **CS1-255**
 ip cef traffic-statistics command **CS1-206**
 ip cgmp command **CS1-419**
 ip classless command **CS1-207**
 ip community-list command **CS1-369**
 ip default-gateway command **CS1-207**
 ip default-network command **CS1-397**
 ip dhcp conflict logging command **CS1-231**
 ip dhcp database command **CS1-232**
 ip dhcp excluded-address command **CS1-232**
 ip dhcp ping packets command **CS1-233**
 ip dhcp ping timeout command **CS1-233**
 ip dhcp pool command **CS1-233**
 ip dhcp relay information check command **CS1-234**
 ip dhcp relay information option command **CS1-234**
 ip dhcp relay information policy command **CS1-234**
 ip dhcp smart-relay command **CS1-235**
 ip directed-broadcast command **CS1-207**
 ip domain-list command **CS1-208**
 ip domain-lookup command **CS1-208**
 ip domain-lookup nsap command **CS1-649**
 ip domain-name command **CS1-208**
 ip drp access-group command **CS1-255**
 ip drp authentication key-chain command **CS1-256**
 ip drp server command **CS1-256**
 ip dvmrp accept-filter command **CS1-419**
 ip dvmrp auto-summary command **CS1-420**
 ip dvmrp default-information command **CS1-420**
 ip dvmrp metric command **CS1-392, CS1-420**
 ip dvmrp metric-offset command **CS1-421**

- ip dvmrp output-report-delay command **CS1-421**
- ip dvmrp reject-non-pruners command **CS1-422**
- ip dvmrp routehog-notification command **CS1-422**
- ip dvmrp route-limit command **CS1-422**
- ip dvmrp summary-address command **CS1-423**
- ip dvmrp unicast-routing command **CS1-423**
- ip finger command **CS1-98**
- ip forward-protocol any-local-broadcast command **CS1-209**
- ip forward-protocol command **CS1-209**
- ip forward-protocol spanning-tree command **CS1-209**
- ip forward-protocol turbo-flood command **CS1-210**
- ip ftp passive command **CS1-84**
- ip ftp password command **CS1-85**
- ip ftp source-interface command **CS1-85**
- ip ftp username command **CS1-85**
- ip hello-interval eigrp command **CS1-339**
- ip helper-address command **CS1-210**
- ip hold-time eigrp command **CS1-339**
- ip host command **CS1-210**
- ip hp-host command **CS1-211**
- ip http access-class command **CS1-43**
- ip http authentication command **CS1-44**
- ip http port command **CS1-44**
- ip http server command **CS1-44**
- ip icmp rate-limit unreachable command **CS1-256**
- ip igmp access-group command **CS1-423**
- ip igmp helper-address command **CS1-424, CS1-463**
- ip igmp join-group command **CS1-424**
- ip igmp mroute-proxy command **CS1-463**
- ip igmp proxy-service command **CS1-464**
- ip igmp query-interval command **CS1-424**
- ip igmp query-max-response-time command **CS1-425**
- ip igmp query-timeout command **CS1-425**
- ip igmp static-group command **CS1-425**
- ip igmp unidirectional-link command **CS1-464**
- ip igmp v3lite command **CS1-426**
- ip irdp command **CS1-211**
- ip irdp holdtime command **CS1-211**
- ip irdp maxadvertinterval command **CS1-211**
- ip irdp multicast command **CS1-211**
- ip local policy route-map command **CS1-397**
- ip mask-reply command **CS1-257**
- ip mobile arp command **CS1-212**
- ip mobile foreign-agent command **CS1-288**
- ip mobile foreign-service command **CS1-289**
- ip mobile homeagent address command **CS1-290**
- ip mobile home-agent command **CS1-289**
- ip mobile homeagent standby command **CS1-290**
- ip mobile host command **CS1-291**
- ip mobile prefix-length command **CS1-291**
- ip mobile registration-lifetime command **CS1-291**
- ip mobile secure command **CS1-292**
- ip mobile tunnel command **CS1-292**
- ip mobile virtual-network command **CS1-293**
- ip mrm accept-manager command **CS1-468**
- ip mrm command **CS1-468**
- ip mrm manager command **CS1-468**
- ip mroute command **CS1-426**
- ip msdp border command **CS1-448**
- ip msdp cache-sa-state command **CS1-448**
- ip msdp default-peer command **CS1-449**
- ip msdp description command **CS1-449**
- ip msdp filter-sa-request command **CS1-449**
- ip msdp mesh-group command **CS1-450**
- ip msdp originator-id command **CS1-450**
- ip msdp peer command **CS1-450**
- ip msdp redistribute command **CS1-451**
- ip msdp sa-filter in command **CS1-451**
- ip msdp sa-filter out command **CS1-452**
- ip msdp sa-request command **CS1-453**
- ip msdp shutdown command **CS1-453**
- ip msdp ttl-threshold command **CS1-453**
- ip mtu command **CS1-257**
- ip multicast boundary command **CS1-427**
- ip multicast cache-headers command **CS1-393, CS1-427**
- ip multicast default-rpf-distance command **CS1-464**
- ip multicast heartbeat command **CS1-428**

- ip multicast helper-map command **CS1-428**
- ip multicast multipath command **CS1-429**
- ip multicast rate-limit command **CS1-429**
- ip multicast ttl-threshold command **CS1-430**
- ip multicast use-functional command **CS1-430**
- ip name-server command **CS1-212**
- ip nat command **CS1-213**
- ip nat inside destination command **CS1-213**
- ip nat inside source command **CS1-213**
- ip nat outside source command **CS1-214**
- ip nat pool command **CS1-215**
- ip nat service skinny tcp port command **CS1-215**
- ip nat translation command **CS1-215**
- ip netmask-format command **CS1-216**
- ip nhrp authentication command **CS1-217**
- ip nhrp holdtime command **CS1-217**
- ip nhrp interest command **CS1-217**
- ip nhrp map command **CS1-218**
- ip nhrp map multicast command **CS1-218**
- ip nhrp max-send command **CS1-218**
- ip nhrp network-id command **CS1-219**
- ip nhrp nhs command **CS1-219**
- ip nhrp record command **CS1-219**
- ip nhrp responder command **CS1-220**
- ip nhrp server-only command **CS1-220**
- ip nhrp trigger-svc command **CS1-220**
- ip nhrp use command **CS1-221**
- ip ospf authentication command **CS1-321**
- ip ospf authentication-key command **CS1-321**
- ip ospf cost command **CS1-322**
- ip ospf database-filter all out command **CS1-322**
- ip ospf dead-interval command **CS1-322**
- ip ospf demand-circuit command **CS1-323**
- ip ospf flood-reduction command **CS1-323**
- ip ospf hello-interval command **CS1-323**
- ip ospf message-digest-key command **CS1-324**
- ip ospf mtu-ignore command **CS1-324**
- ip ospf name-lookup command **CS1-324**
- ip ospf network command **CS1-324**
- ip ospf priority command **CS1-325**
- ip ospf retransmit-interval command **CS1-325**
- ip ospf transmit-delay command **CS1-326**
- ip pgm host command **CS1-458**
- ip pgm router command **CS1-460**
- ip pim accept-rp command **CS1-431**
- ip pim border command **CS1-431**
- ip pim bsr-border command **CS1-431**
- ip pim bsr-candidate command **CS1-431**
- ip pim command **CS1-430**
- ip pim message-interval command **CS1-432**
- ip pim minimum-vc-rate command **CS1-432**
- ip pim multipoint-signalling command **CS1-433**
- ip pim nbma-mode command **CS1-433**
- ip pim neighbor-filter command **CS1-433**
- ip pim query-interval command **CS1-434**
- ip pim register-rate-limit command **CS1-434**
- ip pim register-source command **CS1-434**
- ip pim rp-address command **CS1-435**
- ip pim rp-announce-filter command **CS1-435**
- ip pim rp-candidate command **CS1-435**
- ip pim send-rp-announce command **CS1-436**
- ip pim send-rp-discovery command **CS1-437**
- ip pim spt-threshold command **CS1-437**
- ip pim ssm command **CS1-437**
- ip pim state-refresh disable command **CS1-438**
- ip pim state-refresh origination-interval command **CS1-438**
- ip pim vc-count command **CS1-438**
- ip pim version command **CS1-439**
- ip policy route-map command **CS1-398**
- ip prefix-list command **CS1-369**
- ip prefix-list description command **CS1-370**
- ip prefix-list sequence-number command **CS1-370**
- ip probe proxy command **CS1-221**
- ip proxy-arp command **CS1-221**
- ip rarp-server command **CS1-86**
- ip rcmd domain-lookup command **CS1-86**
- ip rcmd rep-enable command **CS1-86, CS1-88**

- ip rcmd remote-host command **CS1-87**
- ip rcmd remote-username command **CS1-87**
- ip rcmd rsh-enable command **CS1-88**
- ip redirects command **CS1-257**
- ip rgmp command **CS1-439**
- ip rip authentication key-chain command **CS1-302**
- ip rip authentication mode command **CS1-303**
- ip rip receive version command **CS1-303**
- ip rip send version command **CS1-303**
- ip rip triggered command **CS1-304**
- ip route command **CS1-398**
- ip router isis command **CS1-346**
- ip routing command **CS1-222**
- ip rtp compression-connections command **CS1-439**
- ip rtp header-compression command **CS1-440**
- ip sap cache-timeout command **CS1-440**
- ip sap listen command **CS1-440**
- ip sdr cache-timeout command **CS1-440**
- ip sdr listen command **CS1-441**
- ip slb dfp command **CS1-278**
- ip slb serverfarm command **CS1-279**
- ip slb vserver command **CS1-279**
- ip source-route command **CS1-258**
- ip split-horizon command **CS1-309**
- ip split-horizon eigrp command **CS1-340**
- ip split-horizon (RIP) command **CS1-304**
- ip subnet-zero command **CS1-222**
- ip summary-address eigrp command **CS1-340**
- ip summary-address rip command **CS1-304**
- ip tcp chunk-size command **CS1-258**
- ip tcp compression-connections command **CS1-258**
- ip tcp header-compression command **CS1-259**
- ip tcp path-mtu-discovery command **CS1-259**
- ip tcp queuemax command **CS1-259**
- ip tcp selective-ack command **CS1-260**
- ip tcp synwait-time command **CS1-260**
- ip tcp timestamp command **CS1-260**
- ip tcp window-size command **CS1-261**
- ip telnet source-interface command **CS1-98**
- ip tftp source-interface command **CS1-98**
- ip unnumbered command **CS1-222**
- ip unreachable command **CS1-261**
- ip urd command **CS1-441**
- ip wccp command **CS1-192**
- ip wccp enable command
 - See the ip wccp command*
- ip wccp group-address command **CS1-192**
- ip wccp group-list command **CS1-192**
- ip wccp group-listen command **CS1-193**
- ip wccp password command **CS1-192**
- ip wccp redirect command **CS1-193**
- ip wccp redirect exclude in command **CS1-193**
- ip wccp redirect-list command **CS1-192**
- ip wccp version command **CS1-194**
- ipx access-group command **CS1-528**
- ipx access-list command **CS1-528**
- ipx accounting command **CS1-529**
- ipx accounting-list command **CS1-529**
- ipx accounting-threshold command **CS1-529**
- ipx accounting-transits command **CS1-530**
- ipx advertise-default-route-only command **CS1-530**
- ipx advertise-to-lost-route command **CS1-530**
- ipx backup-server-query-interval command **CS1-531**
- ipx bandwidth-percent eigrp command **CS1-531**
- ipx broadcast-fastswitching command **CS1-531**
- ipx default-output-rip-delay command **CS1-532**
- ipx default-output-sap-delay command **CS1-532**
- ipx default-route command **CS1-532**
- ipx default-triggered-rip-delay command **CS1-533**
- ipx default-triggered-rip-holddown command **CS1-533, CS1-534**
- ipx default-triggered-sap-delay command **CS1-533**
- ipx delay command **CS1-534**
- ipx down command **CS1-534**
- ipx encapsulation command **CS1-535**
- ipx flooding-unthrottled command **CS1-536**
- ipx gns-reply-disable command **CS1-536**
- ipx gns-response-delay command **CS1-537**

- ipx gns-round-robin command **CS1-537**
- ipx hello-interval eigrp command **CS1-537**
- ipx helper-address command **CS1-538**
- ipx helper-list command **CS1-538**
- ipx hold-down eigrp command **CS1-539**
- ipx hold-time eigrp command **CS1-539**
- ipx input-network-filter command **CS1-539**
- ipx input-sap-filter command **CS1-540**
- ipx internal-network command **CS1-540**
- ipx ipxwan command **CS1-541**
- ipx ipxwan error command **CS1-542**
- ipx ipxwan static command **CS1-542**
- ipx link-delay command **CS1-542**
- ipx linkup-request command **CS1-543**
- ipx maximum-hops command **CS1-543**
- ipx maximum-paths command **CS1-543**
- ipx netbios input-access-filter command **CS1-544**
- ipx netbios output-access-filter command **CS1-544**
- ipx netbios-socket-input-checks command **CS1-544**
- ipx network (extended) command **CS1-545**
- ipx nhrp authentication command **CS1-546**
- ipx nhrp holdtime command **CS1-546**
- ipx nhrp interest command **CS1-547**
- ipx nhrp map command **CS1-547**
- ipx nhrp max-send command **CS1-547**
- ipx nhrp network-id command **CS1-548**
- ipx nhrp nhs command **CS1-548**
- ipx nhrp record command **CS1-548**
- ipx nhrp responder command **CS1-549**
- ipx nhrp use command **CS1-549**
- ipx nlsp csnp-interval command **CS1-549**
- ipx nlsp enable command **CS1-551**
- ipx nlsp hello-interval command **CS1-551**
- ipx nlsp hello-multiplier command **CS1-552**
- ipx nlsp lsp-interval command **CS1-552**
- ipx nlsp metric command **CS1-552**
- ipx nlsp multicast command **CS1-553**
- ipx nlsp priority command **CS1-553**
- ipx nlsp retransmit-interval command **CS1-553**
- ipx nlsp rip command **CS1-554**
- ipx nlsp sap command **CS1-554**
- ipx output-ggs-filter command **CS1-555**
- ipx output-gns-filter command **CS1-555**
- ipx output-rip-delay command **CS1-556**
- ipx output-sap-delay command **CS1-556**
- ipx output-sap-filter command **CS1-556**
- ipx pad-process-switched-packets command **CS1-557**
- ipx per-host-load-share command **CS1-557**
- ipx ping-default command **CS1-557**
- ipx potential-pseudonode command **CS1-558**
- ipx rip-max-packetsize command **CS1-558, CS1-566**
- ipx rip-multiplier command **CS1-558**
- ipx rip-queue-maximum command **CS1-559**
- ipx rip-response-delay command **CS1-559**
- ipx rip-update-queue-maximum command **CS1-559**
- ipx route command **CS1-560**
- ipx route-cache command **CS1-561**
- ipx route-cache inactivity-timeout command **CS1-561**
- ipx route-cache max-size command **CS1-561**
- ipx route-cache update-timeout command **CS1-562**
- ipx router command **CS1-562**
- ipx router-filter command **CS1-562**
- ipx router-sap-filter command **CS1-563**
- ipx routing command **CS1-563**
- ipx sap command **CS1-564**
- ipx sap follow-route-path command **CS1-564**
- ipx sap-helper command **CS1-565**
- ipx sap-incremental command **CS1-565**
- ipx sap-incremental split-horizon command **CS1-566**
- ipx sap-multiplier command **CS1-566**
- ipx sap-queue-maximum command **CS1-567**
- ipx sap-update-queue-maximum command **CS1-567**
- ipx server-split-horizon-on-serverpaths command **CS1-567**
- ipx split-horizon eigrp command **CS1-568**
- ipx spx-idle-time command **CS1-568**
- ipx spx-spoof command **CS1-568**
- ipx throughput command **CS1-569**

ipx triggered-rip-delay command **CS1-569**
 ipx triggered-sap-delay command **CS1-570**
 ipx triggered-sap-holddown command **CS1-570**
 ipx type-20-helpered command **CS1-570**
 ipx type-20-input-checks command **CS1-571**
 ipx type-20-output-checks command **CS1-571**
 ipx type-20-propagation command **CS1-571**
 ipx update interval command **CS1-572**
 ipx update sap-after-rip command **CS1-572**
 ipx watchdog command **CS1-572**
 ipx watchdog-spoof command **CS1-573**
 isis adjacency-filter command **CS1-650**
 isis circuit-type command **CS1-346**
 isis csnp-interval command **CS1-347**
 isis display delimiter command **CS1-347**
 isis display delimiter (IS-IS) command **CS1-347**
 isis hello-interval command **CS1-347**
 isis hello-multiplier command **CS1-348**
 isis lsp-interval command **CS1-348**
 isis mesh-group command **CS1-349**
 isis metric command **CS1-349**
 isis password command **CS1-349**
 isis priority command **CS1-350**
 isis retransmit-interval command **CS1-350**
 isis retransmit-throttle-interval command **CS1-351**
 iso-igrp adjacency-filter command **CS1-650**
 is-type command **CS1-351**

K

key chain command **CS1-399**
 key command **CS1-398**
 key-string command **CS1-399**

L

lat host-delay command **CS1-629**
 lat service autocommand command **CS1-629**

lease command **CS1-235**
 length command **CS1-18**
 lives-of-history-kept command **CS1-172**
 load-interval command **CS1-99**
 llocation command **CS1-18**
 lock command **CS1-36**
 lockable command **CS1-18**
 log-adjacency-changes (IPX) command **CS1-573**
 log-adjacency-changes (ISO CLNS) command **CS1-650**
 log-adj-changes command **CS1-326**
 logging buffered command **CS1-118**
 logging command **CS1-117**
 logging console command **CS1-118**
 logging facility command **CS1-119**
 logging history command **CS1-120**
 logging history size command **CS1-120**
 logging linecard command **CS1-121**
 logging monitor command **CS1-121**
 logging on command **CS1-122**
 logging rate-limit command **CS1-122**
 logging source-interface command **CS1-123**
 logging synchronous command **CS1-123**
 logging trap command **CS1-124**
 log-neighbor-changes command **CS1-573**
 logout-warning command **CS1-19**
 lsp-gen-interval command **CS1-574**
 lsp-mtu (IPX) command **CS1-574**
 lsp-mtu (ISO CLNS) command **CS1-651**
 lsp-refresh-interval command **CS1-574**
 lsr-path command **CS1-172**

M

manager command **CS1-469**
 match as-path command **CS1-370**
 match clns address command **CS1-651**
 match clns next-hop command **CS1-651**
 match clns route-source command **CS1-652**
 match community-list command **CS1-371**

match interface command **CS1-399, CS1-652**
 match interface (ISO CLNS) command **CS1-652**
 match ip address command **CS1-400**
 match ip next-hop command **CS1-400**
 match ip route-source command **CS1-400**
 match length command **CS1-401**
 match metric (IP) command **CS1-401**
 match metric (ISO CLNS) command **CS1-652**
 match nlri command
 See address-family ipv4 command
 match route-type (IP) command **CS1-401**
 match route-type (ISO CLNS) command **CS1-653**
 match tag command **CS1-402**
 maxconns command **CS1-279**
 maximum-paths command **CS1-371, CS1-402**
 max-lsp-lifetime command **CS1-575**
 memory scan command **CS1-71**
 memory-size iomem command **CS1-72**
 menu clear-screen command **CS1-36**
 menu command **CS1-37**
 menu default command **CS1-37**
 menu (EXEC) command **CS1-6**
 menu line-mode command **CS1-37**
 menu options command **CS1-37**
 menu prompt command **CS1-38**
 menu single-space command **CS1-38**
 menu status-line command **CS1-38**
 menu text command **CS1-38**
 menu title command **CS1-39**
 metric holddown command **CS1-309**
 metric maximum-hops command **CS1-310**
 metric weights command **CS1-340**
 metric weights (ISO CLNS) command **CS1-653**
 microcode (12000) command **CS1-66**
 microcode (7000/7500) command **CS1-65**
 microcode (7200) command **CS1-66**
 microcode reload (12000) command **CS1-68**
 microcode reload (7000/7500) command **CS1-67**
 microcode reload (7200) command **CS1-67**

mkdir command **CS1-51**
 mop device-code command **CS1-88**
 mop retransmit-timer command **CS1-88**
 more begin command **CS1-6**
 more command **CS1-51**
 more exclude command **CS1-6**
 more flh:logfile command **CS1-68**
 more include command **CS1-7**
 motd-banner command **CS1-39**
 mrinfo command **CS1-469**
 mrm command **CS1-469**
 mstat command **CS1-470**
 mtrace command **CS1-470**
 multicast command **CS1-575**

N

name-connection command **CS1-40**
 nat command **CS1-280**
 neighbor advertise-map non-exist-map
 command **CS1-372**
 neighbor advertisement-interval command **CS1-371**
 neighbor database-filter command **CS1-327**
 neighbor default-originate command **CS1-372**
 neighbor description command **CS1-372**
 neighbor distribute-list command **CS1-373**
 neighbor ebgp-multihop command **CS1-373**
 neighbor filter-list command **CS1-373**
 neighbor (IGRP) command **CS1-310**
 neighbor local-as command **CS1-374**
 neighbor maximum-prefix command **CS1-374**
 neighbor next-hop-self command **CS1-375**
 neighbor (OSPF) command **CS1-326**
 neighbor password command **CS1-375**
 neighbor peer-group command
 creating **CS1-376**
 members, assigning **CS1-375**
 neighbor prefix-list command **CS1-376**
 neighbor remote-as command **CS1-376**

neighbor remove-private-as command **CS1-377**
neighbor (RIP) command **CS1-305**
neighbor route-map command **CS1-377**
neighbor route-reflector-client command **CS1-377**
neighbor send-community command **CS1-378**
neighbor shutdown command **CS1-378**
neighbor soft-reconfiguration inbound command **CS1-378**
neighbor unsuppress-map command **CS1-379**
neighbor update-source command **CS1-379**
neighbor version command **CS1-380**
neighbor weight command **CS1-380**
net command **CS1-352**
netbios access-list command **CS1-575**
netbios-name-server command **CS1-235**
netbios-node-type command **CS1-236**
network area command **CS1-327**
network backdoor command **CS1-381**
network (BGP and multiprotocol BGP) command **CS1-380**
network command **CS1-236**
network (Enhanced IGRP) command **CS1-341**
network (IGRP) command **CS1-310**
network (IPX Enhanced IGRP) command **CS1-576**
network (RIP) command **CS1-305**
network weight command **CS1-381**
next-server command **CS1-237**
no menu command **CS1-39**
no snmp-server command **CS1-139**
ntp access-group command **CS1-99**
ntp authenticate command **CS1-99**
ntp authentication-key command **CS1-100**
ntp broadcast client command **CS1-100**
ntp broadcast command **CS1-100**
ntp broadcastdelay command **CS1-101**
ntp clock-period command **CS1-101**
ntp disable command **CS1-101**
ntp master command **CS1-102**
ntp peer command **CS1-102**
ntp refclock command **CS1-103**

ntp server command **CS1-103**
ntp source command **CS1-104**
ntp trusted-key command **CS1-104**
ntp update-calendar command **CS1-104**

O

offset-list (Enhanced IGRP) command **CS1-341**
offset-list (IGRP) command **CS1-311**
offset-list (RIP) command **CS1-305**
option command **CS1-237**
output-delay command **CS1-306**
owner command **CS1-172**

P

padding command **CS1-19**
parity command **CS1-19**
parser cache command **CS1-59**
partition avoidance command **CS1-352**
partition command **CS1-72**
partition flash command **CS1-72**
passive-interface command **CS1-402**
paths-of-statistics-kept command **CS1-173**
periodic command **CS1-105**
permit command **CS1-261**
permit (IPX extended) command **CS1-576**
permit (IPX standard) command **CS1-578**
permit (NLSP) command **CS1-579**
permit (SAP filtering) command **CS1-579**
ping command
 test connectivity **CS1-124, CS1-125**
ping (privileged) command **CS1-124**
ping (user) command **CS1-125**
prc-interval command **CS1-580**
predictor command **CS1-280**
printer command **CS1-20**
private command **CS1-20**

prompt command **CS1-105**

pwd command **CS1-52**

R

real command **CS1-280**

reassign command **CS1-281**

receivers command **CS1-470**

redistribute dvmrp command **CS1-393**

redistribute (IP) command **CS1-403**

redistribute (IPX) command **CS1-580**

redistribute (ISO CLNS) command **CS1-653**

redistribute static clns command **CS1-654**

redistribute static ip command **CS1-403**

refuse-message command **CS1-40**

reload command **CS1-80**

remark command **CS1-264**

rename command **CS1-52**

request-data-size command **CS1-173**

response-data-size command **CS1-173**

retry command **CS1-281**

rmdir command **CS1-52**

rmon alarm command **CS1-161**

rmon capture-userdata command **CS1-162**

rmon collection history command **CS1-162**

rmon collection host command **CS1-163**

rmon collection matrix command **CS1-163**

rmon command **CS1-161**

rmon event command **CS1-164**

rmon queuesize command **CS1-165**

route reflectors, bgp cluster-id command **CS1-360**

route-aggregation command **CS1-581**

route-map (IP) command **CS1-404**

route-map (ISO CLNS) command **CS1-654**

router bgp command **CS1-381**

router eigrp command **CS1-341**

router igrp command **CS1-311**

router isis command **CS1-352**

router iso-igrp command **CS1-655**

router mobile command **CS1-293**

router odr command **CS1-299**

router ospf command **CS1-328**

router reflectors, bgp client-to-client reflection
command **CS1-360**

router rip command **CS1-306**

router, host name **CS1-97**

router-id command **CS1-327**

rsh command **CS1-89**

rtr command **CS1-174**

rtr key-chain command **CS1-174**

rtr low memory command **CS1-174**

rtr reaction-configuration command **CS1-175**

rtr reaction-trigger command **CS1-176**

rtr reset command **CS1-177**

rtr responder command **CS1-177**

rtr schedule command **CS1-178**

S

samples-of-history-kept command **CS1-179**

scheduler allocate command **CS1-106**

scheduler-interval command **CS1-106**

send command **CS1-40**

senders command **CS1-471**

send-lifetime command **CS1-405**

serverfarm command **CS1-282**

service compress-config command **CS1-59**

service config command **CS1-60**

service decimal-tty command **CS1-106**

service dhcp command **CS1-237**

service exec-wait command **CS1-107**

service finger command **CS1-107**

service hide-telnet-address command **CS1-107**

service linenummer command **CS1-41**

service nagle command **CS1-107**

service prompt config command **CS1-108**

service single-slot-reload-enable command **CS1-197**

service slave-log command **CS1-125**

- service tcp-keepalives-in command **CS1-125**
- service tcp-keepalives-out command **CS1-126**
- service tcp-small-servers command **CS1-108**
- service telnet-zero-idle command **CS1-108**
- service timestamps command **CS1-126**
- service udp-small-servers command **CS1-109**
- set as-path command **CS1-382**
- set automatic-tag command **CS1-406**
- set community command **CS1-382**
- set dampening command **CS1-383**
- set default interface command **CS1-406**
- set interface command **CS1-406**
- set ip default next-hop command **CS1-407**
- set ip next-hop (BGP) command **CS1-383**
- set ip next-hop command **CS1-407**
- set ip next-hop verify-availability command **CS1-407**
- set ip precedence command **CS1-407**
- set level (IP) command **CS1-408**
- set level (ISO CLNS) command **CS1-655**
- set local-preference command **CS1-408**
- set metric command **CS1-655**
- set metric command (BGP, OSPF, RIP) **CS1-409**
- set metric (Enhanced IGRP) command **CS1-342**
- set metric (IGRP) command **CS1-311**
- set metric-type command **CS1-409**
- set metric-type internal command **CS1-384**
- set metric-type (ISO CLNS) command **CS1-656**
- set next-hop command **CS1-409**
- set nlri command
 - See address-family ipv4 command; address-family vpv4 command*
- set origin (BGP) command **CS1-384**
- set origin command **CS1-410**
- set tag command **CS1-410**
- set tag (ISO CLNS) command **CS1-656**
- set weight command **CS1-384**
- set-overload-bit command **CS1-353**
- setup command **CS1-11**
- show access-list compiled command **CS1-265**
- show access-lists command **CS1-264**
- show aliases command **CS1-109**
- show apollo arp command **CS1-594**
- show apollo interface command **CS1-594**
- show apollo route command **CS1-594**
- show apollo traffic command **CS1-594**
- show appletalk access-lists command **CS1-504**
- show appletalk adjacent-routes command **CS1-505**
- show appletalk arp command **CS1-505**
- show appletalk aarp events command **CS1-505**
- show appletalk aarp topology command **CS1-505**
- show appletalk cache command **CS1-506**
- show appletalk domain command **CS1-506**
- show appletalk eigrp interfaces command **CS1-506**
- show appletalk eigrp neighbors command **CS1-506**
- show appletalk eigrp topology command **CS1-507**
- show appletalk globals command **CS1-507**
- show appletalk interface command **CS1-507**
- show appletalk macip-clients command **CS1-508**
- show appletalk macip-servers command **CS1-508**
- show appletalk macip-traffic command **CS1-508**
- show appletalk name-cache command **CS1-508**
- show appletalk nbp command **CS1-509**
- show appletalk neighbors command **CS1-509**
- show appletalk remap command **CS1-509**
- show appletalk route command **CS1-510**
- show appletalk sockets command **CS1-510**
- show appletalk static command **CS1-510**
- show appletalk traffic command **CS1-510**
- show appletalk zone command **CS1-511**
- show arp command **CS1-222**
- show async-bootp command **CS1-89**
- show begin command **CS1-7**
- show boot command **CS1-81**
- show bootvar command **CS1-81**
- show c2600 command **CS1-126**
- show c7200 command **CS1-127**
- show calendar command **CS1-110**
- show cdp command **CS1-159**

- show cdp entry command **CS1-159**
- show cdp interface command **CS1-159**
- show cdp neighbors command **CS1-160**
- show cdp traffic command **CS1-160**
- show clns cache command **CS1-656**
- show clns command **CS1-656**
- show clns es-neighbors command **CS1-657**
- show clns filter-expr command **CS1-657**
- show clns filter-set command **CS1-658**
- show clns interface command **CS1-658**
- show clns is-neighbors command **CS1-658**
- show clns neighbor areas command **CS1-659**
- show clns neighbors command **CS1-659**
- show clns protocol command **CS1-659**
- show clns route command **CS1-660**
- show clns traffic command **CS1-660**
- show clock command **CS1-110**
- show configuration command **CS1-52, CS1-60**
- show context command **CS1-127**
- show context command (2600) **CS1-127**
- show controllers (GRP image) command **CS1-128**
- show controllers (line card image) command **CS1-129**
- show controllers logging command **CS1-130**
- show controllers tech-support command **CS1-130**
- show debugging command **CS1-131**
- show decnet accounting command **CS1-630**
- show decnet command **CS1-630**
- show decnet interface command **CS1-630**
- show decnet map command **CS1-630**
- show decnet neighbors command **CS1-631**
- show decnet route command **CS1-631**
- show decnet static command **CS1-631**
- show decnet traffic command **CS1-631**
- show diag command **CS1-131**
- show environment command **CS1-131**
- show exclude command **CS1-7**
- show file command **CS1-60**
- show file descriptors command **CS1-52**
- show file information command **CS1-53**
- show file systems command **CS1-53**
- show flash chips command **CS1-73**
- show flash command **CS1-73**
- show (Flash file system) command **CS1-73**
- show flash filesystem command **CS1-73**
- show flh-log command **CS1-68**
- show frame-relay ip rtp header-compression command **CS1-441**
- show gsr command **CS1-132**
- show gt64010 command **CS1-132**
- show history command **CS1-8**
- show hosts command **CS1-223**
- show include command **CS1-8**
- show ip access-list command **CS1-265**
- show ip accounting command **CS1-265**
- show ip aliases command **CS1-223**
- show ip arp command **CS1-223**
- show ip bgp cidr-only command **CS1-385**
- show ip bgp command **CS1-384**
- show ip bgp community command **CS1-385**
- show ip bgp community-list command **CS1-385**
- show ip bgp dampened-paths command **CS1-386**
- show ip bgp filter-list command **CS1-386**
- show ip bgp flap-statistics command **CS1-386**
- show ip bgp inconsistent-as command **CS1-386**
- show ip bgp ipv4 command **CS1-387**
- show ip bgp ipv4 multicast command **CS1-394**
- show ip bgp ipv4 multicast summary command **CS1-394**
- show ip bgp neighbors command **CS1-387**
- show ip bgp paths command **CS1-387**
- show ip bgp peer-group command **CS1-387**
- show ip bgp regexp command **CS1-388**
- show ip bgp summary command **CS1-388**
- show ip cache policy command **CS1-410**
- show ip casa affinities command **CS1-265**
- show ip casa oper command **CS1-266**
- show ip casa stats command **CS1-266**
- show ip casa wildcard command **CS1-266**
- show ip dhcp binding command **CS1-238**

- show ip dhcp conflict command **CS1-238**
- show ip dhcp database command **CS1-238**
- show ip dhcp import command **CS1-238**
- show ip dhcp server statistics command **CS1-239**
- show ip drp command **CS1-267**
- show ip dvmrp route command **CS1-441**
- show ip eigrp interfaces command **CS1-342**
- show ip eigrp neighbors command **CS1-342**
- show ip eigrp topology command **CS1-343**
- show ip eigrp traffic command **CS1-343**
- show ip igmp groups command **CS1-442**
- show ip igmp interface command **CS1-442**
- show ip igmp udlr command **CS1-465**
- show ip interface command **CS1-223**
- show ip irdp command **CS1-224**
- show ip local policy command **CS1-410**
- show ip masks command **CS1-224**
- show ip mbgp command
 - See show ip bgp ipv4 multicast command
- show ip mbgp summary command
 - See show ip bgp ipv4 multicast summary command
- show ip mcache command **CS1-442**
- show ip mobile binding command **CS1-293**
- show ip mobile globals command **CS1-294**
- show ip mobile host command **CS1-294**
- show ip mobile interface command **CS1-294**
- show ip mobile secure command **CS1-294**
- show ip mobile traffic command **CS1-295**
- show ip mobile tunnel command **CS1-295**
- show ip mobile violation command **CS1-295**
- show ip mobile visitor command **CS1-295**
- show ip mpacket command **CS1-443**
- show ip mrm interface command **CS1-472**
- show ip mrm manager command **CS1-472**
- show ip mrm status-report command **CS1-473**
- show ip mroute command **CS1-443**
- show ip msdp count command **CS1-454**
- show ip msdp peer command **CS1-454**
- show ip msdp sa-cache command **CS1-454**
- show ip msdp summary command **CS1-455**
- show ip nat statistics command **CS1-224**
- show ip nat translations command **CS1-224**
- show ip nhrp command **CS1-225**
- show ip nhrp traffic command **CS1-225**
- show ip ospf border-routers command **CS1-328**
- show ip ospf command **CS1-328**
- show ip ospf database command **CS1-328**
- show ip ospf flood-list command **CS1-331**
- show ip ospf interface command **CS1-332**
- show ip ospf neighbor command **CS1-332**
- show ip ospf request-list command **CS1-332**
- show ip ospf retransmission-list command **CS1-332**
- show ip ospf summary-address command **CS1-333**
- show ip ospf virtual-links command **CS1-333**
- show ip pgm host defaults command **CS1-460**
- show ip pgm host sessions command **CS1-460**
- show ip pgm host traffic command **CS1-460**
- show ip pgm router command **CS1-461**
- show ip pim bsr command **CS1-443**
- show ip pim interface command **CS1-444**
- show ip pim neighbor command **CS1-444**
- show ip pim rp command **CS1-444**
- show ip pim rp-hash command **CS1-445**
- show ip pim vc command **CS1-445**
- show ip policy command **CS1-410**
- show ip protocols command **CS1-411**
- show ip redirects command **CS1-267**
- show ip rip database command **CS1-306**
- show ip route command **CS1-411**
- show ip route summary command **CS1-411**
- show ip route supernets-only command **CS1-411**
- show ip rpf command **CS1-445**
- show ip rtp header-compression command **CS1-445**
- show ip sap command **CS1-446**
- show ip sdr command **CS1-446**
- show ip slb conns command **CS1-282**
- show ip slb dfp command **CS1-282**
- show ip slb reals command **CS1-283**

show ip slb serverfarms command **CS1-283**
show ip slb stats command **CS1-283**
show ip slb sticky command **CS1-283**
show ip tcp header-compression command **CS1-267**
show ip traffic command **CS1-267**
show ip wccp command **CS1-194**
show ip wccp detail command **CS1-194**
show ip wccp view command **CS1-194**
show ipx access-list command **CS1-581**
show ipx accounting command **CS1-582**
show ipx cache command **CS1-582**
show ipx eigrp interfaces command **CS1-582**
show ipx eigrp neighbors command **CS1-582**
show ipx eigrp topology command **CS1-583**
show ipx interface command **CS1-583**
show ipx nhrp command **CS1-583**
show ipx nhrp traffic command **CS1-584**
show ipx nlsr database command **CS1-584**
show ipx nlsr neighbors command **CS1-584**
show ipx nlsr spf-log command **CS1-585**
show ipx route command **CS1-585**
show ipx servers command **CS1-585**
show ipx spx-spoof command **CS1-586**
show ipx traffic command **CS1-586**
show isis database command **CS1-353**
show isis routes command **CS1-660**
show isis spf-log command **CS1-354**
show isis topology command **CS1-354**
show key chain command **CS1-412**
show logging command **CS1-118, CS1-132**
show management event command **CS1-139**
show memory command **CS1-133**
show microcode command **CS1-68**
show ntp associations command **CS1-110**
show ntp status command **CS1-110**
show parser statistics command **CS1-60**
show pci command **CS1-133**
show pci hardware command **CS1-133**
show processes command **CS1-133**
show processes memory command **CS1-134**
show protocols command **CS1-134**
show registry command **CS1-111**
show reload command **CS1-81**
show rmon alarms command **CS1-166**
show rmon capture command **CS1-166**
show rmon command **CS1-165**
show rmon events command **CS1-166**
show rmon filter command **CS1-166**
show rmon history command **CS1-166**
show rmon hosts command **CS1-167**
show rmon matrix command **CS1-167**
show rmon statistics command **CS1-167**
show rmon topn command **CS1-167**
show route-map command **CS1-412, CS1-661**
show route-map ipc command **CS1-412**
show rtr application command **CS1-179**
show rtr authentication command **CS1-179**
show rtr collection-statistics command **CS1-179**
show rtr configuration command **CS1-180**
show rtr distribution-statistics command **CS1-180**
show rtr history command **CS1-180**
show rtr operational-state command **CS1-181**
show rtr reaction-trigger command **CS1-181**
show rtr responder command **CS1-181**
show rtr totals-statistics command **CS1-182**
show running-config command **CS1-60**
show smrp forward command **CS1-511**
show smrp globals command **CS1-511**
show smrp group command **CS1-511**
show smrp mcache command **CS1-512**
show smrp neighbor command **CS1-512**
show smrp port command **CS1-512**
show smrp route command **CS1-512**
show smrp traffic command **CS1-513**
show snmp command **CS1-139**
show snmp engineID command **CS1-140**
show snmp group command **CS1-140**
show snmp pending command **CS1-140**

- show snmp sessions command **CS1-140**
- show snmp user command **CS1-141**
- show snmp command **CS1-111**
- show sse summary command **CS1-586**
- show stacks command **CS1-134**
- show standby command **CS1-268**
- show startup-config command **CS1-61**
- show subsys command **CS1-134**
- show tarp blacklisted-adjacencies command **CS1-661**
- show tarp command **CS1-661**
- show tarp host command **CS1-662**
- show tarp interface command **CS1-662**
- show tarp ldb command **CS1-662**
- show tarp map command **CS1-662**
- show tarp static-adjacencies command **CS1-663**
- show tarp tid-cache command **CS1-663**
- show tarp traffic command **CS1-663**
- show tcp brief command **CS1-135**
- show tcp command **CS1-135**
- show tcp statistics command **CS1-268**
- show tdm connections command **CS1-135**
- show tdm data command **CS1-135**
- show tech-support command **CS1-136**
- show version command **CS1-81**
- show vines access command **CS1-597**
- show vines cache command **CS1-597**
- show vines host command **CS1-597**
- show vines interface command **CS1-598**
- show vines ipc command **CS1-598**
- show vines neighbor command **CS1-598**
- show vines route command **CS1-598**
- show vines service command **CS1-599**
- show vines traffic command **CS1-599**
- show whoami command **CS1-20**
- show xns cache command **CS1-676**
- show xns interface command **CS1-676**
- show xns route command **CS1-676**
- show xns traffic command **CS1-677**
- slave auto-sync config command **CS1-197**
- slave default-slot command **CS1-198**
- slave image command **CS1-198**
- slave reload command **CS1-198**
- slave sync config command **CS1-198**
- slave terminal command **CS1-199**
- snmp mroute-cache protocol appletalk command **CS1-513**
- snmp protocol appletalk command **CS1-513**
- snmp routing command **CS1-514**
- snmp trap link-status command **CS1-156**
- snmp-server access-policy command **CS1-141**
- snmp-server chassis-id command **CS1-141**
- snmp-server community command **CS1-141**
- snmp-server contact command **CS1-142**
- snmp-server context command **CS1-142**
- snmp-server enable informs command **CS1-142**
- snmp-server enable traps aaa_server command **CS1-144**
- snmp-server enable traps atm command **CS1-144**
- snmp-server enable traps bgp command **CS1-144**
- snmp-server enable traps calltracker command **CS1-145**
- snmp-server enable traps command **CS1-142**
- snmp-server enable traps envmon command **CS1-145**
- snmp-server enable traps frame-relay command **CS1-146**
- snmp-server enable traps isdn command **CS1-146**
- snmp-server enable traps repeater command **CS1-147**
- snmp-server enable traps snmp command **CS1-147**
- snmp-server enable traps voice poor-qov command **CS1-148**
- snmp-server engineID command **CS1-148**
- snmp-server group command **CS1-149**
- snmp-server host command **CS1-150**
- snmp-server informs command **CS1-151**
- snmp-server location command **CS1-152**
- snmp-server manager command **CS1-152**
- snmp-server manager session-timeout command **CS1-152**
- snmp-server packet-size command **CS1-153**
- snmp-server queue-length command **CS1-153**
- snmp-server system-shutdown command **CS1-153**
- snmp-server tftp-server-list command **CS1-154**
- snmp-server trap link command **CS1-154**
- snmp-server trap-authentication command **CS1-154**
- snmp-server trap-source command **CS1-155**

snmp-server trap-timeout command **CS1-155**
 snmp-server user command **CS1-155**
 snmp-server view command **CS1-156**
 sntp broadcast client command **CS1-111**
 sntp server command **CS1-111**
 special-character-bits command **CS1-21**
 spf-interval command **CS1-587**
 squeeze command **CS1-53**
 standby authentication command **CS1-268**
 standby ip command **CS1-269**
 standby mac-address command **CS1-269**
 standby mac-refresh command **CS1-269**
 standby name command **CS1-270**
 standby preempt command **CS1-270, CS1-271**
 standby redirects command **CS1-271**
 standby timers command **CS1-272**
 standby track command **CS1-272**
 standby use-bia command **CS1-273**
 start-forwarding-agent command **CS1-273**
 state-machine command **CS1-21**
 statistics-distribution-interval command **CS1-182**
 sticky command **CS1-284**
 stopbits command **CS1-22**
 summary-address command **CS1-333**
 summary-address (IS-IS) command **CS1-354**
 synchronization command **CS1-389**
 synguard command **CS1-284**

T

table-map command **CS1-389**
 tag command **CS1-182**
 tarp allow-caching command **CS1-663**
 tarp arp-request-timer command **CS1-664**
 tarp blacklist-adjacency command **CS1-664**
 tarp cache-timer command **CS1-664**
 tarp enable command **CS1-665, CS1-667**
 tarp global-propagate command **CS1-665**
 tarp ldb-timer command **CS1-665**
 tarp lifetime command **CS1-666**
 tarp map command **CS1-666**
 tarp nselector-type command **CS1-666**
 tarp originate command **CS1-667**
 tarp post-t2-response-timer command **CS1-667**
 tarp propagate command **CS1-667**
 tarp protocol-type command **CS1-668**
 tarp query command **CS1-668**
 tarp resolve command **CS1-668**
 tarp route-static command **CS1-669**
 tarp run command **CS1-669**
 tarp sequence-number command **CS1-669**
 tarp t1-response-timer command **CS1-670**
 tarp t2-response-timer command **CS1-670**
 tarp tid command **CS1-670**
 tarp urc command **CS1-671**
 term ip netmask-format command **CS1-225**
 terminal databits command **CS1-22**
 terminal data-character-bits command **CS1-22**
 terminal dispatch-character command **CS1-22**
 terminal dispatch-timeout command **CS1-23**
 terminal download command **CS1-23**
 terminal editing command **CS1-8**
 terminal escape-character command **CS1-23**
 terminal exec-character-bits command **CS1-24**
 terminal flowcontrol command **CS1-24**
 terminal full-help command **CS1-9**
 terminal history command **CS1-9**
 terminal hold-character command **CS1-24**
 terminal international command **CS1-45**
 terminal keymap-type command **CS1-25**
 terminal length command **CS1-25**
 terminal monitor command **CS1-25**
 terminal notify command **CS1-25**
 terminal padding command **CS1-26**
 terminal parity command **CS1-26**
 terminal rxspeed command **CS1-27, CS1-30**
 terminal special-character-bits command **CS1-27**
 terminal speed command **CS1-27**

terminal start-character command **CS1-27**
terminal stopbits command **CS1-28**
terminal stop-character command **CS1-28**
terminal telnet break-on-ip command **CS1-28**
terminal telnet refuse-negotiations command **CS1-28**
terminal telnet speed command **CS1-29**
terminal telnet sync-on-break command **CS1-29**
terminal telnet transparent command **CS1-29**
terminal terminal-type command **CS1-29**
terminal txspeed command **CS1-30**
terminal width command **CS1-30**
terminal-queue command **CS1-26**
terminal-type command **CS1-30**
test appletalk command **CS1-514**
test flash command **CS1-136**
test interfaces command **CS1-136**
test memory command **CS1-136**
tftp-server command **CS1-90**
tftp-server system command
See tftp-server command
threshold command **CS1-183**
timeout command **CS1-183**
time-range command **CS1-112**
timers active-time command **CS1-343**
timers basic command **CS1-299, CS1-306, CS1-312**
timers basic (ISO CLNS) command **CS1-671**
timers bgp command **CS1-389**
timers lsa-group-pacing command **CS1-334**
timers spf command **CS1-334**
tos command **CS1-183**
trace (privileged) command **CS1-137**
trace (user) command **CS1-137**
trace (VINES) command **CS1-599**
traffic-share balanced (Enhanced IGRP)
command **CS1-344**
traffic-share balanced (IGRP) command **CS1-313**
traffic-share (IGRP) command **CS1-313**
traffic-share min command **CS1-412**
transmit-interface command **CS1-273**

tunnel mode command **CS1-226**
tunnel udI address-resolution command **CS1-465**
tunnel udI receive-only command **CS1-465**
tunnel udI send-only command **CS1-466**
type dhcp command **CS1-184**
type dlsw command **CS1-184**
type dns command **CS1-184**
type echo command **CS1-185**
type ftp command **CS1-185**
type http command **CS1-186**
type jitter command **CS1-187**
type pathEcho command **CS1-187**
type tcpConnect command **CS1-188**
type udpEcho command **CS1-188**

U

udp-port command **CS1-473**
undelete command **CS1-53**

V

vacant-message command **CS1-41**
validate-update-source command **CS1-307**
verify command **CS1-53**
verify-data command **CS1-189**
version command **CS1-307**
vines access-group command **CS1-600**
vines access-list (extended) command **CS1-600**
vines access-list (simple) command **CS1-601**
vines access-list (standard) command **CS1-602**
vines arp-enable command **CS1-603**
vines decimal command **CS1-603**
vines encapsulation command **CS1-603**
vines enhancements command **CS1-604**
vines host command **CS1-604**
vines input-network-filter command **CS1-604, CS1-606**
vines input-router-filter command **CS1-605**

vines metric command **CS1-605**
 vines neighbor command **CS1-605**
 vines output-network-filter command **CS1-606**
 vines propagate command **CS1-606**
 vines redirect command **CS1-607**
 vines route command **CS1-607**
 vines route-cache command **CS1-607**
 vines routing command **CS1-608**
 vines serverless command **CS1-608**
 vines single-route command **CS1-608**
 vines split-horizon command **CS1-609**
 vines srtp-enabled command **CS1-609**
 vines time access-group command **CS1-609**
 vines time destination command **CS1-610**
 vines time participate command **CS1-610**
 vines time services command **CS1-610**
 vines time set-system command **CS1-611**
 vines time use-system command **CS1-611**
 vines update deltas command **CS1-611**
 vines update interval command **CS1-612**
 virtual command **CS1-285**
 virtual MAC address **CS1-269**

 xns encapsulation command **CS1-677**
 xns flood broadcast allnets command **CS1-678**
 xns flood broadcast net-zero command **CS1-678**
 xns flood specific allnets command **CS1-678**
 xns forward-protocol command **CS1-679**
 xns hear-rip command **CS1-679**
 xns helper-address command **CS1-679**
 xns input-network-filter command **CS1-680**
 xns maximum-paths command **CS1-680**
 xns network command **CS1-680**
 xns output-network-filter command **CS1-681**
 xns route command **CS1-681**
 xns route-cache command **CS1-681**
 xns router-filter command **CS1-682**
 xns routing command **CS1-682**
 xns ub-emulation command **CS1-682**
 xns update-time command **CS1-683**

W

weight command **CS1-286**
 where command **CS1-30**
 which-route command **CS1-672**
 width command **CS1-31**
 write erase command
 See erase nvram command
 write memory command **CS1-74**
 write network command **CS1-74**

X

xmodem command **CS1-69**
 xns access-group command **CS1-677**

