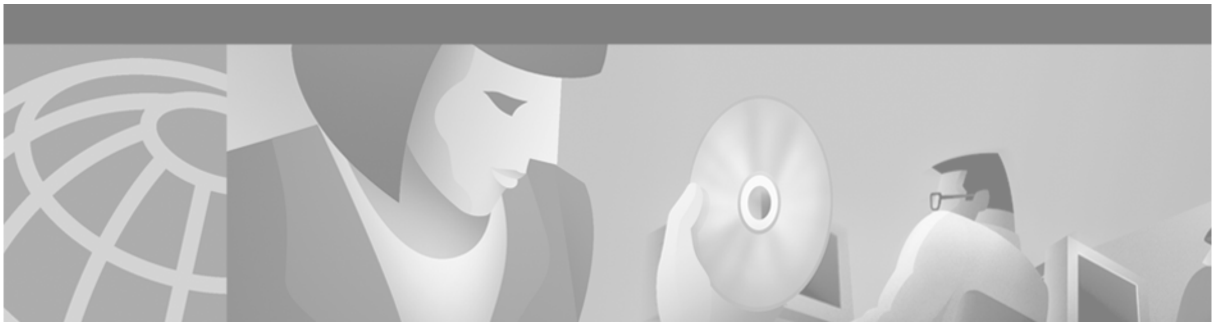
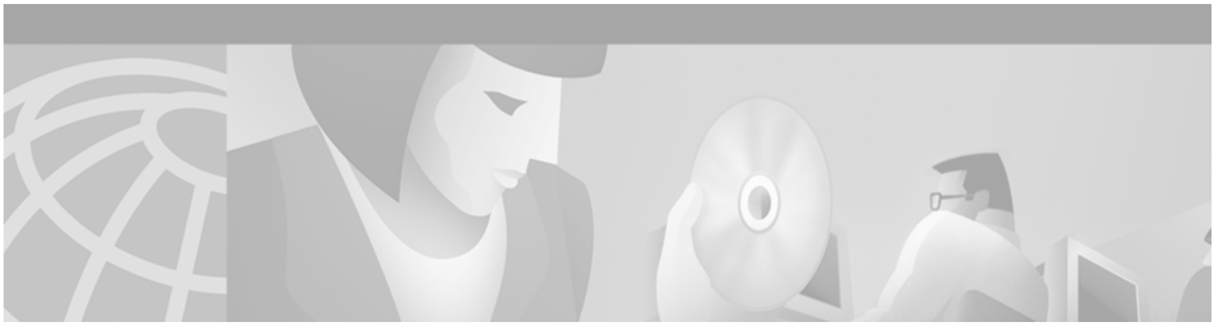
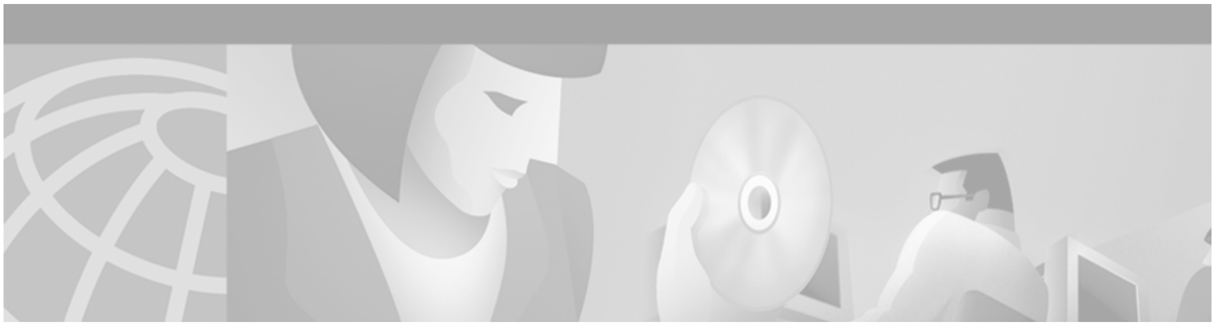


Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols

Release 12.2

Customer Order Number: DOC-7811743=
Text Part Number: 78-11743-01





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.

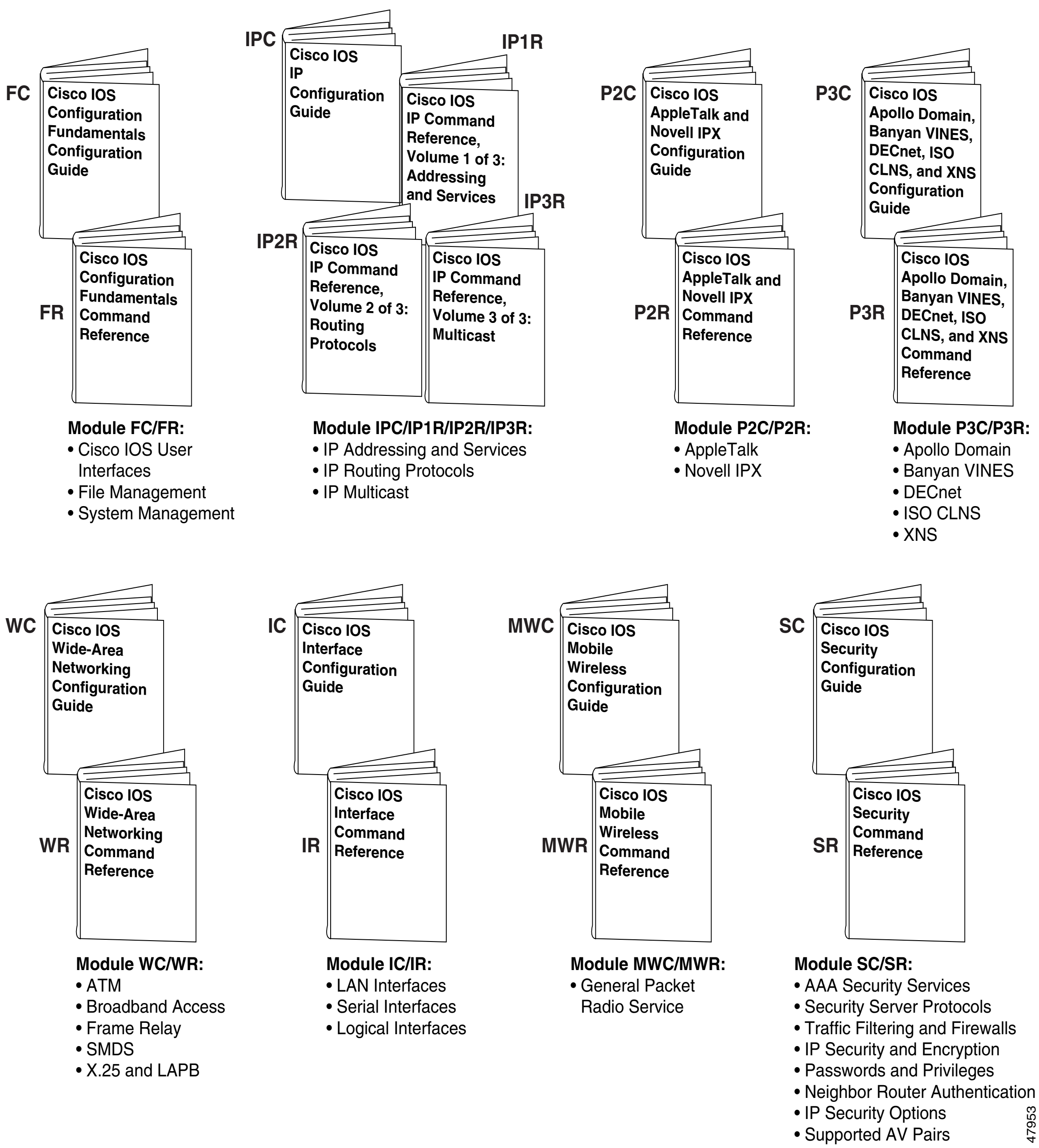
Documentation Modules

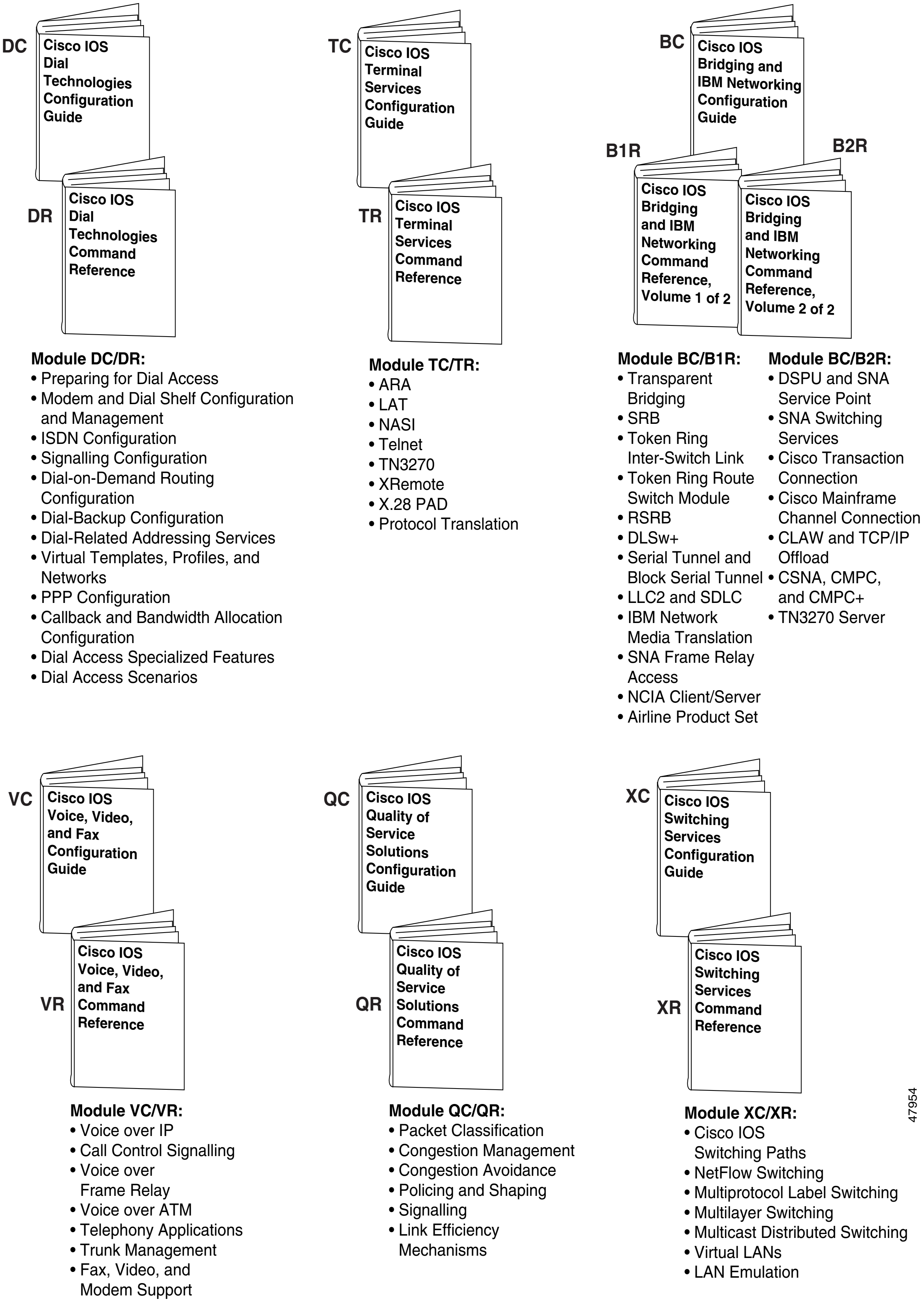
The Cisco IOS documentation modules consist of configuration guides and corresponding command reference publications. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality and contain comprehensive configuration examples. Chapters in a command 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




DC
Cisco IOS Dial Technologies Configuration Guide
DR
Cisco IOS Dial Technologies Command Reference
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
TC
Cisco IOS Terminal Services Configuration Guide
TR
Cisco IOS Terminal Services Command Reference
Module TC/TR:
• ARA
• LAT
• NASI
• Telnet
• TN3270
• XRemote
• X.28 PAD
• Protocol Translation
BC
Cisco IOS Bridging and IBM Networking Configuration Guide
B1R
Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2
B2R
Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2
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
VC
Cisco IOS Voice, Video, and Fax Configuration Guide
VR
Cisco IOS Voice, Video, and Fax Command Reference
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
QC
Cisco IOS Quality of Service Solutions Configuration Guide
QR
Cisco IOS Quality of Service Solutions Command Reference
Module QC/QR:
• Packet Classification
• Congestion Management
• Congestion Avoidance
• Policing and Shaping
• Signalling
• Link Efficiency Mechanisms
XC
Cisco IOS Switching Services Configuration Guide
XR
Cisco IOS Switching Services Command Reference
Module XC/XR:
• Cisco IOS Switching Paths
• NetFlow Switching
• Multiprotocol Label Switching
• Multilayer Switching
• Multicast Distributed Switching
• Virtual LANs
• LAN Emulation
47954

Master Indexes

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

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

Supporting Documents and Resources

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

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

New and Changed Information

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

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

Document Conventions

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

The Cisco IOS documentation set uses the following conventions:

Convention	Description
^ or Ctrl	The ^ and Ctrl symbols represent the Control key. For example, the key combination ^D or Ctrl-D means hold down the Control key while you press the D key. Keys are indicated in capital letters but are not case sensitive.
string	A string is a nonquoted set of characters shown in italics. For example, when setting an SNMP community string to public, do not use quotation marks around the string or the string will include the quotation marks.

Command syntax descriptions use the following conventions:

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

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

<table>
<tr><th>Convention</th><th>Description</th></tr>
<tr><td>[x {y | z}]</td><td>Braces and a vertical line within square brackets indicate a required choice within an optional element.</td></tr>
</table>

Examples use the following conventions:

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

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

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

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

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

Obtaining Documentation

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

World Wide Web

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

http://www.cisco.com

Translated documentation is available at the following website:

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

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation can be ordered in the following ways:

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

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

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

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

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

Documentation Feedback

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

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

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

http://www.cisco.com

Technical Assistance Center

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

Contacting TAC by Using the Cisco TAC Website

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

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

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

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

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

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

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

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

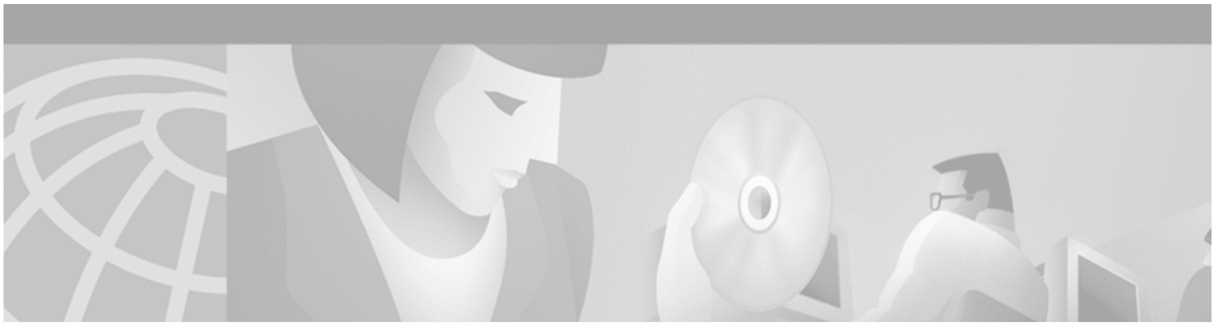
Contacting TAC by Telephone

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

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

P1 and P2 level problems are defined as follows:

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



Using Cisco IOS Software

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

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

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

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

Understanding Command Modes

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

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

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

ROM monitor mode is a separate mode used when the Cisco IOS software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode.

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

Table 1 Accessing and Exiting Command Modes

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

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

Getting Help

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

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

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

Example: How to Find Command Options

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

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

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

Table 2 How to Find Command Options

Command	Comment
Router> **enable** Password: *<password>* Router#	Enter the **enable** command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to Router#.
Router# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z. Router(config)#	Enter the **configure terminal** privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to Router(config)#.
Router(config)# **interface serial ?** <0-6> Serial interface number Router(config)# **interface serial 4 ?** / Router(config)# **interface serial 4/ ?** <0-3> Serial interface number Router(config)# **interface serial 4/0** Router(config-if)#	Enter interface configuration mode by specifying the serial interface that you want to configure using the **interface serial** global configuration command. Enter **?** to display what you must enter next on the command line. In this example, you must enter the serial interface slot number and port number, separated by a forward slash. You are in interface configuration mode when the prompt changes to Router(config-if)#.

Table 2 How to Find Command Options (continued)

Command	Comment

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

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

Table 2 How to Find Command Options (continued)

Command	Comment

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

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

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

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

Using the no and default Forms of Commands

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

Configuration commands also can have a **default** form, which returns the command settings to the default values. Most commands are disabled by default, so in such cases using the **default** form has the same result as using the **no** form of the command. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** form of the command enables the command and sets the variables to their default values. The Cisco IOS software command reference publications describe the effect of the **default** form of a command if the command functions differently than the **no** form.

Saving Configuration Changes

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

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

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

```
[OK]
Router#
```

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

Filtering Output from the show and more Commands

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

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

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

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

```
Router# show interface | include protocol

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

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

Identifying Supported Platforms

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

- Using Feature Navigator
- Using Software Release Notes

Using Feature Navigator

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

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

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

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

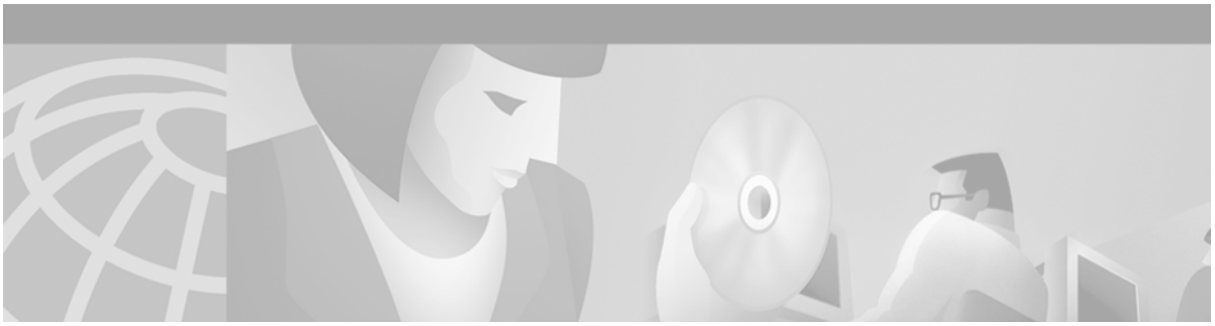
http://www.cisco.com/go/fn

Using Software Release Notes

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

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

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



On-Demand Routing Commands

Use the commands in this chapter to configure On-Demand Routing (ODR). For ODR configuration information and examples, refer to the "Configuring On-Demand Routing" chapter of the *Cisco IOS IP Configuration Guide*.

router odr

To configure a router to accept On-Demand Routing (ODR) routes from a stub routers, use the **router odr** command in global configuration mode. To disable ODR, use the **no** form of this command.

router odr

no router odr

Syntax Description

This command has no arguments or keywords.

Defaults

The router ignores any received ODR information.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command on hub routers to enable ODR to update the routing table with information learned via ODR stub routers.

Examples

The following example sets up the routers in the distribution list to accept ODR routes from the specified access list:

```
router odr
 distribute-list 101 in
access-list 101 permit ip host 10.0.0.1 192.168.110.0 255.255.255.0
access-list 101 permit ip 10.1.1.1 255.0.0.0 192.168.111.0 255.255.255.0
router ospf 1
 redistribute odr subnets
```

Related Commands

Command	Description
distance (IP)	Defines an administrative distance.
distribute-list in (IP)	Filters networks received in updates.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
maximum-paths	Controls the maximum number of parallel routes an IP routing protocol can support.

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

update	Rate (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol.
invalid	Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the *update* 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.
holddown	Interval (in seconds) during which routing information regarding better paths is suppressed. It should be at least three times the value of the *update* argument. A route 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 *holddown* expires, routes advertised by other sources are accepted and the route is no longer inaccessible.
flush	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 *invalid* and *holddown* 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.
sleeptime	(Optional) Interval (in milliseconds) for postponing routing updates in the event of a flash update. The *sleeptime* value should be less than the *update* time. If the *sleeptime* is greater than the *update* time, routing tables will become unsynchronized.

Defaults

update: 90 seconds

invalid: 270 seconds

holddown: 280 seconds

flush: 630 seconds

sleeptime: 0 milliseconds

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The basic timing parameters for ODR are adjustable. Because this routing protocol is executing a distributed, asynchronous routing algorithm, it is important that these timers be the same for all routers and access servers in the network.

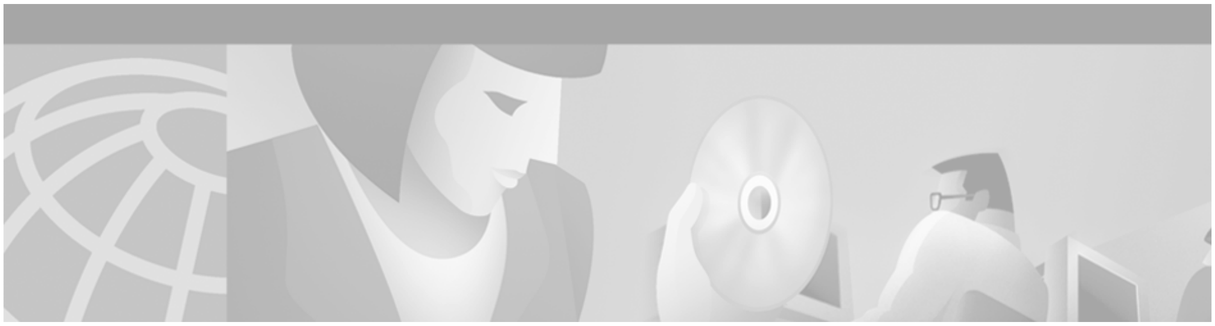
Note The current and default timer values can be seen by inspecting the output of the **show ip protocols** EXEC command. The relationships of the various timers should be preserved as described previously.

Examples

The following example sets updates to be broadcast every 5 seconds. If a router is not heard from in 15 seconds, the route is declared unusable. Further information is suppressed for an additional 15 seconds. At the end of the suppression period, the route is flushed from the routing table.

```
router odr 109
 timers basic 5  15  15  30
```

Note By setting a short update period, you run the risk of congesting slow-speed serial lines; however, this is not a big concern on faster-speed Ethernets and T1-rate serial lines. Also, if you have many routes in your updates, you can cause the routers to spend an excessive amount of time processing updates.



RIP Commands

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

auto-summary (RIP)

To restore the default behavior of automatic summarization of subnet routes into network-level routes, use the **auto-summary** command in router configuration mode. 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.

Defaults

Enabled (the software summarizes subprefixes to the classful network boundary when crossing classful network boundaries).

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Route summarization reduces the amount of routing information in the routing tables.

RIP Version 1 always uses automatic summarization. If you are using RIP Version 2, you can turn off automatic summarization by specifying the **no auto-summary** command. Disable automatic summarization if you must perform routing between disconnected subnets. When automatic summarization is off, subnets are advertised.

Examples

In the following example, network numbers are not summarized automatically:

```
router rip
 version 2
 no auto-summary
```

default-information originate

To generate a default route into Routing Information Protocol (RIP), use the **default-information originate** command in router configuration mode. 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.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The route map referenced in the **default-information originate** command cannot use an extended access list; it can use a standard access list.

Examples

The following example originates a default route (0.0.0.0/0) over a certain interface when 172.68.0.0/16 is present. Applying a condition (in this case a route map) to determine when the default route is originated is called "conditional default origination."

```
router rip
 version 2
 network 172.68.16.0
 default-information originate route-map condition
!
 route-map condition permit 10
 match ip address 10
 set interface s1/0
!
access-list 10 permit 172.68.16.0 0.0.0.255
!
```

default-metric (RIP)

To set default metric values for Routing Information Protocol (RIP), use the **default-metric** command in router configuration mode. To return to the default state, use the **no** form of this command.

default-metric *number-value*

no default-metric [*number-value*]

Syntax Description

number-value	Default metric value.

Defaults

Built-in, automatic metric translations, as appropriate for each routing protocol

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **default-metric** command is used in conjunction with the **redistribute** router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

Examples

The following example shows a router in autonomous system 109 using both the RIP and the Open Shortest Path First (OSPF) routing protocols. The example advertises OSPF-derived routes using RIP and assigns the OSPF-derived routes a RIP metric of 10.

```
router rip
 default-metric 10
 redistribute ospf 109
```

Related Commands

Command	Description
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

distribute-list in (RIP, IGRP, EIGRP)

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* [**gateway** *prefix-list-name*]} **in** [*interface-type interface-number*]

no distribute-list {*access-list-number* | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*]} **in** [*interface-type interface-number*]

Syntax Description

access-list-number	Standard IP access list number. The list defines which networks are to be received and which are to be suppressed in routing updates.
prefix *prefix-list-name*	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.
gateway *prefix-list-name*	(Optional) Name of the prefix list to be applied to the gateway of the prefix being updated.
in	Applies the access list to incoming routing updates.
interface-type	(Optional) Interface type.
interface-number	(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.

Defaults

This command is disabled by default.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-number*, *interface-type*, and *interface-number* arguments were added.
12.0	The *prefix-list-name* argument was added.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

This command is not supported in Intermediate Sytem-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF).

Using a prefix list allows filtering based upon the prefix length, making it possible to filter either on the prefix list, the gateway, or both for incoming updates.

Specify either an access list or a prefix list with the **distribute-list in** command.

Use the **gateway** keyword only with the **prefix-list** keyword.

To suppress networks from being advertised in updates, use the **distribute-list out** command.

Examples

In the following example, the BGP routing process accepts only two networks—network 0.0.0.0 and network 131.108.0.0:

```
access-list 1 permit 0.0.0.0
access-list 1 permit 131.108.0.0
access-list 1 deny 0.0.0.0 255.255.255.255
router bgp
 network 131.108.0.0
 distribute-list 1 in
```

In the following example, The RIP process accepts only prefixes with prefix lengths of /8 to /24:

```
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
router rip
 network 131.108.0.0
 distribute-list prefix max24 in
```

In the following example, the RIP process filters on packet length and accepts routing updates from address 192.1.1.1 only:

```
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
ip prefix-list allowlist seq5 permit 192.1.1.1/32
router rip
 network 131.108.0.0
 distribute-list prefix max24 gateway allowlist in
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
distribute-list out (RIP, IGRP, EIGRP)	Suppresses networks from being advertised in updates.
ip prefix-list	Creates an entry in a prefix list.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

distribute-list out (RIP, IGRP, EIGRP)

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* [**gateway** *prefix-list-name*]} **out** [*interface-name* | *routing-process* | *as-number*]

no distribute-list {*access-list-number* | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*]} **out** [*interface-name* | *routing-process* | *as-number*]

Syntax Description

access-list-number	Standard IP access list number. The list defines which networks are to be received and which are to be suppressed in routing updates.
prefix *prefix-list-name*	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.
gateway *prefix-list-name*	(Optional) Name of the prefix list to be applied to the gateway of the prefix being updated.
out	Applies the access list to outgoing routing updates.
interface-name	(Optional) Name of a particular interface.
routing-process	(Optional) Name of a particular routing process, or the keyword **static** or **connected**.
as-number	(Optional) Autonomous system number.

Defaults

This command is disabled by default.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-number* argument was added.
12.0	The *prefix-list-name* argument was added.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

When redistributing networks, a routing process name can be specified as an optional trailing argument to the **distribute-list** command. Specifying an argument causes the access list or prefix list to be applied to only those routes derived from the specified routing process. After the process-specific access list or prefix list is applied, any access list or prefix list specified by a **distribute-list** command without a process name argument will be applied. Addresses not specified in the **distribute-list** command will not be advertised in outgoing routing updates.

Specify either an access list or a prefix list with the **distribute-list in** command.

Use the **gateway** keyword only with the **prefix-list** keyword.

Note To filter networks received in updates, use the **distribute-list in** command.

Examples

The following example causes only one network (network 131.108.0.0) to be advertised by a RIP routing process:

```
access-list 1 permit 131.108.0.0
access-list 1 deny 0.0.0.0 255.255.255.255
router rip
 network 131.108.0.0
 distribute-list 1 out
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
distribute-list in (RIP, IGRP, EIGRP)	Filters networks received in updates.
ip prefix-list	Creates an entry in a prefix list.

flash-update-threshold

To suppress regularly scheduled flash updates, use the **flash-update-threshold** command in router configuration mode. To return to the default state, use the no form of this command.

flash-update-threshold *seconds*

no flash-update-threshold

Syntax Description

seconds	The time interval in seconds for which the suppression of flash updates can be configured.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command suppresses flash updates when the arrival of a regularly scheduled update matches the number of seconds that is configured with the *seconds* argument. The range of seconds that can be configure is from 0 to 30 seconds. If the number of seconds matches the number of seconds or is less than the number seconds that is configured with the *seconds* argument, the flash update is suppressed. If the numbers seconds until the flash update arrives exceeds the number of seconds that is configured with the *seconds* argument, the flash update is not suppressed. The regular scheduled interval for flash updates and the configuration of the suppression of flash updates can be verified with the **show ip protocol** command.

Examples

The following example configures a router to suppress a regularly scheduled flash update if the update is due in 10 seconds or less:

```
router rip
 flash-update-threshold 10
```

Related Commands

Command	Description
show ip protocols	Displays the parameters and current state of the active routing protocol process.

input-queue

To adjust the depth of the Routing Information Protocol (RIP) input queue, use the **input-queue** command in router configuration mode. 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

depth	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.

Defaults

50

Command Modes

Router configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Consider using the **input-queue** command if you have a high-end router sending at high speed to a low-speed router that might not be able to receive at the high speed. Configuring this command will help prevent the routing table from losing information.

Examples

The following example sets the depth of the RIP input queue to 100:

```
input-queue 100
```

Related Commands

Command	Description
output-delay	Changes interpacket delay for RIP updates sent.

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** command in interface configuration mode. 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

name-of-chain	Enables authentication and specifies the group of keys that are valid.

Defaults

No authentication is provided for RIP packets.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

If no key chain is configured with the **key-chain** command, no authentication is performed on the interface (not even the default authentication).

Examples

The following example configures the interface to accept and send any key belonging to the key chain named trees:

```
ip rip authentication key-chain trees
```

Related Commands

Command	Description
key chain	Enables authentication for routing protocols.

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** command in interface configuration mode. 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.

Defaults

Clear text authentication is provided for RIP packets.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

RIP Version 1 does not support authentication.

Examples

The following example configures the interface to use MD5 authentication:

```
ip rip authentication mode md5
```

Related Commands

Command	Description
ip rip authentication key-chain	Enables authentication for RIP Version 2 packets and specifies the set of keys that can be used on an interface.
key chain	Enables authentication for routing protocols.

ip rip receive version

To specify a Routing Information Protocol (RIP) version to receive on an interface basis, use the **ip rip receive version** command in interface configuration mode. 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.

Defaults

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Use this command to override the default behavior of RIP as specified by the **version** command. This command applies only to the interface being configured. You can configure the interface to accept both RIP versions.

Examples

The following example configures the interface to receive both RIP Version 1 and Version 2 packets:

```
ip rip receive version 1 2
```

The following example configures the interface to receive only RIP Version 1 packets:

```
ip rip receive version 1
```

Related Commands

Command	Description
key chain	Enables authentication for routing protocols.
ip rip authentication key-chain	Enables authentication for RIP Version 2 packets and specifies the set of keys that can be used on an interface.
ip rip send version	Specifies a RIP version to send on an interface basis.
version	Specifies a RIP version used globally by the router.

ip rip send version

To specify a Routing Information Protocol (RIP) version to send on an interface basis, use the **ip rip send version** command in interface configuration mode. 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.

Defaults

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Use this command to override the default behavior of RIP as specified by the **version** command. This command applies only to the interface being configured.

Examples

The following example configures the interface to send both RIP Version 1 and Version 2 packets out the interface:

```
ip rip send version 1 2
```

The following example configures the interface to send only RIP Version 2 packets out the interface:

```
ip rip send version 2
```

Related Commands

Command	Description
ip rip receive version	Specifies a RIP version to receive on an interface basis.
version	Specifies a RIP version used globally by the router.

ip rip triggered

To enable triggered extensions to Routing Information Protocol (RIP), use the **ip rip triggered** command in interface configuration mode. 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.

Defaults

This command is disabled by default.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

When triggered extensions to RIP are enabled, routing updates are sent on the WAN only if one of the following events occurs:

- The router receives a specific request for a routing update. (Full database is sent.)
- Information from another interface modifies the routing database. (Only latest changes are sent.)
- The interface comes up or goes down. (Partial database is sent.)
- The router is first powered on, to ensure that at least one update is sent. (Full database is sent.)

You might want to enable this feature if you are using an on-demand circuit and you are charged for usage time. Fewer routing updates will incur lower usage costs.

Entries in the routing database can be either temporary or semipermanent. Entries learned from broadcasts on LANs are temporary; they will expire if not periodically refreshed by more broadcasts.

Entries learned from a triggered response on the WAN are semipermanent; they do not time out like other entries. Certain events can cause these routes to time out, such as the interface going down, or if the outgoing interface is the same as the incoming interface. Neighbor updates of the routes with a metric of 16 (infinity) mean the route is unreachable, and those routes are eventually removed from the routing table.

Examples

The following example enables triggered extensions to RIP:

```
interface serial 0
 ip rip triggered
```

Related Commands

Command	Description
show ip rip database	Displays the contents of the RIP private database when triggered extensions to RIP are enabled.

ip split-horizon (RIP)

To enable the split horizon mechanism, use the **ip split-horizon** command in interface configuration mode. 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.

Defaults

Default behavior varies with media type.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

For all interfaces except those for which either Frame Relay or Switched Multimegabit Data Service (SMDS) encapsulation is enabled, the default condition for this command is **ip split-horizon**; in other words, the split horizon feature is active. If the interface configuration includes either the **encapsulation frame-relay** or **encapsulation smds** command, then the default is for split horizon to be disabled. Split horizon is not disabled by default for interfaces using any of the X.25 encapsulations.

Note For networks that include links over X.25 packet switched networks (PSNs), the **neighbor** router configuration command can be used to defeat the split horizon feature. You can as an alternative *explicitly* specify the **no ip split-horizon** command in your configuration. However, if you do so you *must* similarly disable split horizon for all routers in any relevant multicast groups on that network.

Note If split horizon has been disabled on an interface and you want to enable it, use the **ip split-horizon** command to restore the split horizon mechanism.

Note In general, changing the state of the default for the **ip split-horizon** command is not recommended, unless you are certain that your application requires a change in order to properly advertise routes. If split horizon is disabled on a serial interface (and that interface is attached to a PSN), you *must* disable split horizon for all routers and access servers in any relevant multicast groups on that network.

Examples

The following simple example disables split horizon on a serial link. The serial link is connected to an X.25 network.

```
interface serial 0
encapsulation x25
no ip split-horizon
```

Related Commands

Command	Description
neighbor (RIP)	Defines a neighboring router with which to exchange routing information.

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** command in router configuration mode. To disable the configuration of the **ip summary-address rip** command, 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

ip-address	IP address to be summarized.
ip-network-mask	IP network mask that drives route summarization for the specified IP address.

Defaults

No default behavior or values.

Command Modes

Router configuration

Command History

Release	Modification
12.0(6)T	This command was introduced.

Usage Guidelines

The host name entries are not removed from NVRAM but are cleared in running memory.

Examples

In the following example the major network is 10.0.0.0. The summary address 10.2.0.0 overrides the autosummary address of 10.0.0.0, so that 10.2.0.0 is advertised out Ethernet interface 1 and 10.0.0.0 is not advertised.

Note If split horizon is enabled, neither autosummary nor interface summary addresses (those configured with the **ip summary-address rip** command) are advertised.

```
router rip
router interface e1
 ip address 10.1.1.1 255.255.255.0
 ip summary-address rip 10.2.0.0 255.255.0.0

no ip split-horizon

router rip
network 10.0.0.0

 neighbor 2.2.2.2 peer-group mygroup
```

Related Commands

Command	Description
auto-summary (RIP)	Restores the default behavior of automatic summarization of subnet routes into network-level routes.
ip split-horizon (RIP)	Enables the split horizon mechanism.

neighbor (RIP)

To define a neighboring router with which to exchange routing information, use the **neighbor** command in router configuration mode. To remove an entry, use the **no** form of this command.

neighbor *ip-address*

no neighbor *ip-address*

Syntax Description

ip-address	IP address of a peer router with which routing information will be exchanged.

Defaults

No neighboring routers are defined.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command permits the point-to-point (nonbroadcast) exchange of routing information. When it is used in combination with the **passive-interface** router configuration command, routing information can be exchanged between a subset of routers and access servers on a LAN.

Multiple **neighbor** commands can be used to specify additional neighbors or peers.

Examples

In the following example, RIP updates are sent to all interfaces on network 10.108.0.0 except Ethernet interface 1. However, in this case a **neighbor** router configuration command is included. This command permits the sending of routing updates to specific neighbors. One copy of the routing update is generated per neighbor.

```
router rip
 network 10.108.0.0
 passive-interface ethernet 1
 neighbor 10.108.20.4
```

Related Commands

Command	Description
passive-interface	Disables sending routing updates on an interface.

network (RIP)

To specify a list of networks for the Routing Information Protocol (RIP) routing process, use the **network** command in router configuration mode. To remove an entry, use the **no** form of this command.

network *ip-address*

no network *ip-address*

Syntax Description

ip-address	IP address of the network of directly connected networks.

Defaults

No networks are specified.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The network number specified must not contain any subnet information. There is no limit to the number of **network** commands you can use on the router. RIP routing updates will be sent and received only through interfaces on this network.

RIP sends updates to the interfaces in the specified networks. Also, if the network of an interface is not specified, the interface will not be advertised in any RIP update.

Examples

The following example defines RIP as the routing protocol to be used on all interfaces connected to networks 10.99.0.0 and 192.168.7.0:

```
router rip
 network 10.99.0.0
 network 192.168.7.0
```

Related Commands

Command	Description
router rip	Configures the RIP routing process.

offset-list

To add an offset to incoming and outgoing metrics to routes learned via Routing Information Protocol (RIP), use the **offset-list** command in router configuration mode. 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

access-list-number	Standard access list number to be applied. Access list number 0 indicates all access lists. If *offset* is 0, no action is taken. For IGRP, the offset is added to the delay component only.
access-list-name	Standard access list name to be applied.
in	Applies the access list to incoming metrics.
out	Applies the access list to outgoing metrics.
offset	Positive offset to be applied to metrics for networks matching the access list. If the offset is 0, no action is taken.
interface-type	(Optional) Interface type to which the offset list is applied.
interface-number	(Optional) Interface number to which the offset list is applied.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The *interface-type* and *interface-number* arguments were added.
11.2	The *access-list-name* argument was added.

Usage Guidelines

The offset value is added to the routing metric. An offset list with an interface type and interface number is considered extended and takes precedence over an offset list that is not extended. Therefore, if an entry passes the extended offset list and the normal offset list, the offset of the extended offset list is added to the metric.

Examples

In the following example, the router applies an offset of 10 to the delay component of a router only to access list 21:

```
offset-list 21 out 10
```

In the following example, the router applies an offset of 10 to routes learned from Ethernet interface 0:

```
offset-list 21 in 10 ethernet 0
```

output-delay

To change the interpacket delay for Routing Information Protocol (RIP) updates sent, use the **output-delay** command in router configuration mode. To remove the delay, use the **no** form of this command.

output-delay *delay*

no output-delay [*delay*]

Syntax Description

delay	Delay (in milliseconds) between packets in a multiple-packet RIP update. The range is from 8 to 50 milliseconds. The default is no delay.

Defaults

0 milliseconds

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Consider using this command if you have a high-end router sending at high speed to a low-speed router that might not be able to receive at the high speed. Configuring this command will help prevent the routing table from losing information.

Examples

The following example sets the interpacket delay to 10 milliseconds:

```
output-delay 10
```

router rip

To configure the Routing Information Protocol (RIP) routing process, use the **router rip** command in global configuration mode. 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.

Defaults

No RIP routing process is defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example shows how to begin the RIP routing process:

```
router rip
```

Related Commands

Command	Description
network (RIP)	Specifies a list of networks for the RIP process.

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** command in EXEC mode.

show ip rip database[*ip-address* {*mask*}]

Syntax Description

ip-address	(Optional) Address about which routing information should be displayed.
mask	Argument for the subnet mask. The subnet mask must also be specified if the IP address argument is entered.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(6)T	This command was introduced.

Usage Guidelines

Summary address entries will appear in the database only if relevant child routes are being summarized. When the last child route for a summary address becomes invalid, the summary address is also removed from the routing table.

The RIP private database is populated only if triggered extensions to RIP are enabled with the **ip rip triggered** command.

Examples

The following output shows a summary address entry for route 10.11.0.0/16, with three child routes active:

```
Router# show ip rip database
 10.0.0.0/8    auto-summary
 10.11.11.0/24    directly connected, Ethernet2
 10.1.0.0/8    auto-summary
 10.11.0.0/16    int-summary
 ^^^^^^^^^^^^^^^^^^^^^^^^^^
 10.11.10.0/24    directly connected, Ethernet3
 10.11.11.0/24    directly connected, Ethernet4
 10.11.12.0/24    directly connected, Ethernet5
```

The following is sample output from the **show ip rip database** command with a prefix and mask:

```
Router# show ip rip database 172.19.86.0 255.255.255.0
172.19.86.0/24
    [1] via 172.19.67.38, 00:00:25, Serial0
    [2] via 172.19.70.36, 00:00:14, Serial1
```

Table 3 describes the fields in the displays.

Table 3 show ip rip database Field Descriptions

Field	Description
10.0.0.0/16 auto-summary	Summary address entry.
10.11.11.0/24 directly connected, Ethernet0	Directly connected entry for Ethernet 0.
172.19.65.0/24 [1] via 172.19.70.36, 00:00:17, Serial0 [2] via 172.19.67.38, 00:00:25, Serial1	The destination 172.19.65.0/24 is learned via RIP. There are two sources advertising it. One is 172.19.70.36 via Serial interface0, and it was updated 17 seconds ago. The other source is 172.19.67.38 via Serial interface 1, and it was updated 25 seconds ago.

Command	Description
ip rip triggered	Enables triggered extensions of RIP.
ip summary-address rip	Configures a Cisco router running RIP Version 2 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 specifies the IP address and network mask that identify the routes to be summarized.
show ip protocols	Displays the parameters and current state of the active routing protocol process.

timers basic

To adjust Routing Information Protocol (RIP) network timers, use the **timers basic** command in router configuration mode. To restore the default timers, use the **no** form of this command.

timers basic *update invalid holddown flush*

no timers basic

Syntax Description

update	Rate (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol. The default is 30 seconds.
invalid	Interval of time (in seconds) after which a route is declared invalid. The interval should be at least three times the value of *update* time. The interval is measured from the last update received for the route. The route becomes invalid when there is an absence of updates during the *invalid* time that refresh the route. The route is marked inaccessible and advertised as unreachable. However, the route still forwards packets until the *flush* interval expires. The default is 180 seconds.
holddown	Interval (in seconds) during which routing information regarding better paths is suppressed. The interval should be at least three times the value of *update* time. A route 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 continues to forward packets until an update is received with a better metric or until the holddown time expires. When the holddown expires, routes advertised by other sources are accepted and the route is no longer inaccessible. The default is 180 seconds.
flush	Amount of time (in seconds) that must pass before the route is removed from the routing table. The interval is measured from the last update received for the route. The interval should be longer than the larger of the *invalid* and *holddown* values. If the interval is less than the sum of the *update* and *holddown* values, the proper holddown interval cannot elapse, which results in a new route being accepted before the holddown interval expires. The default is 240 seconds.

Defaults

update: 30 seconds
invalid: 180 seconds
holddown: 180 seconds
flush: 240 seconds

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The basic timing parameters for RIP are adjustable. Because RIP is executing a distributed, asynchronous routing algorithm, these timers must be the same for all routers and access servers in the network.

Note The current and default timer values can be seen by inspecting the output of the **show ip protocols** EXEC command. The relationships of the various timers should be preserved as described previously.

Examples

The following example sets updates to be broadcast every 5 seconds. If a router is not heard from in 15 seconds, the route is declared unusable. Further information is suppressed for an additional 15 seconds. At the end of the suppression period, the route is flushed from the routing table.

```
router rip
 timers basic 5  15  15  30
```

Note By setting a short update period, you run the risk of congesting slow-speed serial lines. A short update period can be a concern on faster-speed Ethernets and T1-rate serial lines. Also, if you have many routes in your updates, you can cause the routers to spend an excessive amount of time processing updates.

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** command in router configuration mode. 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.

Defaults

The behavior of this command is enabled by default.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command is applicable only to RIP and IGRP. The software ensures that the source IP address of incoming routing updates is on the same IP network as one of the addresses defined for the receiving interface.

Disabling split horizon on the incoming interface will also cause the system to perform this validation check.

For unnumbered IP interfaces (interfaces configured as IP unnumbered), no checking is performed.

Examples

The following example configures a router not to perform validation checks on the source IP address of incoming RIP updates:

```
router rip
 network 10.105.0.0
 no validate-update-source
```

version

To specify a Routing Information Protocol (RIP) version used globally by the router, use the **version** command in router configuration mode. 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.

Defaults

The software receives RIP Version 1 and Version 2 packets, but sends only Version 1 packets.

Command Modes

Router configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

To specify RIP versions used on an interface basis, use the **ip rip receive version** and **ip rip send version** commands.

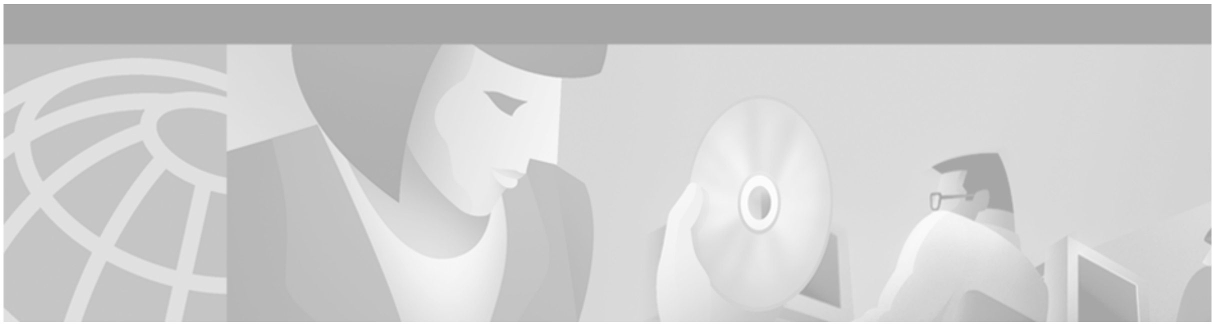
Examples

The following example enables the software to send and receive RIP Version 2 packets:

```
version 2
```

Related Commands

Command	Description
ip rip receive version	Specifies a RIP version to receive on an interface basis.
ip rip send version	Specifies a RIP version to send on an interface basis.
show ip protocols	Displays the parameters and current state of the active routing protocol process.



IGRP Commands

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

default-metric (IGRP)

To set metrics for IGRP or Enhanced IGRP (EIGRP), use the **default-metric** command in router configuration mode. 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

bandwidth	Minimum bandwidth of the route (in kbps). It can be 0 or any positive integer.
delay	Route delay (in tens of microseconds). It can be 0 or any positive number that is a multiple of 39.1 nanoseconds.
reliability	Likelihood of successful packet transmission expressed as a number from 0 to 255. The value 255 means 100 percent reliability; 0 means no reliability.
loading	Effective bandwidth of the route expressed as a number from 0 to 255 (255 is 100 percent loading).
mtu	Maximum transmission unit (MTU) size of the route in bytes. It can be 0 or any positive integer.

Defaults

Only connected routes and interface static routes can be redistributed without a default metric.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

A default metric is required to redistribute a protocol into IGRP or EIGRP, unless you use the **redistribute** command. Automatic metric translations occur between IGRP and EIGRP. You do not need default metrics to redistribute IGRP or EIGRP into itself.

Note The default metric command does not affect EIGRP-to-EIGRP or IGRP-to-EIGRP distribution. To configure EIGRP-to-EIGRP or IGRP-to-EIGRP distribution, use route maps.

Metric defaults have been carefully set to work for a wide variety of networks. Take great carewhen changing these values.

Keeping the same metrics is supported only when redistributing from IGRP, EIGRP, or static routes.

Examples

The following example takes redistributed Routing Information Protocol (RIP) metrics and translates them into IGRP metrics with values as follows: bandwidth = 1000, delay = 100, reliability = 250, loading = 100, and MTU = 1500.

```
router igrp 109
 network 172.16.0.0
 redistribute rip
 default-metric 1000 100 250 100 1500
```

Related Commands

Command	Description
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

distribute-list in (RIP, IGRP, EIGRP)

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* [**gateway** *prefix-list-name*]} **in** [*interface-type interface-number*]

no distribute-list {*access-list-number* | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*]} **in** [*interface-type interface-number*]

Syntax Description

access-list-number	Standard IP access list number. The list defines which networks are to be received and which are to be suppressed in routing updates.
prefix *prefix-list-name*	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.
gateway *prefix-list-name*	(Optional) Name of the prefix list to be applied to the gateway of the prefix being updated.
in	Applies the access list to incoming routing updates.
interface-type	(Optional) Interface type.
interface-number	(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.

Defaults

This command is disabled by default.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-number*, *interface-type*, and *interface-number* arguments were added.
12.0	The *prefix-list-name* argument was added.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

This command is not supported in Intermediate Sytem-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF).

Using a prefix list allows filtering based upon the prefix length, making it possible to filter either on the prefix list, the gateway, or both for incoming updates.

Specify either an access list or a prefix list with the **distribute-list in** command.

Use the **gateway** keyword only with the **prefix-list** keyword.

To suppress networks from being advertised in updates, use the **distribute-list out** command.

Examples

In the following example, the BGP routing process accepts only two networks—network 0.0.0.0 and network 192.168.0.0:

```
access-list 1 permit 0.0.0.0
access-list 1 permit 192.168.0.0
access-list 1 deny 0.0.0.0 255.255.255.255
router bgp
 network 192.168.0.0
 distribute-list 1 in
```

In the following example, The RIP process accepts only prefixes with prefix lengths of /8 to /24:

```
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
router rip
 network 192.168.0.0
 distribute-list prefix max24 in
```

In the following example, the RIP process filters on packet length and accepts routing updates from address 192.168.1.1 only:

```
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
ip prefix-list allowlist seq5 permit 192.168.1.1/32
router rip
 network 10.108.0.0
 distribute-list prefix max24 gateway allowlist in
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
distribute-list out (RIP, IGRP, EIGRP)	Suppresses networks from being advertised in updates.
ip prefix-list	Creates an entry in a prefix list.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

distribute-list out (RIP, IGRP, EIGRP)

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* [**gateway** *prefix-list-name*]} **out** [*interface-name* | *routing-process* | *as-number*]

no distribute-list {*access-list-number* | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*]} **out** [*interface-name* | *routing-process* | *as-number*]

Syntax Description

access-list-number	Standard IP access list number. The list defines which networks are to be received and which are to be suppressed in routing updates.
prefix *prefix-list-name*	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.
gateway *prefix-list-name*	(Optional) Name of the prefix list to be applied to the gateway of the prefix being updated.
out	Applies the access list to outgoing routing updates.
interface-name	(Optional) Name of a particular interface.
routing-process	(Optional) Name of a particular routing process, or the keyword **static** or **connected**.
as-number	(Optional) Autonomous system number.

Defaults

This command is disabled by default.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-number* argument was added.
12.0	The *prefix-list-name* argument was added.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

When redistributing networks, a routing process name can be specified as an optional trailing argument to the **distribute-list** command. Specifying an argument causes the access list or prefix list to be applied to only those routes derived from the specified routing process. After the process-specific access list or prefix list is applied, any access list or prefix list specified by a **distribute-list** command without a process name argument will be applied. Addresses not specified in the **distribute-list** command will not be advertised in outgoing routing updates.

Specify either an access list or a prefix list with the **distribute-list in** command.

Use the **gateway** keyword only with the **prefix-list** keyword.

Note To filter networks received in updates, use the **distribute-list in** command.

Examples

The following example causes only one network (network 192.168.0.0) to be advertised by a RIP routing process:

```
access-list 1 permit 192.168.0.0
access-list 1 deny 0.0.0.0 255.255.255.255
router rip
 network 192.168.0.0
 distribute-list 1 out
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
distribute-list in (RIP, IGRP, EIGRP)	Filters networks received in updates.
ip prefix-list	Creates an entry in a prefix list.

ip split-horizon (IGRP)

To enable the split horizon mechanism, use the **ip split-horizon** command in interface configuration mode. 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.

Defaults

Default behavior varies with media type.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

For all interfaces except those for which either Frame Relay or Switched Multimegabit Data Service (SMDS) encapsulation is enabled, the default condition for this command is **ip split-horizon**; in other words, the split horizon feature is active. If the interface configuration includes either the **encapsulation frame-relay** or **encapsulation smds** command, then the default is for split horizon to be disabled. Split horizon is not disabled by default for interfaces using any of the X.25 encapsulations.

Note For networks that include links over X.25 packet-switched networks (PSNs), the **neighbor** router configuration command can be used to defeat the split horizon feature. You can as an alternative *explicitly* specify the **no ip split-horizon** command in your configuration. However, if you do so you *must* similarly disable split horizon for all routers in any relevant multicast groups on that network.

Note If split horizon has been disabled on an interface and you want to enable it, use the **ip split-horizon** command to restore the split horizon mechanism.

Note In general, changing the state of the default for the **ip split-horizon** command is not recommended, unless you are certain that your application requires a change in order to advertise routes properly. If split horizon is disabled on a serial interface (and that interface is attached to a PSN), you *must* disable split horizon for all routers and access servers in any relevant multicast groups on that network.

Examples

The following simple example disables split horizon on a serial link. The serial link is connected to an X.25 network.

```
interface serial 0
 encapsulation x25
 no ip split-horizon
```

Related Commands

Command	Description
network (IGRP)	Specifies a list of networks for the IGRP or EIGRP routing process.

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** command in router configuration mode. 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.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The *holddown* state keeps new routing information from being used for a certain period of time. This function can prevent routing loops caused by slow convergence. It is sometimes advantageous to disable the *holddown* state to increase the ability of the network to quickly respond to topology changes; this command provides this function.

Use the **metric holddown** command if other routers or access servers within the IGRP autonomous system are not configured with the **no metric holddown** command. If all routers are not configured the same way, you increase the possibility of routing loops being created.

Examples

The following example disables metric holddown:

```
router igrp 15
 network 10.108.0.0
 network 192.168.7.0
 no metric holddown
```

Related Commands

Command	Description
metric maximum-hops	Causes the IP routing software to advertise as unreachable those routes with a hop count higher than is specified by the command (IGRP only).
metric weights (Enhanced IGRP)	Allows the tuning of the IGRP or EIGRP metric calculation.
timers basic (IGRP)	Adjusts IGRP network timers.

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** command in router configuration mode. 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

hops-number	Maximum hop count (in decimal). The default value is 100 hops; the maximum number of hops that can be specified is 255.

Defaults

100 hops

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command provides a safety mechanism that breaks any potential *count-to-infinity* problems. It causes the IP routing software to advertise as unreachable routes with a hop count greater than the value assigned to the *hops-number* argument.

Examples

In the following example, a router in autonomous system 71 attached to network 10.0.0.0 wants a maximum hop count of 200, doubling the default. The network administrators configured the router hop count to 200 because they have a complex WAN that can generate a large hop count under normal (nonlooping) operations.

```
router igrp 71
 network 10.0.0.0
 metric maximum-hops 200
```

Related Commands

Command	Description
metric holddown	Keeps new IGRP routing information from being used for a certain period of time.
metric weights (Enhanced IGRP)	Allows the tuning of the IGRP or EIGRP metric calculations.

metric weights (IGRP)

To allow the tuning of the IGRP or Enhanced IGRP (EIGRP) metric calculations, use the **metric weights** command in router configuration mode. 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

tos	Type of service must always be zero.
k1 k2 k3 k4 k5	Constants that convert an IGRP or EIGRP metric vector into a scalar quantity.

Defaults

tos: 0

k1: 1

k2: 0

k3: 1

k4: 0

k5: 0

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command to alter the default behavior of IGRP routing and metric computation and allow the tuning of the IGRP metric calculation for a particular type of service (ToS).

If k5 equals 0, the composite IGRP or EIGRP metric is computed according to the following formula:

metric = [k1 * bandwidth + (k2 * bandwidth)/(256 - load) + k3 * delay]

If k5 does not equal zero, an additional operation is performed:

metric = metric * [k5/(reliability + k4)]

Bandwidth is inverse minimum bandwidth of the path in BPS scaled by a factor of $2.56 * 10^{12}$. The range is from a 1200-bps line to 10 terabits per second.

Delay is in units of 10 microseconds. The range of delay is from 10 microseconds to 168 seconds. A delay of all ones indicates that the network is unreachable.

The delay parameter is stored in a 32-bit field, in increments of 39.1 nanoseconds. The range of delay is from 1 (39.1 nanoseconds) to hexadecimal FFFFFFFF (decimal 4,294,967,040 nanoseconds). A delay of all ones (that is, a delay of hexadecimal FFFFFFFF) indicates that the network is unreachable.

Table 4 lists the default values used for several common media.

Table 4 Bandwidth Values by Media Type

Media Type	Delay	Bandwidth
Satellite	5120 (2 seconds)	5120 (500 megabits)
Ethernet	25600 (1 [ms])	256000 (10 megabits)
1.544 Mbps	512000 (20,000 [ms])	1,657,856 bits
64 kbps	512000 (20,000 [ms])	40,000,000 bits
56 kbps	512000 (20,000 [ms])	45,714,176 bits
10 kbps	512000 (20,000 [ms])	256,000,000 bits
1 kbps	512000 (20,000 [ms])	2,560,000,000 bits

Reliability is given as a fraction of 255. That is, 255 is 100 percent reliability or a perfectly stable link.

Load is given as a fraction of 255. A load of 255 indicates a completely saturated link.

Examples

The following example sets the metric weights to slightly different values than the defaults:

```
router igrp 109
 network 192.168.0.0
 metric weights 0 2 0 2 0 0
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.
delay (interface)	Sets a delay value for an interface.
metric holddown	Keeps new IGRP routing information from being used for a certain period of time.
metric maximum-hops	Causes the IP routing software to advertise as unreachable those routes with a hop count higher than is specified by the command (IGRP only).

neighbor (IGRP)

To define a neighboring router with which to exchange routing information, use the **neighbor** command in router configuration mode. To remove an entry, use the **no** form of this command.

neighbor *ip-address*

no neighbor *ip-address*

Syntax Description

ip-address	IP address of a peer router with which routing information will be exchanged.

Defaults

No neighboring routers are defined.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command permits the point-to-point (nonbroadcast) exchange of routing information. When used in combination with the **passive-interface** router configuration command, routing information can be exchanged between a subset of routers and access servers on a LAN.

Multiple **neighbor** commands can be used to specify additional neighbors or peers.

Examples

In the following example, Interior Gateway Routing Protocol (IGRP) updates are sent to all interfaces on network 192.168.0.0 except Ethernet interface 1. However, in this case a **neighbor** router configuration command is included. This command permits the sending of routing updates to specific neighbors. One copy of the routing update is generated per neighbor.

```
router igrp 109
 network 192.168.0.0
 passive-interface ethernet 1
 neighbor 192.168.20.4
```

Related Commands

Command	Description
passive-interface	Disables sending routing updates on an interface.

network (IGRP)

To specify a list of networks for the Enhanced Interior Gateway Routing Protocol (IGRP) routing process, use the **network** command in router configuration mode. To remove an entry, use the **no** form of this command.

network *network-number*

no network *network-number*

Syntax Description

network-number	IP address of the directly connected networks.

Defaults

No networks are specified.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The network number specified must not contain any subnet information. There is no limit to the number of **network** commands you can use on the router.

IGRP or Enhanced IGRP (EIGRP) sends updates to the interfaces in the specified networks. Also, if a network interface is not specified, it will not be advertised in any IGRP or EIGRP update.

Examples

The following example configures a router for IGRP and assigns autonomous system 109. The **network** commands indicate the networks directly connected to the router.

```
router igrp 109
 network 10.108.0.0
 network 192.168.7.0
```

Related Commands

Command	Description
router igrp	Configures the IGRP routing process.

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** command in router configuration mode. 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

access-list-number	Standard access list number to be applied. Access list number 0 indicates all access lists. If the *offset* argument is 0, no action is taken. For IGRP, the offset is added to the delay component only.
access-list-name	Standard access name to be applied.
in	Applies the access list to incoming metrics.
out	Applies the access list to outgoing metrics.
offset	Positive offset to be applied to metrics for networks matching the access list. If the offset is 0, no action is taken.
interface-type	(Optional) Interface type to which the offset list is applied.
interface-number	(Optional) Interface number to which the offset list is applied.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The *interface-type* and *interface-number* arguments were added.
11.2	The *access-list-name* argument was added.

Usage Guidelines

The offset value is added to the routing metric. An offset list with an interface type and interface number is considered extended and takes precedence over an offset list that is not extended. Therefore, if an entry passes the extended offset list and the normal offset list, the offset of the extended offset list is added to the metric.

Examples

In the following example, the router applies an offset of 10 to the delay component of the router only to access list 121:

```
offset-list 21 out 10
```

In the following example, the router applies an offset of 10 to routes learned from Ethernet interface 0:

```
offset-list 21 in 10 ethernet 0
```

router igrp

To configure the Interior Gateway Routing Protocol (IGRP) routing process, use the **router igrp** command in global configuration mode. 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

as-number	Autonomous system number that identifies the routes to the other IGRP routers. It is also used to tag the routing information.

Defaults

No IGRP routing process is defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

It is not necessary to have a registered autonomous system number to use IGRP. If you do not have a registered number, you are free to create your own. We recommend that if you do have a registered number, you use it to identify the IGRP process.

Examples

The following example configures an IGRP routing process and assigns process number 109:

```
router igrp 109
```

Related Commands

Command	Description
network (IGRP)	Specifies a list of networks for the IGRP or EIGRP routing process.

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

bandwidth	Metric value or IGRP bandwidth of the route, in kbps. It can be in the range from 0 to 4294967295.
delay	Route delay (in tens of microseconds). It can be in the range from 0 to 4294967295.
reliability	Likelihood of successful packet transmission expressed as a number from 0 to 255. The value 255 means 100 percent reliability; 0 means no reliability.
loading	Effective bandwidth of the route expressed as a number from 0 to 255 (255 is 100 percent loading).
mtu	Minimum maximum transmission unit (MTU) size of the route, in bytes. It can be in the range from 0 to 4294967295.

Defaults

No metric will be set in the route map.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Note We recommend that you consult your Cisco technical support representative before changing the default value.

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution *set actions* to be performed when all of the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

The following example sets the bandwidth to 10,000, the delay to 10, the reliability to 255, the loading to 1, and the MTU to 1500:

```
set metric 10000 10 255 1 1500
```

Related Commands

Command	Description
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.

timers basic (IGRP)

To adjust Interior Gateway Routing Protocol (IGRP) network timers, use the **timers basic** command in router configuration mode. To restore the default timers, use the **no** form of this command.

timers basic *update invalid holddown flush* [*sleeptime*]

no timers basic

Syntax Description

update	Rate (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol. The default is 90 seconds.
invalid	Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the *update* argument. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters *holddown* state. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. The default is 270 seconds.
holddown	Interval (in seconds) during which routing information regarding better paths is suppressed. It should be at least three times the value of the *update* 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 *holddown* expires, routes advertised by other sources are accepted and the route is no longer inaccessible. The default is 280 seconds.
flush	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 *invalid* argument and the *holddown* argument. 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. The default is 630 seconds.
sleeptime	(Optional) Interval (in milliseconds) for postponing routing updates in the event of a flash update. The value of the *sleeptime* argument should be less than the *update* value. If the *sleeptime* value is greater than the *update* value, routing tables will become unsynchronized. The default is 0 milliseconds.

Defaults

update: 90 seconds

invalid: 270 seconds

holddown: 280 seconds

flush: 630 seconds

sleeptime: 0 milliseconds

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The basic timing parameters for IGRP are adjustable. Because IGRP is executing a distributed, asynchronous routing algorithm, these timers must be the same for all routers and access servers in the network.

Note The current and default timer values can be seen by inspecting the output of the **show ip protocols** EXEC command. The relationships of the various timers should be preserved as described previously.

Examples

The following example sets updates to be broadcast every 5 seconds. If a router is not heard from in 15 seconds, the route is declared unusable. Further information is suppressed for an additional 15 seconds. At the end of the suppression period, the route is flushed from the routing table.

```
router igrp 109
 timers basic 5  15  15  30
```

Note By setting a short update period, you run the risk of congesting slow-speed serial lines; however, this is not a serious concern on faster-speed Ethernets and T1-rate serial lines. Also, if you have many routes in your updates, you can cause the routers to spend an excessive amount of time processing updates.

Related Commands

Command	Description
show ip protocols	Displays the parameters and current state of the active routing protocol process.

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** command in router configuration mode. 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.

Defaults

Traffic is distributed proportionately to the ratios of the metrics.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command applies to Interior Gateway Routing Protocol (IGRP) and Enhanced IGRP (EIGRP) routing protocols only. With the default setting, routes that have higher metrics represent less-preferable routes and get less traffic.

Examples

In the following example, traffic is balanced across multiple routes:

```
router igrp 5
 traffic-share balanced
 variance 1
```

Related Commands

Command	Description
variance (IGRP)	Controls load balancing in an EIGRP and IGRP internetwork.

variance (IGRP)

To control load balancing in an Enhanced IGRP-based internetwork, use the **variance** command in router configuration mode. To reset the variance to the default value, use the **no** form of this command.

variance *multiplier*

no variance

Syntax Description

multiplier	Metric value used for load balancing. It can be a value from 1 to 128. The default is 1, which means equal-cost load balancing.

Defaults

1 (equal-cost load balancing)

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Setting a variance value lets the Cisco IOS software determine the feasibility of a potential route. A route is feasible if the next router in the path is closer to the destination than the current router and if the metric for the entire path is within the variance. Only paths that are feasible can be used for load balancing and included in the routing table.

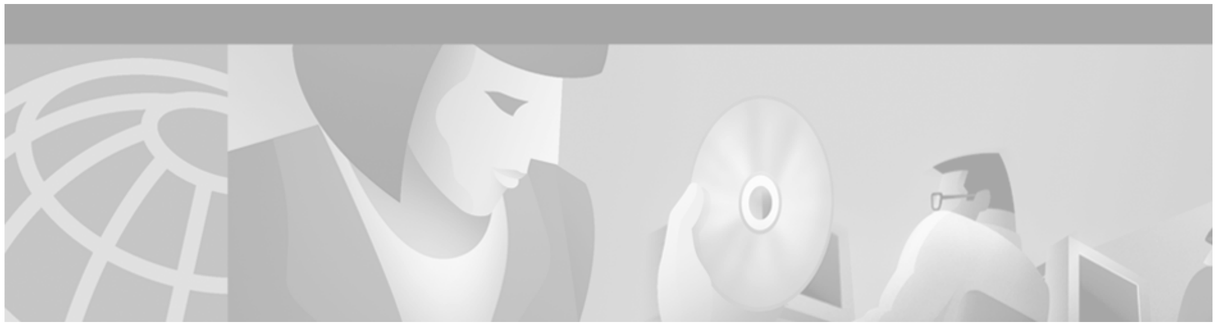
If the following two conditions are met, the route is deemed feasible and can be added to the routing table:

- The local best metric must be greater than the metric learned from the next router.
- The multiplier times the local best metric for the destination must be greater than or equal to the metric through the next router.

Examples

The following example sets a variance value of 4:

```
router igrp 109
 variance 4
```



OSPF Commands

Use the commands in this chapter to configure and monitor the Open Shortest Path First (OSPF) routing protocol. For OSPF configuration information and examples, refer to the "Configuring OSPF" chapter of the *Cisco IOS IP Configuration Guide*.

area authentication

To enable authentication for an OSPF area, use the **area authentication** command in router configuration mode. 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

area-id	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 *area-id* argument.

Defaults

Type 0 authentication (no authentication)

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.0	The **message-digest** keyword was added.

Usage Guidelines

Specifying authentication for an area sets the authentication to Type 1 (simple password) as specified in RFC 1247. If this command is not included in the configuration file, authentication of Type 0 (no authentication) is assumed.

The authentication type must be the same for all routers and access servers in an area. The authentication password for all OSPF routers on a network must be the same if they are to communicate with each other via OSPF. Use the **ip ospf authentication-key** interface command to specify this password.

If you enable MD5 authentication with the **message-digest** keyword, you must configure a password with the **ip ospf message-digest-key** interface command.

To remove the authentication specification for an area, use the **no** form of this command with the **authentication** keyword.

Note To remove the specified area from the software configuration, use the **no area** *area-id* command (with no other keywords). That is, the **no area** *area-id* command removes all area options, such as **area authentication**, **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Examples

The following example mandates authentication for areas 0 and 10.0.0.0 of OSPF routing process 201. Authentication keys are also provided.

```
interface ethernet 0
 ip address 192.168.251.201 255.255.255.0
 ip ospf authentication-key adcdefgh
!
interface ethernet 1
 ip address 10.56.0.201 255.255.0.0
 ip ospf authentication-key ijklmnop
!
router ospf 201
 network 10.0.0.0 0.255.255.255 area 10.0.0.0
 network 192.168.0.0 0.0.255.255 area 0
 area 10.0.0.0 authentication
 area 0 authentication
```

Related Commands

Command	Description
area default-cost	Specifies a cost for the default summary route sent into a stub area.
area stub	Defines an area as a stub area.
ip ospf authentication-key	Assigns a password to be used by neighboring routers that are using the simple password authentication of OSPF.
ip ospf message-digest-key	Enables OSPF MD5 authentication.

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** command in router configuration mode. 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

area-id	Identifier for the stub or NSSA. The identifier can be specified as either a decimal value or as an IP address.
cost	Cost for the default summary route used for a stub or NSSA. The acceptable value is a 24-bit number.

Defaults

cost: 1

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The command is used only on an Area Border Router (ABR) attached to a stub or NSSA.

There are two stub area router configuration commands: the **stub** and **default-cost** options of the **area** command. In all routers and access servers attached to the stub area, the area should be configured as a stub area using the **stub** option of the **area** command. Use the **default-cost** option only on an ABR attached to the stub area. The **default-cost** option provides the metric for the summary default route generated by the ABR into the stub area.

Note To remove the specified area from the software configuration, use the **no area** *area-id* command (with no other keywords). That is, the **no area** *area-id* command removes all area options, such as **area authentication**, **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Examples

The following example assigns a default cost of 20 to stub network 10.0.0.0:

```
interface ethernet 0
 ip address 10.56.0.201 255.255.0.0
!
router ospf 201
 network 10.0.0.0 0.255.255.255 area 10.0.0.0
 area 10.0.0.0 stub
 area 10.0.0.0 default-cost 20
```

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
area stub	Defines an area as a stub area.

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

area-id	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.
prefix-list-name	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.

Defaults

This command has no default behavior.

Command Modes

Router configuration

Command History

Release	Modification
12.0(15)S	This command was introduced.

Usage Guidelines

With this feature enabled in the "in" direction, all type 3 LSAs originated by the ABR to this area, based on information from all other areas, are filtered by the prefix list. Type 3 LSAs that were originated as a result of the **area-range** command in another area are treated like any other type 3 LSA that was originated individually. Any prefix that does not match an entry in the prefix list is implicitly denied.

With this feature enabled in the "out" direction, all type 3 LSAs advertised by the ABR, based on information from this area to all other areas, are filtered by the prefix list. If the **area-range** command has been configured for this area, type 3 LSAs that correspond to the area range are sent to all other areas, only if there is at least one prefix in the area range that matches an entry in the prefix list.

If all specific prefixes are denied by the prefix list, type 3 LSAs that correspond to the **area-range** command will not be sent to any other area. Prefixes that are not permitted by the prefix list are implicitly denied.

Examples

The following example filters prefixes that are sent from all other areas to area 1:

```
area 1 filter-list prefix-list AREA_1 in
```

area nssa

To configure an area as a not-so-stubby area (NSSA), use the **area nssa** command in router configuration mode. To remove the NSSA distinction from the area, use the **no** form of this command.

area *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric**] [**metric-type**]] [**no-summary**]

no area *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric**] [**metric-type**]] [**no-summary**]

Syntax Description

area-id	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 takes effect only on NSSA ABR or NSSA Autonomous System Boundary Router (ASBR).
metric	OSPF default metric.
metric-type	OSPF metric type for default routes.
no-summary	(Optional) Allows an area to be a not-so-stubby area but not have summary routes injected into it.

Defaults

No NSSA area is defined.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

To remove the specified area from the software configuration, use the **no area** *area-id* command (with no other keywords). That is, the **no area** *area-id* command removes all area options, such as **area authentication**, **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Examples

The following example makes area 1 an NSSA area:

```
router ospf 1
 redistribute rip subnets
 network 172.19.92.0 0.0.0.255 area 1
 area 1 nssa
```

area range

To consolidate and summarize routes at an area boundary, use the **area range** command in router configuration mode. To disable this function, use the **no** form of this command.

area *area-id* **range** *ip-address mask* [**advertise** | **not-advertise**] [**cost** *cost*]

no area *area-id* **range** *ip-address mask* [**advertise** | **not-advertise**] [**cost** *cost*]

Syntax Description

area-id	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.
ip-address	IP address.
mask	IP address mask.
advertise	(Optional) Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (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.
cost *cost*	(Optional) Metric or cost for this summary route, which is used during OSPF SPF calculation to determine the shortest paths to the destination. The value can be 0 to 16777215.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2	The **cost** *cost* keyword and argument were added.

Usage Guidelines

The **area range** command is used only with Area Border Routers (ABRs). It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This behavior is called *route summarization*.

Multiple **area** router configuration commands specifying the **range** option can be configured. Thus, OSPF can summarize addresses for many different sets of address ranges.

Note To remove the specified area from the software configuration, use the **no area** *area-id* command (with no other keywords). That is, the **no area** *area-id* command removes all area options, such as **area authentication**, **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Examples

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 10.0.0.0 and for all hosts on network 192.168.110.0:

```
interface ethernet 0
 ip address 192.168.110.201 255.255.255.0
!
interface ethernet 1
 ip address 192.168.120.201 255.255.255.0
!
router ospf 201
 network 192.168.110.0 0.0.0.255 area 0
 area 10.0.0.0 range 10.0.0.0 255.0.0.0
 area 0 range 192.168.110.0 255.255.0.0 cost 60
```

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
area default-cost	Specifies a cost for the default summary route sent into a stub area.
area nssa	Configures an area as an NSSA.
area stub	Defines an area as a stub area.
area virtual-link	Defines an OSPF virtual link.

area stub

To define an area as a stub area, use the **area stub** command in router configuration mode. 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

area-id	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.

Defaults

No stub area is defined.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You must configure the **area stub** command on all routers and access servers in the stub area. Use the **area** router configuration command with the **default-cost** option to specify the cost of a default internal router sent into a stub area by an ABR.

There are two stub area router configuration commands: the **stub** and **default-cost** options of the **area** router configuration command. In all routers attached to the stub area, the area should be configured as a stub area using the **stub** option of the **area** command. Use the **default-cost** option only on an ABR attached to the stub area. The **default-cost** option provides the metric for the summary default route generated by the ABR into the stub area.

To further reduce the number of link-state advertisements (LSAs) sent into a stub area, you can configure the **no-summary** keyword on the ABR to prevent it from sending summary LSAs (LSA type 3) into the stub area.

Note To remove the specified area from the software configuration, use the **no area** *area-id* command (with no other keywords). That is, the **no area** *area-id* command removes all area options, such as **area authentication**, **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Examples

The following example assigns a default cost of 20 to stub network 10.0.0.0:

```
interface ethernet 0
 ip address 10.56.0.201 255.255.0.0
!
router ospf 201
 network 10.0.0.0 0.255.255.255 area 10.0.0.0
 area 10.0.0.0 stub
 area 10.0.0.0 default-cost 20
```

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
area default-cost	Specifies a cost for the default summary route sent into a stub area.

area virtual-link

To define an OSPF virtual link, use the **area virtual-link** command in router configuration mode 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

area-id	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.
router-id	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 *seconds*	(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 *seconds*	(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 *seconds*	(Optional) Estimated time (in seconds) required 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 *seconds*	(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 *key*	(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 *key-id* **md5** *key*	(Optional) Key identifier and password to be used by neighboring routers and this router for Message Digest 5 (MD5) authentication. The *key-id* argument is a number in the range from 1 to 255. The *key* 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.

Defaults

area-id: No area ID is predefined.

router-id: No router ID is predefined.

hello-interval *seconds*: 10 seconds

retransmit-interval *seconds*: 5 seconds

transmit-delay *seconds*: 1 second

dead-interval *seconds*: 40 seconds

authentication-key *key*: No key is predefined.

message-digest-key *key-id* **md5** *key*: No key is predefined.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.0	The **message-digest-key** *key-id* **md5** *key* keywords and arguments were added.
12.0	The **authentication**, **message-digest**, and **null** keywords were added.

Usage Guidelines

In OSPF, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link.

The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue.

The setting of the retransmit interval should be conservative, or needless retransmissions will result. The value should be larger for serial lines and virtual links.

The transmit delay value should take into account the transmission and propagation delays for the interface.

The Cisco IOS software will use the specified authentication key only when authentication is enabled for the backbone with the **area** *area-id* **authentication** router configuration command.

The two authentication schemes, simple text and MD5 authentication, are mutually exclusive. You can specify one or the other or neither. Any keywords and arguments you specify after **authentication-key** *key* or **message-digest-key** *key-id* **md5** *key* are ignored. Therefore, specify any optional arguments before such a keyword-argument combination.

Note Each virtual link neighbor must include the transit area ID and the corresponding virtual link neighbor router ID in order for a virtual link to be properly configured. Use the **show ip ospf** EXEC command to see the router ID.

Note To remove the specified area from the software configuration, use the **no area** *area-id* command (with no other keywords). That is, the **no area** *area-id* command removes all area options, such as **area authentication**, **area default-cost**, **area nssa**, **area range**, **area stub**, and **area virtual-link**.

Examples

The following example establishes a virtual link with default values for all optional parameters:

```
router ospf 201
 network 10.0.0.0 0.255.255.255 area 10.0.0.0
 area 10.0.0.0 virtual-link 10.3.4.5
```

The following example establishes a virtual link with MD5 authentication:

```
router ospf 201
 network 10.0.0.0 0.255.255.255 area 10.0.0.0
 area 10.0.0.0 virtual-link 10.3.4.5 message-digest-key 3 md5 sa5721bk47
```

Note If MD5 authentication is used for the virtual link, then all other routers in area 0 must use MD5 authentication.

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
service password-encryption	Encrypts passwords.
show ip ospf	Displays general information about OSPF routing processes.

auto-cost

To control how OSPF calculates default metrics for the interface, use the **auto-cost** command in router configuration mode. 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 *ref-bw*	Rate in Mbps (bandwidth). The range is from 1 to 4294967; the default is 100.

Defaults

100 Mbps

Command Modes

Router configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

In Cisco IOS Release 10.3 and later releases, by default OSPF will calculate the OSPF metric for an interface according to the bandwidth of the interface. For example, a 64K link will get a metric of 1562, and a T1 link will have a metric of 64.

The OSPF metric is calculated as the *ref-bw* value divided by the bandwidth, with *ref-bw* equal to 10^8 by default, and bandwidth determined by the **bandwidth** command. The calculation gives FDDI a metric of 1.

If you have multiple links with high bandwidth (such as FDDI or ATM), you might want to use a larger number to differentiate the cost on those links.

The value set by the **ip ospf cost** command overrides the cost resulting from the **auto-cost** command.

Examples

The following example changes the cost of the FDDI link to 10, while the gigabit Ethernet link remains at a cost of 1. Thus, the link costs are differentiated.

```
router ospf 1
 auto-cost reference-bandwidth 1000
```

Related Commands

Command	Description
ip ospf cost	Explicitly specifies the cost of sending a packet on an interface.

clear ip ospf

To clear redistribution based on the OSPF routing process ID, use the **clear ip ospf** command in privileged EXEC mode.

clear ip ospf [*pid*] {**process** | **redistribution** | **counters** [**neighbor** [*neighbor-interface*] [*neighbor-id*]]}

Syntax Description

pid	(Optional) Process ID.
process	Reset OSPF process.
redistribution	Clear OSPF route redistribution.
counters	OSPF counters.
neighbor	(Optional) Neighbor statistics per interface.
neighbor-interface	(Optional) Neighbor interface.
neighbor-id	(Optional) Neighbor ID.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Use the *pid* option to clear only one OSPF process. If the *pid* option is not specified, all OSPF processes are cleared.

Examples

The following example clears all OSPF processes:

```
clear ip ospf process
```

compatible rfc1583

To restore the method used to calculate summary route costs per RFC 1583, use the **compatible rfc1583** command in router configuration mode. 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.

Defaults

Compatible with RFC 1583.

Command Modes

Router configuration

Command History

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

Usage Guidelines

This command is backward compatible with Cisco IOS Release 12.0.

To minimize the chance of routing loops, all OSPF routers in an OSPF routing domain should have RFC compatibility set identically.

Because of the introduction of RFC 2328, *OSPF Version 2*, the method used to calculate summary route costs has changed. Use the **no compatible rfc1583** command to enable the calculation method used per RFC 2328.

Examples

The following example specifies that the router process is compatible with RFC 1583:

```
router ospf 1
  compatible rfc1583
 !
```

default-information originate (OSPF)

To generate a default external route into an OSPF routing domain, use the **default-information originate** command in router configuration mode. 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 *metric-value*	(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 *type-value*	(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 *map-name*	(Optional) Routing process will generate the default route if the route map is satisfied.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Whenever you use the **redistribute** or the **default-information** router configuration command to redistribute routes into an OSPF routing domain, the Cisco IOS software automatically becomes an Autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a *default route* into the OSPF routing domain. The software still must have a default route for itself before it generates one, except when you have specified the **always** keyword.

When you use this command for the OSPF process, the default network must reside in the routing table, and you must satisfy the **route-map** *map-name* keyword and argument. Use the **default-information originate always route-map** *map-name* form of the command when you do not want the dependency on the default network in the routing table.

Notes:

- If you use the **ip prefix-list** command with the **default-information originate** command to generate default routes, specify only IP adress matching. Avoid using the **ge** and **le** keywords.

  For example, the following command works:

  ```
  ip prefix-list anyrtcondition seq 5 permit 0.0.0.0/0
  ```

  However, the following command is not supported:

  ```
  ip prefix-list anyrtcondition seq 5 permit 0.0.0.0/0 le 32
  ```

- Using the **ip prefix-list** command with the **route-map** and **match ip next-hop** commands is not supported. Only IP address match clauses are supported.

Examples

The following example specifies a metric of 100 for the default route redistributed into the OSPF routing domain and an external metric type of Type 1:

```
router ospf 109
 redistribute igrp 108 metric 100 subnets
 default-information originate metric 100 metric-type 1
```

Related Commands

Command	Description
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

default-metric (OSPF)

To set default metric values for the OSPF routing protocol, use the **default-metric** command in router configuration mode. To return to the default state, use the **no** form of this command.

default-metric *metric-value*

no default-metric *metric-value*

Syntax Description

metric-value	Default metric value appropriate for the specified routing protocol.

Defaults

Built-in, automatic metric translations, as appropriate for each routing protocol

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **default-metric** command is used in conjunction with the **redistribute** router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

Examples

The following example shows a router in autonomous system 109 using both the Routing Information Protocol (RIP) and the OSPF routing protocols. The example advertises OSPF-derived routes using RIP and assigns the Internal Gateway Routing Protocol (IGRP)-derived routes a RIP metric of 10.

```
router rip
 default-metric 10
 redistribute ospf 109
```

Related Commands

Command	Description
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

distance ospf

To define OSPF route administrative distances based on route type, use the **distance ospf** command in router configuration mode. 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 *dist1*	(Optional) Sets the distance for all routes within an area. The default value is 110.
inter-area *dist2*	(Optional) Sets the distance for all routes from one area to another area. The default value is 110.
external *dist3*	(Optional) Sets the distance for routes from other routing domains, learned by redistribution. The default value is 110.

Defaults

dist1: 110

dist2: 110

dist3: 110

Command Modes

Router configuration

Command History

Release	Modification
11.1(14)	This command was introduced.

Usage Guidelines

You must specify at least one of the keyword-argument pairs.

This command performs the same function as the **distance** command used with an access list. However, the **distance ospf** command allows you to set a distance for an entire group of routes, rather than a specific route that passes an access list.

A common reason to use the **distance ospf** command is when you have multiple OSPF processes with mutual redistribution, and you want to prefer internal routes from one over external routes from the other.

Examples

The following example changes the external distance to 200, making the route less reliable:

Router A Configuration

```
router ospf 1
 redistribute ospf 2 subnet
 distance ospf external 200
!
router ospf 2
 redistribute ospf 1 subnet
 distance ospf external 200
```

Router B Configuration

```
router ospf 1
 redistribute ospf 2 subnet
 distance ospf external 200
!
router ospf 2
 redistribute ospf 1 subnet
 distance ospf external 200
```

Related Commands

Command	Description
distance (IP)	Defines an administrative distance.

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** command in router configuration mode. 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.

Defaults

This command is disabled by default. Each MOSPF packet causes the router to send a syslog message.

Command Modes

Router configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Cisco routers do not support LSA Type 6 MOSPF packets, and they generate syslog messages if they receive such packets. If the router is receiving many MOSPF packets, you might want to configure the router to ignore the packets and thus prevent a large number of syslog messages.

Examples

The following example configures the router to suppress the sending of syslog messages when it receives MOSPF packets:

```
router ospf 109
 ignore lsa mospf
```

ip ospf authentication

To specify the authentication type for an interface, use the **ip ospf authentication** command in interface configuration mode. 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.

Defaults

The area default is no authentication (null authentication).

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Before using the **ip ospf authentication** command, configure a password for the interface using the **ip ospf authentication-key** command. If you use the **ip ospf authentication message-digest** command, configure the message-digest key for the interface with the **ip ospf message-digest-key** command.

For backward compatibility, authentication type for an area is still supported. If the authentication type is not specified for an interface, the authentication type for the area will be used (the area default is null authentication).

Examples

The following example enables message-digest authentication:

```
ip ospf authentication message-digest
```

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
ip ospf authentication-key	Assigns a password to be used by neighboring routers that are using the simple password authentication of OSPF.
ip ospf message-digest-key	Enables OSPF MD5 authentication.

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** command in interface configuration mode. 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

password	Any continuous string of characters that can be entered from the keyboard up to 8 bytes in length.

Defaults

No password is specified.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The password created by this command is used as a “key” that is inserted directly into the OSPF header when the Cisco IOS software originates 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 exchange OSPF information.

Note The Cisco IOS software will use this key only when authentication is enabled for an area with the **area authentication** router configuration command.

Examples

The following example enables the authentication key with the string yourpass:

```
ip ospf authentication-key yourpass
```

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
ip ospf authentication	Specifies authentication type for an interface.

ip ospf cost

To explicitly specify the cost of sending a packet on an interface, use the **ip ospf cost** command in interface configuration mode. 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

interface-cost	Unsigned integer value expressed as the link-state metric. It can be a value in the range from 1 to 65535.

Defaults

No default cost is predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can set the metric manually using this command, if you need to change the default. Using the **bandwidth** command changes the link cost as long as this command is not used.

The link-state metric is advertised as the link cost in the router link advertisement. We do not support type of service (tos), so you can assign only one cost per interface.

In general, the path cost is calculated using the following formula:

10^8 / bandwidth

Using this formula, the default path costs were calculated as noted in the following list. If these values do not suit your network, you can use your own method of calculating path costs.

- 56-kbps serial link—Default cost is 1785
- 64-kbps serial link—Default cost is 1562
- T1 (1.544-Mbps serial link)—Default cost is 64
- E1 (2.048-Mbps serial link)—Default cost is 48
- 4-Mbps Token Ring—Default cost is 25
- Ethernet—Default cost is 10
- 16-Mbps Token Ring—Default cost is 6
- FDDI—Default cost is 1
- X25—Default cost is 5208
- Asynchronous—Default cost is 10,000

- ATM— Default cost is 1

Examples

The following example sets the interface cost value to 65:

```
ip ospf cost 65
```

ip ospf database-filter all out

To filter outgoing link-state advertisements (LSAs) to an OSPF interface, use the **ip ospf database-filter all out** command in interface configuration mode. 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.

Defaults

This command is disabled by default. All outgoing LSAs are flooded to the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command performs the same function that the **neighbor database-filter** command performs on a neighbor basis.

Examples

The following example prevents flooding of OSPF LSAs to broadcast, nonbroadcast, or point-to-point networks reachable through Ethernet interface 0:

```
interface ethernet 0
 ip ospf database-filter all out
```

Related Commands

Command	Description
neighbor database-filter	Filters outgoing LSAs to an OSPF neighbor.

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** command in interface configuration mode. 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

seconds	Specifies the interval (in seconds); the value must be the same for all nodes on the network.

Defaults

Four times the interval set by the **ip ospf hello-interval** command

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The interval is advertised in router hello packets. This value must be the same for all routers and access servers on a specific network.

Examples

The following example sets the OSPF dead interval to 60 seconds:

```
interface ethernet 1
 ip ospf dead-interval 60
```

Related Commands

Command	Description
ip ospf hello-interval	Specifies the interval between hello packets that the Cisco IOS software sends on the interface.

ip ospf demand-circuit

To configure OSPF to treat the interface as an OSPF demand circuit, use the **ip ospf demand-circuit** command in interface configuration mode. 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.

Defaults

The circuit is not a demand circuit.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

On point-to-point interfaces, only one end of the demand circuit must be configured with this command. Periodic hello messages are suppressed and periodic refreshes of link-state advertisements (LSAs) do not flood the demand circuit. This command allows the underlying data link layer to be closed when the topology is stable. In point-to-multipoint topology, only the multipoint end must configured with this command.

Examples

The following example sets the configuration for an ISDN on-demand circuit:

```
router ospf 1
 network 10.0.3.0 255.255.255.0 area 0
interface BRI0
 ip ospf demand-circuit
```

ip ospf flood-reduction

To suppress the unnecessary flooding of link-state advertisements (LSAs) in stable topologies, use the **ip ospf flood-reduction** command in interface configuration mode. 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.

Defaults

This command is disabled by default.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

All routers supporting the OSPF demand circuit are compatible and can interact with routers supporting flooding reduction.

Examples

The following example reduces the flooding of unnecessary LSAs on serial interface 0:

```
interface serial 0
 ip ospf flood-reduction
```

Related Commands

Command	Description
show ip ospf interface	Displays OSPF-related interface information.
show ip ospf neighbor	Displays OSPF-neighbor information on a per-interface basis.

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** command in interface configuration mode. 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.

Defaults

10 seconds (Ethernet)

30 seconds (nonbroadcast)

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This value is advertised in the hello packets. The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

Examples

The following example sets the interval between hello packets to 15 seconds:

```
interface ethernet 1
 ip ospf hello-interval 15
```

Related Commands

Command	Description
ip ospf dead-interval	Sets the time period for which hello packets must not have been seen before neighbors declare the router down.

ip ospf message-digest-key

To enable OSPF Message Digest 5 (MD5) authentication, use the **ip ospf message-digest-key** command in interface configuration mode. 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

key-id	An identifier in the range from 1 to 255.
key	Alphanumeric password of up to 16 bytes.

Defaults

OSPF MD5 authentication is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Usually, one key per interface is used to generate authentication information when sending packets and to authenticate incoming packets. The same key identifier on the neighbor router must have the same *key* value.

The process of changing keys is as follows. Suppose the current configuration is as follows:

```
interface ethernet 1
 ip ospf message-digest-key 100 md5 OLD
```

You change the configuration to the following:

```
interface ethernet 1
 ip ospf message-digest-key 101 md5 NEW
```

The system assumes its neighbors do not have the new key yet, so it begins a rollover process. It sends multiple copies of the same packet, each authenticated by different keys. In this example, the system sends out two copies of the same packet—the first one authenticated by key 100 and the second one authenticated by key 101.

Rollover allows neighboring routers to continue communication while the network administrator is updating them with the new key. Rollover stops once the local system finds that all its neighbors know the new key. The system detects that a neighbor has the new key when it receives packets from the neighbor authenticated by the new key.

After all neighbors have been updated with the new key, the old key should be removed. In this example, you would enter the following:

```
interface ethernet 1
 no ip ospf message-digest-key 100
```

Then, only key 101 is used for authentication on Ethernet interface 1.

We recommend that you not keep more than one key per interface. Every time you add a new key, you should remove the old key to prevent the local system from continuing to communicate with a hostile system that knows the old key. Removing the old key also reduces overhead during rollover.

Note If the **service password-encryption** command is not used when implementing OSPF MD5 authentication, the MD5 secret will be stored as plain text in NVRAM.

Examples

The following example sets a new key 19 with the password 8ry4222:

```
interface ethernet 1
 ip ospf message-digest-key 10 md5 xvv560qle
 ip ospf message-digest-key 19 md5 8ry4222
```

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
ip ospf authentication	Specifies authentication type for an interface.
service password-encryption	Encrypts a password.

ip ospf mtu-ignore

To disable OSPF MTU mismatch detection on receiving DBD packets, use the **ip ospf mtu-ignore** command in interface configuration mode. 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 keywords or arguments.

Defaults

OSPF MTU mismatch detection is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)	This command was introduced.

Usage Guidelines

OSPF checks whether neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange Database Descriptor (DBD) packets. If the receiving MTU in the DBD packet is higher than the IP MTU configured on the incoming interface, OSPF adjacency will not be established.

Examples

The following example disables MTU mismatch detection on receiving DBD packets:

```
interface serial 0/0
 ip ospf mtu-ignore
```

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** command in global configuration mode. 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.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command makes it easier to identify a router because the router is displayed by name rather than by its router ID or neighbor ID.

Examples

The following example configures OSPF to look up DNS names for use in all OSPF **show** EXEC command displays:

```
ip ospf name-lookup
```

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** command in interface configuration mode. 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.

Defaults

Depends on the network type.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The **point-to-multipoint** keyword was added.
11.3 AA	The **non-broadcast** keyword used with the **point-to-multipoint** keyword was added.

Usage Guidelines

Using this feature, you can configure broadcast networks as NBMA networks when, for example, routers in your network do not support multicast addressing. You can also configure nonbroadcast multiaccess networks (such as X.25, Frame Relay, and Switched Multimegabit Data Service (SMDS)) as broadcast networks. This feature saves you from needing to configure neighbors.

Configuring NBMA networks as either broadcast or nonbroadcast assumes that there are virtual circuits from every router to every router or fully meshed networks. However, there are other configurations where this assumption is not true. For example, a partially meshed network. In these cases, you can configure the OSPF network type as a point-to-multipoint network. Routing between two routers that are not directly connected will go through the router that has virtual circuits to both routers. You need not configure neighbors when using this feature.

If this command is issued on an interface that does not allow it, this command will be ignored.

OSPF has two features related to point-to-multipoint networks. One feature applies to broadcast networks; the other feature applies to nonbroadcast networks:

- On point-to-multipoint, broadcast networks, you can use the **neighbor** command, and you must specify a cost to that neighbor.
- On point-to-multipoint, nonbroadcast networks, you must use the **neighbor** command to identify neighbors. Assigning a cost to a neighbor is optional.

Examples

The following example sets your OSPF network as a broadcast network:

```
interface serial 0
 ip address 192.168192.168.77.17 255.255.255.0
 ip ospf network broadcast
 encapsulation frame-relay
```

The following example illustrates a point-to-multipoint network with broadcast:

```
interface serial 0
 ip address 10.0.1.1 255.255.255.0
 encapsulation frame-relay
 ip ospf cost 100
 ip ospf network point-to-multipoint
 frame-relay map ip 10.0.1.3 202 broadcast
 frame-relay map ip 10.0.1.4 203 broadcast
 frame-relay map ip 10.0.1.5 204 broadcast
 frame-relay local-dlci 200
!
router ospf 1
 network 10.0.1.0 0.0.0.255 area 0
 neighbor 10.0.1.5 cost 5
 neighbor 10.0.1.4 cost 10
```

Related Commands

Command	Description
frame-relay map	Defines mapping between a destination protocol address and the DLCI used to connect to the destination address.
neighbor (OSPF)	Configures OSPF routers interconnecting to nonbroadcast networks.
x25 map	Sets up the LAN protocols-to-remote host mapping.

ip ospf priority

To set the router priority, which helps determine the designated router for this network, use the **ip ospf priority** command in interface configuration mode. 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

number-value	A number value that specifies the priority of the router. The range is from 0 to 255.

Defaults

Priority of 1

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the designated router or backup designated router. Router priority is configured only for interfaces to multiaccess networks (in other words, not to point-to-point networks).

This priority value is used when you configure OSPF for nonbroadcast networks using the **neighbor** router configuration command for OSPF.

Examples

The following example sets the router priority value to 4:

```
interface ethernet 0
 ip ospf priority 4
```

Related Commands

Command	Description
ip ospf network	Configures the OSPF network type to a type other than the default for a given medium.
neighbor (OSPF)	Configures OSPF routers interconnecting to nonbroadcast networks.

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** command in interface configuration mode. 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

seconds	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.

Defaults

5 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When a router sends an LSA to its neighbor, it keeps the LSA until it receives back the acknowledgment message. If the router receives no acknowledgment, it will resend the LSA.

The setting of this parameter should be conservative, or needless retransmission will result. The value should be larger for serial lines and virtual links.

Examples

The following example sets the retransmit interval value to 8 seconds:

```
interface ethernet 2
 ip ospf retransmit-interval 8
```

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** command in interface configuration mode. 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

seconds	Time (in seconds) required to send a link-state update. The range is from 1 to 65535 seconds. The default is 1 second.

Defaults

1 second

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the *seconds* argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface.

If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low-speed links.

Examples

The following example sets the retransmit delay value to 3 seconds:

```
interface ethernet 0
 ip ospf transmit-delay 3
```

log-adjacency-changes

To configure the router to send a syslog message when an OSPF neighbor goes up or down, use the **log-adjacency-changes** command in router configuration mode. To turn off this function, use the **no** form of this command.

log-adjacency-changes [**detail**]

no log-adjacency-changes [**detail**]

Syntax Description

detail	(Optional) Sends a syslog message for each state change, not just when a neighbor goes up or down.

Defaults

Enabled

Command Modes

Router configuration

Command History

Release	Modification
11.2	This command was introduced as "**ospf log-adjacency-changes**".
12.1	The **ospf** keyword was omitted and the **detail** keyword was added.

Usage Guidelines

This command allows you to know about OSPF neighbors going up or down without turning on the **debug ip ospf adjacency** command. The **log-adjacency-changes** command provides a higher level view of those changes of the peer relationship with less output. This command is on by default but only up/down (full/down) events are reported, unless the **detail** keyword is also configured.

Examples

The following example configures the router to send a syslog message when an OSPF neighbor state changes:

```
log-adjacency-changes detail
```

neighbor (OSPF)

To configure OSPF routers interconnecting to nonbroadcast networks, use the **neighbor** command in router configuration mode. 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

ip-address	Interface IP address of the neighbor.
priority *number*	(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 *seconds*	(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 *number* argument are the only options that are applicable. This keyword does not apply to nonbroadcast multiaccess (NBMA) networks.
database-filter all	(Optional) Filters outgoing link-state advertisements (LSAs) to an OSPF neighbor.

Defaults

No configuration is specified.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3 AA	The **cost** keyword was added.

Usage Guidelines

X.25 and Frame Relay provide an optional broadcast capability that can be configured in the map to allow OSPF to run as a broadcast network. At the OSPF level you can configure the router as a broadcast network. Refer to the **x25 map** and **frame-relay map** commands in the “X.25 Commands” and “Frame Relay Commands” chapters, respectively, in the *Cisco IOS Wide-Area Networking Command Reference* for more detail.

One neighbor entry must be included in the Cisco IOS software configuration for each known nonbroadcast network neighbor. The neighbor address must be on the primary address of the interface.

If a neighboring router has become inactive (hello packets have not been received for the Router Dead Interval period), it may still be necessary to send hello packets to the dead neighbor. These hello packets will be sent at a reduced rate called *Poll Interval*.

When the router first starts up, it sends only hello packets to those routers with nonzero priority, that is, routers that are eligible to become designated routers (DRs) and backup designated routers (BDRs). After the DR and BDR are selected, DR and BDR will then start sending hello packets to all neighbors in order to form adjacencies.

Prior to Cisco IOS Release 12.0, the **neighbor** command applied to NBMA networks only. With Release 12.0, the **neighbor** command applies to NBMA networks and point-to-multipoint networks. On NBMA networks, the **cost** keyword is not accepted.

Examples

The following example declares a router at address 192.168.3.4 on a nonbroadcast network, with a priority of 1 and a poll interval of 180 seconds:

```
router ospf
 neighbor 192.168.3.4 priority 1 poll-interval 180
```

The following example illustrates a point-to-multipoint network with nonbroadcast:

```
interface Serial0
ip address 10.0.1.1 255.255.255.0
ip ospf network point-to-multipoint non-broadcast
encapsulation frame-relay
no keepalive
frame-relay local-dlci 200
frame-relay map ip 10.0.1.3 202
frame-relay map ip 10.0.1.4 203
frame-relay map ip 10.0.1.5 204
no shut
!
router ospf 1
network 10.0.1.0 0.0.0.255 area 0
neighbor 10.0.1.3 cost 5
neighbor 10.0.1.4 cost 10
neighbor 10.0.1.5 cost 15
```

Related Commands

Command	Description
ip ospf priority	Sets the router priority, which helps determine the designated router for this network.

neighbor database-filter

To filter outgoing link-state advertisements (LSAs) to an OSPF neighbor, use the **neighbor database-filter** command in router configuration mode. 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

ip-address **all out**	IP address of the neighbor to which outgoing LSAs are blocked.

Defaults

This command is disabled by default. All outgoing LSAs are flooded to the neighbor.

Command Modes

Router configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This command performs the same function that the **ip ospf database-filter** command performs on an interface basis.

Examples

The following example prevents flooding of OSPF LSAs to point-to-multipoint networks to the neighbor at IP address 10.2.3.4:

```
router ospf 109
 neighbor 10.2.3.4 database-filter all out
```

Related Commands

Command	Description
ip ospf database-filter all out	Filters outgoing LSAs to an OSPF interface.

network area

To define the interfaces on which OSPF runs and to define the area ID for those interfaces, use the **network area** command in router configuration mode. 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

ip-address	IP address.
wildcard-mask	IP-address-type mask that includes "don't care" bits.
area-id	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 value of the *area-id* argument.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The *ip-address* and *wildcard-mask* arguments together allow you to define one or multiple interfaces to be associated with a specific OSPF area using a single command. Using the *wildcard-mask* argument allows you to define one or multiple interfaces to be associated with a specific OSPF area using a single command. If you intend to associate areas with IP subnets, you can specify a subnet address as the value of the *area-id* argument.

For OSPF to operate on the interface, the primary address of the interface must be covered by the **network area** command. If the **network area** command covers only the secondary address, it will not enable OSPF over that interface.

The Cisco IOS software sequentially evaluates the *ip-address*s *wildcard-mask* pair for each interface as follows:

1. The *wildcard-mask* argument is logically ORed with the interface IP address.
2. The *wildcard-mask* argument is logically ORed with the *ip-address* argument in the **network** command.
3. The software compares the two resulting values. If they match, OSPF is enabled on the associated interface and this interface is attached to the OSPF area specified.

There is no limit to the number of **network area** commands you can use on the router.

> **Note** Any individual interface can only be attached to a single area. If the address ranges specified for different areas overlap, the software will adopt the first area in the **network** command list and ignore the subsequent overlapping portions. In general, we recommend that you configure address ranges that do not overlap in order to avoid inadvertent conflicts.

When a more specific OSPF network range is removed, interfaces belonging to that network range will be retained and remain active if and only if a less specific network range exists.

For example, consider the following configuration:

```
router ospf 1
 network 205.188.129.16 0.0.0.3 area 20
 network 205.188.129.40 0.0.0.3 area 20
 network 205.188.129.44 0.0.0.3 area 20
 network 205.188.129.96 0.0.0.3 area 20
 network 205.188.128.0  0.0.127.255 area 20
!
```

Enter the following:

```
no network 205.188.129.40 0.0.0.3 area 20
```

Interfaces falling into the network range 205.188.129.40/0.0.0.3 will still remain active because the superset, 205.188.128.0/0.0.127.255, exists for area 20. A more specific network statement will cause interfaces belonging to that range to be removed from a different area only if a less specific network statement (superset) exists.

Consider a configuration such as the following:

```
!
router ospf 1
 network 205.188.128.0 0.0.127.255 area 20
!
```

If the following network statement is entered:

```
network 205.188.129.96 0.0.0.3 area 40
```

then interfaces belonging to range 205.188.129.96/0.0.0.3, if any, are removed from area 20 and moved to area 40. Network statements with identical ranges but with different area IDs are considered as area changes. For example, the following network statements will cause interfaces belonging to network range 205.188.129.40/0.0.0.3 to move from area 20 to area 40:

```
network 205.188.129.40 0.0.0.3 area 20
network 205.188.129.40 0.0.0.3 area 40
```

Examples

The following partial example initializes OSPF routing process 109, and defines four OSPF areas: 10.9.50.0, 2, 3, and 0. Areas 10.9.50.0, 2, and 3 mask specific address ranges, and area 0 enables OSPF for all other networks.

```
interface ethernet 0
 ip address 10.108.20.1 255.255.255.0
router ospf 109
 network 10.108.20.0 0.0.0.255 area 10.9.50.0
 network 10.108.0.0 0.0.255.255 area 2
 network 10.109.10.0 0.0.0.255 area 3
 network 0.0.0.0 255.255.255.255 area 0
```

Related Commands

Command	Description
router ospf	Configures an OSPF routing process.

router-id

To use a fixed router ID, use the **router-id** command in router configuration mode. 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

ip-address	Router ID in IP address format.

Defaults

No OSPF routing process is defined.

Command Modes

Router configuration

Command History

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

Usage Guidelines

You can configure an arbitrary value in the IP address format for each router. However, each router ID must be unique.

If this command is used on an OSPF router process which is already active (has neighbors), the new router-ID is used at the next reload or at a manual OSPF process restart. To manually restart the OSPF process, use the **clear ip ospf** command.

Examples

The following example specifies a fixed router-id:

```
router-id 10.1.1.1
```

Related Commands

Command	Description
clear ip ospf	Clears redistribution based on the OSPF routing process ID.
router ospf	Configures the OSPF routing process.

router ospf

To configure an OSPF routing process, use the **router ospf** command in global configuration mode. To terminate an OSPF routing process, use the **no** form of this command.

router ospf *process-id*

no router ospf *process-id*

Syntax Description

process-id	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.

Defaults

No OSPF routing process is defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can specify multiple OSPF routing processes in each router.

Examples

The following example configures an OSPF routing process and assign a process number of 109:

```
router ospf 109
```

Related Commands

Command	Description
network area	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.

show ip ospf

To display general information about OSPF routing processes, use the **show ip ospf** command in EXEC mode.

show ip ospf [*process-id*]

Syntax Description

process-id	(Optional) Process ID. If this argument is included, only information for the specified routing process is included.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show ip ospf** command when entered without a specific OSPF process ID:

```
Router# show ip ospf

Routing Process "ospf 201" with ID 192.42.110.200
Supports only single TOS(TOS0) route
It is an area border and autonomous system boundary router
Redistributing External Routes from,
   igrp 200 with metric mapped to 2, includes subnets in redistribution
   rip with metric mapped to 2
   igrp 2 with metric mapped to 100
   igrp 32 with metric mapped to 1
Number of areas in this router is 3
Area 192.42.110.0
   Number of interfaces in this area is 1
   Area has simple password authentication
   SPF algorithm executed 6 times
```

Table 5 describes the significant fields shown in the display.

Table 5 show ip ospf Field Descriptions

Field	Description
Routing process "ospf 201" with ID 192.42.110.200	Process ID and OSPF router ID.
Supports ...	Number of types of service supported (Type 0 only).
It is ...	Possible types are internal, area border, or autonomous system boundary.
Summary Link update interval	Specifies summary update interval in hours:minutes:seconds, and time until next update.

Table 5 show ip ospf Field Descriptions (continued)

Field	Description
External Link update interval	Specifies external update interval in hours:minutes:seconds, and time until next update.
Redistributing External Routes from	Lists of redistributed routes, by protocol.
Number of areas	Number of areas in router, area addresses, and so on.
Link State Update Interval	Specifies router and network link-state update interval in hours:minutes:seconds, and time until next update.
Link State Age Interval	Specifies max-aged update deletion interval, and time until next database cleanup, in hours:minutes:seconds.

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** command in privileged EXEC mode.

show ip ospf border-routers

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show ip ospf border-routers** command:

```
Router# show ip ospf border-routers

OSPF Process 109 internal Routing Table

Destination      Next Hop        Cost   Type     Rte Type Area           SPF No

192.168.97.53     172.16.1.53    10     ABR      INTRA    0.0.0.3        3
192.168.103.51    192.168.96.51    10     ABR      INTRA    0.0.0.3        3
192.168.103.52    192.168.96.51    20     ASBR     INTER    0.0.0.3        3
192.168.103.52    172.16.1.53    22     ASBR     INTER    0.0.0.3        3
```

Table 6 describes the significant fields shown in the display.

Table 6 show ip ospf border-routers Field Descriptions

Field	Description
Destination	Router ID of the destination.
Next Hop	Next hop toward the destination.
Cost	Cost of using this route.
Type	The router type of the destination; it is either an ABR or ASBR or both.
Rte Type	The type of this route; it is either an intra-area or interarea route.
Area	The area ID of the area from which this route is learned.
SPF No	The internal number of the shortest path first (SPF) calculation that installs this route.

show ip ospf database

To display lists of information related to the OSPF database for a specific router, use the **show ip ospf database** command in EXEC mode. 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

process-id	(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.
area-id	(Optional) Area number associated with the OSPF address range defined in the **network** router configuration command used to define the particular area.
adv-router [*ip-address*]	(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.
link-state-id	(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. When the LSA is describing a network, the *link-state-id* argument can take one of two forms: • 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.) When the LSA is describing a router, the link-state ID is always the OSPF router ID of the described router. 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).
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.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.0	The **database-summary** keyword was added.
12.0	The following keywords were added: • **self-originate** • **adv-router**
12.1	The following keywords were added: • **opaque-area** • **opaque-as** • **opaque-link**

Examples

The following is sample output from the **show ip ospf database** command when no arguments or keywords are used:

```
Router# show ip ospf database

OSPF Router with ID(192.168.1.11) (Process ID 1)

                 Router Link States(Area 0)

 Link ID          ADV Router        Age         Seq#       Checksum Link count
 192.168.1.8      192.168.1.8       1381       0x8000010D    0xEF60   2
 192.168.1.11     192.168.1.11      1460       0x800002FE    0xEB3D   4
 192.168.1.12     192.168.1.12      2027       0x80000090    0x875D   3
 192.168.1.27     192.168.1.27      1323       0x800001D6    0x12CC   3

                 Net Link States(Area 0)

 Link ID        ADV Router        Age         Seq#       Checksum
 172.16.1.27     192.168.1.27      1323       0x8000005B    0xA8EE
 172.17.1.11     192.168.1.11      1461       0x8000005B    0x7AC

                 Type-10 Opaque Link Area Link States (Area 0)

  Link ID         ADV Router        Age         Seq#       Checksum Opaque ID
 10.0.0.0         192.168.1.11      1461       0x800002C8    0x8483     0
 10.0.0.0         192.168.1.12      2027       0x80000080    0xF858     0
 10.0.0.0         192.168.1.27      1323       0x800001BC    0x919B     0
 10.0.0.1         192.168.1.11      1461       0x8000005E    0x5B43     1
```

Table 7 describes the significant fields shown in the display.

Table 7 show ip ospf database Field Descriptions

Field	Description
Link ID	Router ID number.
ADV Router	Advertising router ID.
Age	Link-state age.
Seq#	Link-state sequence number (detects old or duplicate LSAs).
Checksum	Fletcher checksum of the complete contents of the LSA.

Table 7 show ip ospf database Field Descriptions (continued)

Field	Description
Link count	Number of interfaces detected for router.
Opaque ID	Opaque LSA ID number.

The following is sample output from the **show ip ospf database** command with the **asbr-summary** keyword:

```
Router# show ip ospf database asbr-summary

OSPF Router with id(192.168.239.66) (Process ID 300)

                Displaying Summary ASB Link States(Area 0.0.0.0)

LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links(AS Boundary Router)
Link State ID: 172.16.245.1 (AS Boundary Router address)
Advertising Router: 172.16.241.5
LS Seq Number: 80000072
Checksum: 0x3548
Length: 28
Network Mask: 0.0.0.0 TOS: 0  Metric: 1
```

Table 8 describes the significant fields shown in the display.

Table 8 show ip ospf database asbr-summary Field Descriptions

Field	Description
OSPF Router with id	Router ID number.
Process ID	OSPF process ID.
LS age	Link-state age.
Options	Type of service options (Type 0 only).
LS Type	Link-state type.
Link State ID	Link-state ID (ASBR).
Advertising Router	Advertising router ID.
LS Seq Number	Link-state sequence (detects old or duplicate LSAs).
Checksum	Link-state checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length in bytes of the LSA.
Network Mask	Network mask implemented.
TOS	Type of service.
Metric	Link-state metric.

The following is sample output from the **show ip ospf database** command with the **external** keyword:

```
Router# show ip ospf database external

OSPF Router with id(192.168.239.66) (Autonomous system 300)

                   Displaying AS External Link States

LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 143.10.0.0 (External Network Number)
Advertising Router: 10.187.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0
     Metric Type: 2 (Larger than any link state path)
     TOS: 0
     Metric: 1
     Forward Address: 0.0.0.0
     External Route Tag: 0
```

Table 9 describes the significant fields shown in the display.

Table 9 show ip ospf database external Field Descriptions

Field	Description
OSPF Router with id	Router ID number.
Autonomous system	OSPF autonomous system number (OSPF process ID).
LS age	Link-state age.
Options	Type of service options (Type 0 only).
LS Type	Link-state type.
Link State ID	Link-state ID (external network number).
Advertising Router	Advertising router ID.
LS Seq Number	Link-state sequence number (detects old or duplicate LSAs).
Checksum	Checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length in bytes of the LSA.
Network Mask	Network mask implemented.
Metric Type	External type.
TOS	Type of service.
Metric	Link-state metric.
Forward Address	Forwarding address. Data traffic for the advertised destination will be forwarded to this address. If the forwarding address is set to 0.0.0.0, data traffic will be forwarded to the originator of the advertisement.
External Route Tag	External route tag, a 32-bit field attached to each external route. This is not used by the OSPF protocol itself.

The following is sample output from the **show ip ospf database** command with the **network** keyword:

```
Router# show ip ospf database network

 OSPF Router with id(192.168.239.66) (Process ID 300)

                Displaying Net Link States(Area 0.0.0.0)

LS age: 1367
Options: (No TOS-capability)
LS Type: Network Links
Link State ID: 10.187.1.3 (address of Designated Router)
Advertising Router: 192.168.239.66
LS Seq Number: 800000E7
Checksum: 0x1229
Length: 52
Network Mask: 255.255.255.0
        Attached Router: 192.168.239.66
        Attached Router: 10.187.241.5
        Attached Router: 10.187.1.1
        Attached Router: 10.187.54.5
        Attached Router: 10.187.1.5
```

Table 10 describes the significant fields shown in the display.

Table 10 show ip ospf database network Field Descriptions

Field	Description
OSPF Router with id	Router ID number.
Process ID 300	OSPF process ID.
LS age	Link-state age.
Options	Type of service options (Type 0 only).
LS Type	Link-state type.
Link State ID	Link-state ID of designated router.
Advertising Router	Advertising router ID.
LS Seq Number	Link-state sequence (detects old or duplicate LSAs).
Checksum	Checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length in bytes of the link-state advertisement.
Network Mask	Network mask implemented.
AS Boundary Router	Definition of router type.
Attached Router	List of routers attached to the network, by IP address.

The following is sample output, carrying Multiprotocol Label Switching (MPLS) traffic engineering specification information, from the **show ip ospf database** command with the **opaque-area** keyword:

```
Router# show ip ospf database opaque-area adv-router 192.168.1.12

OSPF Router with id(192.168.1.11) (Process ID 1)

                Type-10 Opaque Link Area Link States (Area 0)

LS age: 224
   Options: (No TOS-capability, DC)
   LS Type: Opaque Area Link
   Link State ID: 1.0.0.0
   Opaque Type: 1
   Opaque ID: 0
   Advertising Router: 192.168.1.12
   LS Seq Number: 80000081
   Checksum: 0xF659
   Length: 132
   Fragment number : 0

     MPLS TE router ID : 192.168.1.12

     Link connected to Point-to-Point network
       Link ID : 192.168.1.11
       Interface Address : 172.16.1.12
       Neighbor Address : 172.16.1.11
       Admin Metric : 10
       Maximum bandwidth : 193000
       Maximum reservable bandwidth : 125000
       Number of Priority : 8
       Priority 0 : 125000      Priority 1 : 125000
       Priority 2 : 125000      Priority 3 : 125000
       Priority 4 : 125000      Priority 5 : 125000
       Priority 6 : 125000      Priority 7 : 100000
       Affinity Bit : 0x0

     Number of Links : 1
```

Table 11 describes the significant fields shown in the display.

Table 11 show ip ospf database opaque-area Field Descriptions

Field	Description
OSPF Router with id	Router ID number.
Process ID	OSPF process ID.
LS age	Link-state age.
Options	Type of service options (Type 0 only).
LS Type	Link-state type.
Link State ID	Link-state ID.
Opaque Type	Opaque link-state type.
Opaque ID	Opaque ID number.
Advertising Router	Advertising router ID.
LS Seq Number	Link-state sequence (detects old or duplicate LSAs).
Checksum	Checksum (Fletcher checksum of the complete contents of the LSA).

Table 11 show ip ospf database opaque-area Field Descriptions (continued)

Field	Description
Length	Length in bytes of the LSA.
Fragment number	Arbitrary value used to maintain multiple traffic engineering LSAs.
Link ID	Link ID number.
Interface Address	ID address of the interface.
Neighbor Address	IP address of the neighbor.
Admin Metric	Administrative distance metric value used by Multiprotocol Label Switching traffic engineering (MPLS-TE).
Maximum bandwidth	Specifies maximum bandwidth.
Maximum reservable bandwidth	Specifies maximum reservable bandwidth.
Number of Priority	Priority number.
Affinity Bit	Used by MPLS-TE.

The following is sample output from the **show ip ospf database** command with the **router** keyword:

```
Router# show ip ospf database router

OSPF Router with id(192.168.239.66) (Process ID 300)


                Displaying Router Link States(Area 0.0.0.0)

LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 10.187.21.6
Advertising Router: 10.187.21.6
LS Seq Number: 80002CF6
Checksum: 0x73B7
Length: 120
AS Boundary Router
155   Number of Links: 8

Link connected to: another Router (point-to-point)
(link ID) Neighboring Router ID: 10.187.21.5
(Link Data) Router Interface address: 10.187.21.6
Number of TOS metrics: 0
TOS 0 Metrics: 2
```

Table 12 describes the significant fields shown in the display.

Table 12 show ip ospf database router Field Descriptions

Field	Description
OSPF Router with id	Router ID number.
Process ID	OSPF process ID.
LS age	Link-state age.
Options	Type of service options (Type 0 only).

Table 12 show ip ospf database router Field Descriptions (continued)

Field	Description
LS Type	Link-state type.
Link State ID	Link-state ID.
Advertising Router	Advertising router ID.
LS Seq Number	Link-state sequence (detects old or duplicate LSAs).
Checksum	Checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length in bytes of the LSA.
AS Boundary Router	Definition of router type.
Number of Links	Number of active links.
link ID	Link type.
Link Data	Router interface address.
TOS	Type of service metric (Type 0 only).

The following is sample output from **show ip ospf database** command with the **summary** keyword:

```
Router# show ip ospf database summary

       OSPF Router with id(192.168.239.66) (Process ID 300)

                Displaying Summary Net Link States(Area 0.0.0.0)

LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links(Network)
Link State ID: 10.187.240.0 (summary Network Number)
Advertising Router: 10.187.241.5
LS Seq Number: 80000072
Checksum: 0x84FF
Length: 28
Network Mask: 255.255.255.0   TOS: 0  Metric: 1
```

Table 13 describes the significant fields shown in the display.

Table 13 show ip ospf database summary Field Descriptions

Field	Description
OSPF Router with id	Router ID number.
Process ID	OSPF process ID.
LS age	Link-state age.
Options	Type of service options (Type 0 only).
LS Type	Link-state type.
Link State ID	Link-state ID (summary network number).
Advertising Router	The ID of the advertising router.
LS Seq Number	Link-state sequence (detects old or duplicate LSAs).
Checksum	Checksum (Fletcher checksum of the complete contents of the LSA).
Length	Length in bytes of the link-state advertisement.

Table 13 show ip ospf database summary Field Descriptions (continued)

Field	Description
Network Mask	Network mask implemented.
TOS	Type of service.
Metric	Link-state metric.

The following is sample output from **show ip ospf database** command with the **database-summary** keyword:

```
Router# show ip ospf database database-summary

          OSPF Router with ID (172.19.65.21) (Process ID 1)

Area ID     Router     Network     Sum-Net     Sum-ASBR     Subtotal     Delete     Maxage
202         1          0           0           0            1            0          0
AS External                                                 0            0          0
Total       1          0           0           0            1
```

Table 14 describes the significant fields shown in the display.

Table 14 show ip ospf database database-summary Field Descriptions

Field	Description
Area ID	Area number.
Router	Number of router LSAs in that area.
Network	Number of network LSAs in that area.
Sum-Net	Number of summary LSAs in that area.
Sum-ASBR	Number of summary ASBR LSAs in that area.
Subtotal	Sum of Router, Network, Sum-Net, and Sum-ASBR for that area.
Delete	Number of LSAs that are marked “Deleted” in that area.
Maxage	Number of LSAs that are marked “Maxaged” in that area.
AS External	Number of external 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** command in EXEC mode.

show ip ospf flood-list *interface-type interface-number*

Syntax Description

interface-type	Interface type over which the LSAs will be flooded.
interface-number	Interface number over which the LSAs will be flooded.

Command Modes

EXEC

Command History

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

Usage Guidelines

Use this command to observe OSPF packet pacing.

Examples

The following is sample output of the **show ip ospf flood-list** command:

```
Router# show ip ospf flood-list ethernet 1

 Interface Ethernet1, Queue length 20
 Link state flooding due in 12 msec

 Type  LS ID            ADV RTR          Seq NO      Age    Checksum
    5  10.2.195.0       192.168.0.163    0x80000009  0      0xFB61
    5  10.1.192.0       192.168.0.163    0x80000009  0      0x2938
    5  10.2.194.0       192.168.0.163    0x80000009  0      0x757
    5  10.1.193.0       192.168.0.163    0x80000009  0      0x1E42
    5  10.2.193.0       192.168.0.163    0x80000009  0      0x124D
    5  10.1.194.0       192.168.0.163    0x80000009  0      0x134C
```

Table 15 describes the significant fields shown in the display.

Table 15   show ip ospf flood-list Field Descriptions

Field	Description
Interface Ethernet1	Interface for which information is displayed.
Queue length	Number of LSAs waiting to be flooded.
Link state retransmission due in	Length of time before next link-state transmission.
Type	Type of LSA.
LS ID	Link-state ID of the LSA.
ADV RTR	IP address of advertising router.
Seq NO	Sequence number of LSA.

Table 15 show ip ospf flood-list Field Descriptions (continued)

Field	Description
Age	Age of LSA (in seconds).
Checksum	Checksum of LSA.

show ip ospf interface

To display OSPF-related interface information, use the **show ip ospf interface** command in EXEC mode.

show ip ospf interface [*interface-type interface-number*]

Syntax Description

interface-type	(Optional) Interface type.
interface-number	(Optional) Interface number.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output of the **show ip ospf interface** command when Ethernet interface 0 is specified:

```
Router# show ip ospf interface ethernet 0

Ethernet 0 is up, line protocol is up
Internet Address 192.168.254.202, Mask 255.255.255.0, Area 0.0.0.0
AS 201, Router ID 192.77.99.1, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State OTHER, Priority 1
Designated Router id 192.168.254.10, Interface address 192.168.254.10
Backup Designated router id 192.168.254.28, Interface addr 192.168.254.28
Timer intervals configured, Hello 10, Dead 60, Wait 40, Retransmit 5
Hello due in 0:00:05
Neighbor Count is 8, Adjacent neighbor count is 2
  Adjacent with neighbor 192.168.254.28  (Backup Designated Router)
  Adjacent with neighbor 192.168.254.10  (Designated Router)
```

Table 16 describes the significant fields shown in the display.

Table 16 show ip ospf interface Field Descriptions

Field	Description
Ethernet	Status of physical link and operational status of protocol.
Internet Address	Interface IP address, subnet mask, and area address.
AS	Autonomous system number (OSPF process ID), router ID, network type, link-state cost.
Transmit Delay	Transmit delay, interface state, and router priority.
Designated Router	Designated router ID and respective interface IP address.
Backup Designated router	Backup designated router ID and respective interface IP address.
Timer intervals configured	Configuration of timer intervals.

Table 16 show ip ospf interface Field Descriptions (continued)

Field	Description
Hello	Number of seconds until next hello packet is sent out this interface.
Neighbor Count	Count of network neighbors and list of adjacent neighbors.

show ip ospf neighbor

To display OSPF-neighbor information on a per-interface basis, use the **show ip ospf neighbor** command in EXEC mode.

show ip ospf neighbor [*interface-type interface-number*] [*neighbor-id*] [**detail**]

Syntax Description

interface-type	(Optional) Interface type.
interface-number	(Optional) Interface number.
neighbor-id	(Optional) Neighbor ID.
detail	(Optional) Displays all neighbors given in detail (list all neighbors).

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show ip ospf neighbor** command showing a single line of summary information for each neighbor:

```
Router# show ip ospf neighbor

   ID           Pri   State        Dead Time     Address          Interface
10.199.199.137  1     FULL/DR       0:00:31    192.168.80.37      Ethernet0
172.16.48.1     1     FULL/DROTHER  0:00:33    172.16.48.1        Fddi0
172.16.48.200   1     FULL/DROTHER  0:00:33    172.16.48.200      Fddi0
10.199.199.137  5     FULL/DR       0:00:33    172.16.48.189      Fddi0
```

The following is sample output showing summary information about the neighbor that matches the neighbor ID:

```
Router# show ip ospf neighbor 10.199.199.137

Neighbor 10.199.199.137, interface address 192.168.80.37
    In the area 0.0.0.0 via interface Ethernet0
    Neighbor priority is 1, State is FULL
    Options 2
    Dead timer due in 0:00:32
    Link State retransmission due in 0:00:04
 Neighbor 10.199.199.137, interface address 172.16.48.189
    In the area 0.0.0.0 via interface Fddi0
    Neighbor priority is 5, State is FULL
    Options 2
    Dead timer due in 0:00:32
    Link State retransmission due in 0:00:03
```

If you specify the interface along with the neighbor ID, the Cisco IOS software displays the neighbors that match the neighbor ID on the interface, as in the following sample display:

```
Router# show ip ospf neighbor ethernet 0 10.199.199.137

Neighbor 10.199.199.137, interface address 192.168.80.37
    In the area 0.0.0.0 via interface Ethernet0
    Neighbor priority is 1, State is FULL
    Options 2
    Dead timer due in 0:00:37
    Link State retransmission due in 0:00:04
```

You can also specify the interface without the neighbor ID to show all neighbors on the specified interface, as in the following sample display:

```
Router# show ip ospf neighbor fddi 0

   ID          Pri   State        Dead Time     Address         Interface
172.16.48.1     1    FULL/DROTHER  0:00:33    172.16.48.1       Fddi0
172.16.48.200   1    FULL/DROTHER  0:00:32    172.16.48.200     Fddi0
10.199.199.137  5    FULL/DR       0:00:32    172.16.48.189     Fddi0
```

The following is sample output from the **show ip ospf neighbor detail** command:

```
Router# show ip ospf neighbor detail

Neighbor 192.168.5.2, interface address 10.225.200.28
    In the area 0 via interface Ethernet1
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 10.225.200.28 BDR is 10.225.200.30
    Options is 0x42
    Dead timer due in 00:00:36
    Neighbor is up for 00:09:46
   Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

Table 17 describes the significant fields shown in the displays.

Table 17 show ip ospf neighbor detail Field Descriptions

Field	Description
Neighbor	Neighbor router ID.
interface address	IP address of the interface.
In the area	Area and interface through which the OSPF neighbor is known.
Neighbor priority	Router priority of the neighbor, neighbor state.
State	OSPF state.
state changes	Number of state changes since the neighbor was created.This value can be reset using the **clear ip ospf counters neighbor** command.
DR is	Router ID of the designated router for the interface.
BDR is	Router ID of the backup designated router for the interface.
Options	Hello packet options field contents. (E-bit only. Possible values are 0 and 2; 2 indicates area is not a stub; 0 indicates area is a stub.)
Dead timer	Expected time before Cisco IOS software will declare the neighbor dead.

Table 17 show ip ospf neighbor detail Field Descriptions (continued)

Field	Description
Neighbor is up for	Number of hours:minutes:seconds since the neighbor went into 2-way state.
Index	Neighbor location in the area-wide and autonomous system-wide retransmission queue.
retransmission queue length	Number of elements in retransmission queue.
number of retransmission	Number of times update packets have been retransmitted during flooding.
First	Memory location of the flooding details.
Next	Memory location of the flooding details.
Last retransmission scan length	Number of LSAs in the last retransmission packet.
maximum	Maximum number of LSAs sent in any retransmission packet.
Last retransmission scan time	Time taken to build last retransmission packet.
maximum	Maximum time taken to build any retransmission packet.

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** command in EXEC mode.

show ip ospf request-list [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

neighbor	(Optional) Displays the list of all LSAs requested by the router from this neighbor.
interface	(Optional) Displays the list of all LSAs requested by the router from this interface.
interface-neighbor	(Optional) Displays the list of all LSAs requested by the router on this interface, from this neighbor.

Command Modes

EXEC

Command History

Release	Modification
10.2	This command was introduced.

Usage Guidelines

The information displayed by the **show ip ospf request-list** command is useful in debugging OSPF routing operations.

Examples

The following is sample output from the **show ip ospf request-list** command:

```
Router# show ip ospf request-list serial 0

             OSPF Router with ID (192.168.1.11) (Process ID 1)

  Neighbor 192.168.1.12, interface Serial0 address 172.16.1.12

  Type  LS ID            ADV RTR          Seq NO      Age    Checksum
     1  192.168.1.12     192.168.1.12     0x8000020D  8      0x6572
```

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** command in EXEC mode.

show ip ospf retransmission-list [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

neighbor	(Optional) Displays the list of all LSAs waiting to be resent for this neighbor.
interface	(Optional) Displays the list of all LSAs waiting to be resent on this interface.
interface-neighbor	(Optional) Displays the list of all LSAs waiting to be resent on this interface, from this neighbor.

Command Modes

EXEC

Command History

Release	Modification
10.2	This command was introduced.

Usage Guidelines

The information displayed by the **show ip ospf retransmission-list** command is useful in debugging OSPF routing operations.

Examples

The following is sample output from the **show ip ospf retransmission-list** command:

```
Router# show ip ospf retransmission-list serial 0

             OSPF Router with ID (192.168.1.12) (Process ID 1)

  Neighbor 192.168.1.11, interface Serial0 address 172.16.1.11
  Link state retransmission due in 3764 msec, Queue length 2

  Type  LS ID             ADV RTR           Seq NO      Age    Checksum
     1  192.168.1.12      192.168.1.12      0x80000210  0      0xB196
```

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** command in EXEC mode.

show ip ospf [*process-id*] **summary-address**

Syntax Description

process-id	(Optional) OSPF area ID.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The *process-id* argument can be entered as a decimal number or as an IP address format.

Examples

The following is sample output from the **show ip ospf summary-address** command:

```
Router# show ip ospf summary-address

OSPF Process 2, Summary-address

10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 0
10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 10
```

show ip ospf virtual-links

To display parameters and the current state of OSPF virtual links, use the **show ip ospf virtual-links** command in EXEC mode.

show ip ospf virtual-links

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The information displayed by the **show ip ospf virtual-links** command is useful in debugging OSPF routing operations.

Examples

The following is sample output from the **show ip ospf virtual-links** command:

```
Router# show ip ospf virtual-links

Virtual Link to router 192.168.101.2 is up
Transit area 0.0.0.1, via interface Ethernet0, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

Table 18 describes the significant fields shown in the display.

Table 18 show ip ospf virtual-links Field Descriptions

Field	Description
Virtual Link to router 192.168.101.2 is up	Specifies the OSPF neighbor, and if the link to that neighbor is up or down.
Transit area 0.0.0.1	The transit area through which the virtual link is formed.
via interface Ethernet0	The interface through which the virtual link is formed.
Cost of using 10	The cost of reaching the OSPF neighbor through the virtual link.
Transmit Delay is 1 sec	The transmit delay (in seconds) on the virtual link.
State POINT_TO_POINT	The state of the OSPF neighbor.
Timer intervals...	The various timer intervals configured for the link.
Hello due in 0:00:08	When the next hello is expected from the neighbor.
Adjacency State FULL	The adjacency state between the neighbors.

summary-address (OSPF)

To create aggregate addresses for OSPF, use the **summary-address** command in router configuration mode. To restore the default, use the **no** form of this command.

summary-address {{*ip-address mask*} | {*prefix mask*}} [**not-advertise**] [**tag** *tag*]

no summary-address {{*ip-address mask* } | {*prefix mask*}} [**not-advertise**] [**tag** *tag*]

Syntax Description

ip-address	Summary address designated for a range of addresses.
mask	IP subnet mask used for the summary route.
prefix	IP route prefix for the destination.
mask	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.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Multiple groups of addresses can be summarized for a given level. Routes learned from other routing protocols can also be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. This command helps reduce the size of the routing table.

Using this command for OSPF causes an OSPF Autonomous System Boundary Router (ASBR) to advertise one external route as an aggregate for all redistributed routes that are covered by the address. For OSPF, this command summarizes only routes from other routing protocols that are being redistributed into OSPF. Use the **area range** command for route summarization between OSPF areas.

OSPF does not support **summary-address 0.0.0.0 0.0.0.0**.

Examples

In the following example, the summary address 10.1.0.0 includes address 10.1.1.0, 10.1.2.0, 10.1.3.0, and so on. Only the address 10.1.0.0 is advertised in an external link-state advertisement.

```
summary-address 10.1.0.0 255.255.0.0
```

Related Commands

Command	Description
area range	Consolidates and summarizes routes at an area boundary.
ip ospf authentication-key	Assigns a password to be used by neighboring routers that are using the simple password authentication of OSPF.
ip ospf message-digest-key	Enables OSPF MD5 authentication.

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** command in router configuration mode. To restore the default value, use the **no** form of this command.

timers lsa-group-pacing *seconds*

no timers lsa-group-pacing

Syntax Description

seconds	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.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

OSPF LSA group pacing is enabled by default. For typical customers, the default group pacing interval for refreshing, checksumming, and aging is appropriate and you need not configure this feature.

The duration of the LSA group pacing is inversely proportional to the number of LSAs the router is handling. For example, if you have about 10,000 LSAs, decreasing the pacing interval would benefit you. If you have a very small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might benefit you slightly.

Examples

The following example changes the OSPF pacing between LSA groups to 60 seconds:

```
router ospf
 timers lsa-group-pacing 60
```

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** command in router configuration mode. 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

spf-delay	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.
spf-holdtime	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.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.

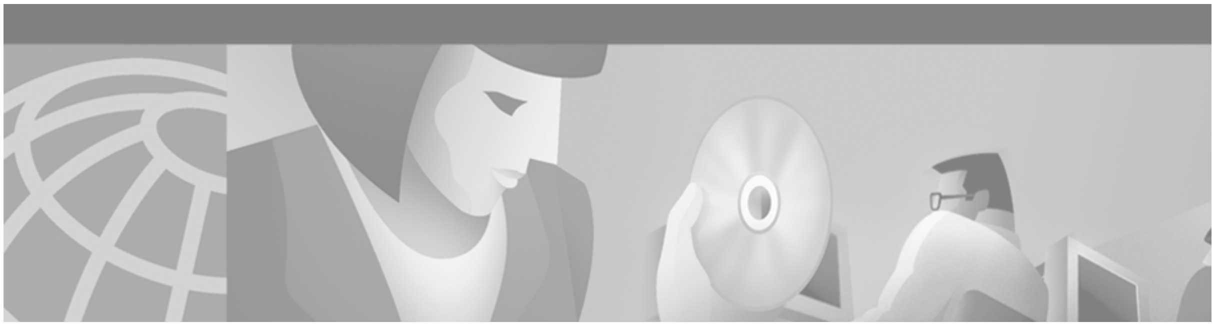
Usage Guidelines

Setting the delay and hold time low causes routing to switch to the alternate path more quickly in the event of a failure. However, it requires the router to use more CPU processing time.

Examples

The following example changes the delay to 10 seconds and the hold time to 20 seconds:

```
timers spf 10 20
```



Enhanced IGRP Commands

Use the commands in this chapter to configure and monitor Enhanced IGRP (EIGRP). For EIGRP configuration information and examples, refer to the “Configuring IP Enhanced IGRP” chapter of the *Cisco IOS IP Configuration Guide*.

auto-summary (Enhanced IGRP)

To restore the default behavior of automatic summarization of subnet routes into network-level routes, use the **auto-summary** command in router configuration mode. 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.

Defaults

The behavior of this command is enabled by default (the software summarizes subprefixes to the classful network boundary when crossing classful network boundaries).

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Route summarization reduces the amount of routing information in the routing tables.

By default, Border Gateway Protocol (BGP) does not accept subnets redistributed from an Interior Gateway Protocol (IGP). To advertise and carry subnet routes in BGP, use an explicit **network** command or the **no auto-summary** command. If you disable automatic summarization and have not entered a **network** command, you will not advertise network routes for networks with subnet routes unless they contain a summary route.

IP Enhanced IGRP summary routes are given an administrative distance value of 5. You cannot configure this value.

Routing Information Protocol (RIP) Version 1 always uses automatic summarization. If you are using RIP Version 2, you can turn off automatic summarization by specifying the **no auto-summary** command. Disable automatic summarization if you must perform routing between disconnected subnets. When automatic summarization is off, subnets are advertised.

Examples

The following example disables automatic summarization for process eigrp 109:

```
router eigrp 109
 no auto-summary
```

Related Commands

Command	Description
ip summary-address eigrp	Configures a summary aggregate address for a specified interface.

clear ip eigrp neighbors

To delete entries from the neighbor table, use the **clear ip eigrp neighbors** command in EXEC mode.

clear ip eigrp neighbors [*ip-address* | *interface-type interface-number*]

Syntax Description

ip-address	(Optional) Address of the neighbor.
interface-type interface-number	(Optional) Interface type and number. Specifying these arguments removes the specified interface type from the neighbor table that all entries learned via this interface.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example removes the neighbor whose address is 172.16.8.3:

```
Router# clear ip eigrp neighbors 172.16.8.3
```

Related Commands

Command	Description
show ip eigrp interfaces	Displays information about interfaces configured for EIGRP.

default-information

To control the candidate default routing information between IGRP or Enhanced IGRP processes, use the **default-information** command in router configuration mode. To suppress IGRP or Enhanced IGRP candidate information in incoming or outbound updates, use the **no default-information in** 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.
access-list-number | *access-list-name*	Number or name of an access list. It can be a number in the range from 1 to 99 or an access list name.

Defaults

Normally, exterior routes are always accepted and default information is passed between IGRP or EIGRP processes when redistribution occurs.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-number* and *access-list-name* arguments were added.

Usage Guidelines

The default network of 0.0.0.0 used by Routing Information Protocol (RIP) cannot be redistributed by IGRP but can be redistributed by Enhanced IGRP.

Examples

The following example allows IGRP exterior or default routes to be received by the IGRP process in autonomous system 23:

```
router igrp 23
 default-information in
```

The following example allows EIGRP exterior or default routes to be received by the EIGRP process in autonomous system 23:

```
router eigrp 23
 default-information in
```

default-metric (Enhanced IGRP)

To set metrics for IGRP or Enhanced IGRP (EIGRP), use the **default-metric** command in router configuration mode. 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

bandwidth	Minimum bandwidth of the route in kbps. It can be 0 or any positive integer.
delay	Route delay (in tens of microseconds). It can be 0 or any positive number that is a multiple of 39.1 nanoseconds.
reliability	Likelihood of successful packet transmission expressed as a number from 0 to 255. The value 255 means 100 percent reliability; 0 means no reliability.
loading	Effective bandwidth of the route expressed as a number from 0 to 255 (255 is 100 percent loading).
mtu	Maximum transmission unit (MTU) size of the route in bytes. It can be 0 or any positive integer.

Defaults

Only connected routes and interface static routes can be redistributed without a default metric.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

A default metric is required to redistribute a protocol into IGRP or EIGRP, unless you use the **redistribute** command. Automatic metric translations occur between IGRP and EIGRP. You do not need default metrics to redistributed IGRP or EIGRP into itself.

Note The default metric command does not affect EIGRP-to-EIGRP or IGRP-to-EIGRP distribution. To configure EIGRP-to-EIGRP or IGRP-to-EIGRP distribution, use route maps.

Metric defaults have been carefully set to work for a wide variety of networks. Take great care when changing these values.

Keeping the same metrics is supported only when redistributing from IGRP, EIGRP, or static routes.

Examples

The following example takes redistributed Routing Information Protocol (RIP) metrics and translates them into IGRP metrics with values as follows: bandwidth = 1000, delay = 100, reliability = 250, loading = 100, and MTU = 1500.

```
router igrp 109
 network 172.16.0.0
 redistribute rip
 default-metric 1000 100 250 100 1500
```

Related Commands

Command	Description
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

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** command in router configuration mode. 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

internal-distance	Administrative distance for Enhanced IGRP (EIGRP) internal routes. Internal routes are those that are learned from another entity within the same autonomous system. The distance can be a value from 1 to 255.
external-distance	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. The distance can be a value from 1 to 255.

Defaults

internal-distance: 90

external-distance: 170

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

Use the **distance eigrp** command if another protocol is known to be able to provide a better route to a node than was actually learned via external EIGRP, or if some internal routes should really be preferred by EIGRP.

Table 19 lists the default administrative distances.

Table 19 Default Administrative Distances

Route Source	Default Distance
Connected interface	0
Static route	1
Enhanced IGRP summary route	5
External BGP	20

Table 19 Default Administrative Distances (continued)

Route Source	Default Distance
Internal Enhanced IGRP	90
IGRP	100
Open Shortest Path First (OSPF)	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
EIGRP external route	170
Internal Border Gateway Protocol (BGP)	200
Unknown	255

To display the default administrative distance for a specified routing process, use the **show ip protocols** EXEC command.

Examples

In the following example, the **router eigrp** global configuration command sets up Enhanced IGRP routing in autonomous system number 109. The **network** router configuration commands specify Enhanced IGRP routing on networks 192.168.7.0 and 172.16.0.0. The **distance eigrp** command sets the administrative distance of all EIGRP internal routes to 80 and all EIGRP external routes to 130.

```
Router(config)# router eigrp 109
Router(router-config)# network 192.168.7.0
Router(router-config)# network 172.16.0.0
Router(router-config)# distance eigrp 80 130
```

Note You cannot set the administrative distance in EIGRP against certain routes or sources, as you can with other protocols. The command does not work this way with EIGRP.

Related Commands

Command	Description
show ip protocols	Displays the parameters and current state of the active routing protocol process.

distribute-list in (RIP, IGRP, EIGRP)

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* [**gateway** *prefix-list-name*]} **in** [*interface-type interface-number*]

no distribute-list {*access-list-number* | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*]} **in** [*interface-type interface-number*]

Syntax Description

access-list-number	Standard IP access list number. The list defines which networks are to be received and which are to be suppressed in routing updates.
prefix *prefix-list-name*	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.
gateway *prefix-list-name*	(Optional) Name of the prefix list to be applied to the gateway of the prefix being updated.
in	Applies the access list to incoming routing updates.
interface-type	(Optional) Interface type.
interface-number	(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.

Defaults

This command is disabled by default.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-number*, *interface-type*, and *interface-number* arguments were added.
12.0	The *prefix-list-name* argument was added.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

This command is not supported in Intermediate Sytem-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF).

Using a prefix list allows filtering based upon the prefix length, making it possible to filter either on the prefix list, the gateway, or both for incoming updates.

Specify either an access list or a prefix list with the **distribute-list in** command.

Use the **gateway** keyword only with the **prefix-list** keyword.

To suppress networks from being advertised in updates, use the **distribute-list out** command.

Examples

In the following example, the BGP routing process accepts only two networks—network 0.0.0.0 and network 131.108.0.0:

```
access-list 1 permit 0.0.0.0
access-list 1 permit 131.108.0.0
access-list 1 deny 0.0.0.0 255.255.255.255
router bgp
 network 131.108.0.0
 distribute-list 1 in
```

In the following example, The RIP process accepts only prefixes with prefix lengths of /8 to /24:

```
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
router rip
 network 131.108.0.0
 distribute-list prefix max24 in
```

In the following example, the RIP process filters on packet length and accepts routing updates from address 192.1.1.1 only:

```
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
ip prefix-list allowlist seq5 permit 192.1.1.1/32
router rip
 network 131.108.0.0
 distribute-list prefix max24 gateway allowlist in
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
distribute-list out (RIP, IGRP, EIGRP)	Suppresses networks from being advertised in updates.
ip prefix-list	Creates an entry in a prefix list.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

distribute-list out (RIP, IGRP, EIGRP)

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* [**gateway** *prefix-list-name*]} **out** [*interface-name* | *routing-process* | *as-number*]

no distribute-list {*access-list-number* | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*]} **out** [*interface-name* | *routing-process* | *as-number*]

Syntax Description

access-list-number	Standard IP access list number. The list defines which networks are to be received and which are to be suppressed in routing updates.
prefix *prefix-list-name*	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.
gateway *prefix-list-name*	(Optional) Name of the prefix list to be applied to the gateway of the prefix being updated.
out	Applies the access list to outgoing routing updates.
interface-name	(Optional) Name of a particular interface.
routing-process	(Optional) Name of a particular routing process, or the keyword **static** or **connected**.
as-number	(Optional) Autonomous system number.

Defaults

This command is disabled by default.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-number* argument was added.
12.0	The *prefix-list-name* argument was added.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

When redistributing networks, a routing process name can be specified as an optional trailing argument to the **distribute-list** command. Specifying an argument causes the access list or prefix list to be applied to only those routes derived from the specified routing process. After the process-specific access list or prefix list is applied, any access list or prefix list specified by a **distribute-list** command without a process name argument will be applied. Addresses not specified in the **distribute-list** command will not be advertised in outgoing routing updates.

Specify either an access list or a prefix list with the **distribute-list in** command.

Use the **gateway** keyword only with the **prefix-list** keyword.

Note To filter networks received in updates, use the **distribute-list in** command.

Examples

The following example causes only one network (network 131.108.0.0) to be advertised by a RIP routing process:

```
access-list 1 permit 131.108.0.0
access-list 1 deny 0.0.0.0 255.255.255.255
router rip
 network 131.108.0.0
 distribute-list 1 out
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
distribute-list in (RIP, IGRP, EIGRP)	Filters networks received in updates.
ip prefix-list	Creates an entry in a prefix list.

eigrp log-neighbor-changes

To enable the logging of changes in Enhanced IGRP (EIGRP) neighbor adjacencies, use the **eigrp log-neighbor-changes** command in router configuration mode. 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.

Defaults

No adjacency changes are logged.

Command Modes

Router configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The configuration of this command enables the logging of neighbor adjacency changes to monitor the stability of the routing system and to help detect problems.

Examples

The following configuration will log neighbor changes for EIGRP process 209:

```
router eigrp 209
 eigrp log-neighbor-changes
```

eigrp log-neighbor-warnings

To enable the logging of Enhanced IGRP (EIGRP) neighbor warning messages, use the **eigrp log-neighbor-warnings** command in router configuration mode. 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

seconds	(Optional) The time interval (in seconds) between repeated neighbor warning messages. The range of seconds is from 1 to 65535.

Defaults

Neighbor warning messages are logged.

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)	This command was introduced.

Usage Guidelines

When neighbor warning messages occur, they are logged by default. With this command, you can disable and enable neighbor warning messages, and configure the interval between repeated neighbor warning messages.

Examples

The following command will log neighbor warning messages for EIGRP process 209 and repeat the warning messages in 5-minute (300 seconds) intervals:

```
router eigrp 209
 eigrp log-neighbor-warnings 300
```

eigrp stub

To configure a router as a stub using Enhanced IGRP (EIGRP), use the **eigrp stub** command in router configuration mode. 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.

Defaults

Stub routing is not enabled by default.

Command Modes

Router configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(15)S	This command was integrated into Cisco IOS Release 12.0(15)S.

Usage Guidelines

Use the **eigrp stub** command to configure a router as a stub where the router directs all IP traffic to a distribution router.

The **eigrp stub** command can be modified with several options, and these options can be used in any combination except for the **receive-only** keyword. The **receive-only** keyword will restrict the router from sharing any of its routes with any other router in that EIGRP autonomous system, and the **receive-only** keyword will not permit any other option to be specified because it prevents any type of route from being sent. The three other optional keywords (**connected**, **static**, and **summary**) can be used in any combination but cannot be used with the **receive-only** keyword. If any of these three keywords is used individually with the **eigrp stub** command, connected and summary routes will not be sent automatically.

The **connected** keyword will permit the EIGRP Stub Routing feature to send connected routes. If the connected routes are not covered by a network statement, it may be necessary to redistribute connected routes with the **redistribute connected** command under the EIGRP process. This option is enabled by default.

The **static** keyword will permit the EIGRP Stub Routing feature to send static routes. Without the configuration of this option, EIGRP will not send any static routes, including internal static routes that normally would be automatically redistributed. It will still be necessary to redistribute static routes with the **redistribute static** command.

The **summary** keyword will permit the EIGRP Stub Routing feature to send summary routes. Summary routes can be created manually with the **summary address** command or automatically at a major network border router with the **auto-summary** command enabled. This option is enabled by default.

Note Multi-access interfaces, such as ATM, Ethernet, Frame Relay, ISDN PRI, and X.25, are supported by the EIGRP Stub Routing feature only when all routers on that interface, except the hub, are configured as stub routers.

Examples

In the following example, the **eigrp stub** command is used to configure the router as a stub that advertises connected and summary routes:

```
router eigrp 1
network 10.0.0.0
eigrp stub
```

In the following example, the **eigrp stub** command is issued with the **connected** and **static** keywords to configure the router as a stub that advertises connected and static routes (sending summary routes will not be permitted):

```
router eigrp 1
network 10.0.0.0
eigrp stub connected static
```

In the following example, the **eigrp stub** command is issued with the **receive-only** keyword to configure the router as a receive-only neighbor (connected, summary, and static routes will not be sent):

```
router eigrp 1
network 10.0.0.0 eigrp
eigrp stub receive-only
```

ip authentication key-chain eigrp

To enable authentication of Enhanced IGRP (EIGRP) packets, use the **ip authentication key-chain eigrp** command in interface configuration mode. 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

as-number	Autonomous system number to which the authentication applies.
key-chain	Name of the authentication key chain.

Defaults

No authentication is provided for EIGRP packets.

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Examples

The following example applies authentication to autonomous system 2 and identifies a key chain named SPORTS:

```
ip authentication key-chain eigrp 2 SPORTS
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ip authentication mode eigrp	Specifies the type of authentication used in EIGRP packets.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication of routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

ip authentication mode eigrp

To specify the type of authentication used in Enhanced IGRP (EIGRP) packets, use the **ip authentication mode eigrp** command in interface configuration mode. 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

as-number	Autonomous system number.
md5	Keyed Message Digest 5 (MD5) authentication.

Defaults

No authentication is provided for EIGRP packets.

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

Configure authentication to prevent unapproved sources from introducing unauthorized or false routing messages. When authentication is configured, an MD5 keyed digest is added to each EIGRP packet in the specified autonomous system.

Examples

The following example configures the interface to use MD5 authentication in EIGRP packets in autonomous system 10:

```
ip authentication mode eigrp 10 md5
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ip authentication key-chain eigrp	Enables authentication of EIGRP packets.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication of routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

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** command in interface configuration mode. 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

as-number	Autonomous system number.
percent	Percent of bandwidth that EIGRP may use.

Defaults

50 percent

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

EIGRP will use up to 50 percent of the bandwidth of a link, as defined by the **bandwidth** interface configuration command. This command may be used if some other fraction of the bandwidth is desired. Note that values greater than 100 percent may be configured. The configuration option may be useful if the bandwidth is set artificially low for other reasons.

Examples

The following example allows EIGRP to use up to 75 percent (42 kbps) of a 56-kbps serial link in autonomous system 209:

```
interface serial 0
 bandwidth 56
 ip bandwidth-percent eigrp 209 75
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.

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** command in interface configuration mode. 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

as-number	Autonomous system number.
seconds	Hello interval (in seconds).

Defaults

For low-speed, nonbroadcast multiaccess (NBMA) networks: 60 seconds

For all other networks: 5 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The default of 60 seconds applies only to low-speed, NBMA media. Low speed is considered to be a rate of T1 or slower, as specified with the **bandwidth** interface configuration command. Note that for the purposes of Enhanced IGRP, Frame Relay and Switched Multimegabit Data Service (SMDS) networks may be considered to be NBMA. These networks are considered NBMA if the interface has not been configured to use physical multicasting; otherwise, they are considered not to be NBMA.

Examples

The following example sets the hello interval for Ethernet interface 0 to 10 seconds:

```
interface ethernet 0
 ip hello-interval eigrp 109 10
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.
ip hold-time eigrp	Configures the hold time for a particular EIGRP routing process designated by the autonomous system number.

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** command in interface configuration mode. 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

as-number	Autonomous system number.
seconds	Hold time (in seconds).

Defaults

For low-speed, nonbroadcast multiaccess (NBMA) networks: 180 seconds

For all other networks: 15 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

On very congested and large networks, the default hold time might not be sufficient time for all routers and access servers to receive hello packets from their neighbors. In this case, you may want to increase the hold time.

We recommend that the hold time be at least three times the hello interval. If a router does not receive a hello packet within the specified hold time, routes through this router are considered unavailable.

Increasing the hold time delays route convergence across the network.

The default of 180 seconds hold time and 60 seconds hello interval apply only to low-speed, NBMA media. Low speed is considered to be a rate of T1 or slower, as specified with the **bandwidth** interface configuration command.

Examples

The following example sets the hold time for Ethernet interface 0 to 40 seconds:

```
interface ethernet 0
 ip hold-time eigrp 109 40
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.
ip hello-interval eigrp	Configures the hello interval for the EIGRP routing process designated by an autonomous system number.

ip split-horizon eigrp

To enable Enhanced IGRP (EIGRP) split horizon, use the **ip split-horizon eigrp** command in interface configuration mode. 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

as-number	Autonomous system number.

Defaults

The behavior of this command is enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

For networks that include links over X.25 packet-switched networks (PSNs), you can use the **neighbor** router configuration command to defeat the split horizon feature. As an alternative, you can explicitly specify the **no ip split-horizon eigrp** command in your configuration. However, if you do so, you must similarly disable split horizon for all routers and access servers in any relevant multicast groups on that network.

Note In general, we recommend that you not change the default state of split horizon unless you are certain that your application requires the change in order to properly advertise routes. Remember that if split horizon is disabled on a serial interface and that interface is attached to a packet-switched network, you must disable split horizon for all routers and access servers in any relevant multicast groups on that network.

Examples

The following example disables split horizon on a serial link connected to an X.25 network:

```
interface serial 0
 encapsulation x25
 no ip split-horizon eigrp 101
```

Related Commands

Command	Description
ip split-horizon (IGRP)	Enables the split horizon mechanism.
neighbor (IGRP)	Defines a neighboring router with which to exchange routing information.

ip summary-address eigrp

To configure a summary aggregate address for a specified interface, use the **ip summary-address eigrp** command in interface configuration mode. 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

as-number	Autonomous system number.
network-address	IP summary aggregate address to apply to an interface.
subnet-mask	Subnet mask.
admin-distance	(Optional) Administrative distance. A value from 0 to 255.

Defaults

No summary aggregate addresses are predefined. The default administrative distance metric for EIGRP is 90.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	The *admin-distance* argument was added.

Usage Guidelines

EIGRP summary routes are given an administrative distance value of 5. The administrative distance metric is used to advertise a summary without installing it in the routing table.

Examples

The following example sets the IP summary aggregate address for Ethernet interface 0 with an administrative distance of 95:

```
interface ethernet 0
 ip summary-address eigrp 109 192.168.0.0 255.255.0.0 95
```

Related Commands

Command	Description
auto-summary (Enhanced IGRP)	Restores the default behavior of automatic summarization of subnet routes into network-level routes.

metric weights (Enhanced IGRP)

To allow the tuning of the IGRP or Enhanced IGRP (EIGRP) metric calculations, use the **metric weights** command in router configuration mode. 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

tos	Type of service must always be zero.
k1k2 k3 k4 k5	Constants that convert an IGRP or EIGRP metric vector into a scalar quantity.

Defaults

tos: 0

k1: 1

k2: 0

k3: 1

k4: 0

k5: 0

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command to alter the default behavior of IGRP routing and metric computation and allow the tuning of the IGRP metric calculation for a particular type of service (ToS).

If k5 equals 0, the composite IGRP or EIGRP metric is computed according to the following formula:

metric = [k1 * bandwidth + (k2 * bandwidth)/(256 - load) + k3 * delay]

If k5 does not equal zero, an additional operation is performed:

metric = metric * [k5/(reliability + k4)]

Bandwidth is inverse minimum bandwidth of the path in BPS scaled by a factor of $2.56 * 10^{12}$. The range is from a 1200-bps line to 10 terabits per second.

Delay is in units of 10 microseconds. The range of delay is from 10 microseconds to 168 seconds. A delay of all ones indicates that the network is unreachable.

The delay parameter is stored in a 32-bit field, in increments of 39.1 nanoseconds. The range of delay is from 1 (39.1 nanoseconds) to hexadecimal FFFFFFFF (decimal 4,294,967,040 nanoseconds). A delay of all ones (that is, a delay of hexadecimal FFFFFFFF) indicates that the network is unreachable.

Table 20 lists the default values used for several common media.

Table 20 Bandwidth Values by Media Type

Media Type	Delay	Bandwidth
Satellite	5120 (2 seconds)	5120 (500 megabits)
Ethernet	25600 (1 milliseconds [ms])	256000 (10 megabits)
1.544 Mbps	512000 (20,000 ms)	1,657,856 bits
64 kbps	512000 (20,000 ms)	40,000,000 bits
56 kbps	512000 (20,000 ms)	45,714,176 bits
10 kbps	512000 (20,000 ms)	256,000,000 bits
1 kbps	512000 (20,000 ms)	2,560,000,000 bits

Reliability is given as a fraction of 255. That is, 255 is 100 percent reliability or a perfectly stable link.

Load is given as a fraction of 255. A load of 255 indicates a completely saturated link.

Examples

The following example sets the metric weights to slightly different values than the defaults:

```
router igrp 109
 network 192.168.0.0
 metric weights 0 2 0 2 0 0
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.
delay (interface)	Sets a delay value for an interface.
metric holddown	Keeps new IGRP routing information from being used for a certain period of time.
metric maximum-hops	Causes the IP routing software to advertise as unreachable those routes with a hop count higher than is specified by the command (IGRP only).

network (Enhanced IGRP)

To specify a list of networks for the Enhanced IGRP (EIGRP) routing process, use the **network** command in router configuration mode. To remove an entry, use the **no** form of this command.

network *network-number* [*network-mask*]

no network *network-number* [*network-mask*]

Syntax Description

network-number	IP address of the directly connected networks.
network-mask	(Optional) Network mask.

Defaults

No networks are specified.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(4)T	The *network-mask* argument was added.

Usage Guidelines

There is no limit to the number of **network** commands you can use on the router.

IGRP or EIGRP sends updates to the interfaces in the specified networks. Also, if the network of an interface is not specified, it will not be advertised in any IGRP or EIGRP update.

The network mask can be as specific as the interface mask.

Examples

The following example configures a router for IGRP and assigns autonomous system 109. The **network** commands indicate the networks directly connected to the router.

```
router igrp 109
 network 172.16.0.0
 network 192.168.7.0
```

Related Commands

Command	Description
router eigrp	Configures the EIGRP routing process.
router igrp	Configures the IGRP routing process.

offset-list (Enhanced IGRP)

To add an offset to incoming and outgoing metrics to routes learned via Enhanced IGRP (EIGRP), use the **offset-list** command in router configuration mode. 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

access-list-number | *access-list-name*	Standard access list number or name to be applied. Access list number 0 indicates all access lists. If the *offset* 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.
offset	Positive offset to be applied to metrics for networks matching the access list. If the offset is 0, no action is taken.
interface-type	(Optional) Interface type to which the offset list is applied.
interface-number	(Optional) Interface number to which the offset list is applied.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The *interface-type* and *interface-number* arguments were added.
11.2	The *access-list-name* argument was added.

Usage Guidelines

The offset value is added to the routing metric. An offset list with an interface type and interface number is considered extended and takes precedence over an offset list that is not extended. Therefore, if an entry passes the extended offset list and the normal offset list, the offset of the extended offset list is added to the metric.

Examples

In the following example, the router applies an offset of 10 to the delay component of the router only to access list 21:

```
offset-list 21 out 10
```

In the following example, the router applies an offset of 10 to routes learned from Ethernet interface 0:

```
offset-list 21 in 10 ethernet 0
```

router eigrp

To configure the Enhanced IGRP (EIGRP) routing process, use the **router eigrp** command in global configuration mode. To shut down a routing process, use the **no** form of this command.

router eigrp *as-number*

no router eigrp *as-number*

Syntax Description

as-number	Autonomous system number that identifies the routes to the other EIGRP routers. It is also used to tag the routing information.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example configures an EIGRP routing process and assigns process number 109:

```
router eigrp 109
```

Related Commands

Command	Description
network (Enhanced IGRP)	Specifies a list of networks for the EIGRP routing process.

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

bandwidth	Metric value or IGRP bandwidth of the route in kbps. It can be in the range 0 to 4294967295.
delay	Route delay (in tens of microseconds). It can be in the range from 0 to 4294967295.
reliability	Likelihood of successful packet transmission expressed as a number from 0 to 255. The value 255 means 100 percent reliability; 0 means no reliability.
loading	Effective bandwidth of the route expressed as a number from 0 to 255 (255 is 100 percent loading).
mtu	Minimum maximum transmission unit (MTU) size of the route, in bytes. It can be in the range from 0 to 4294967295.

Defaults

No metric will be set in the route map.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

We recommend you consult your Cisco technical support representative before changing the default value.

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution *set actions* to be performed when all of the match criteria for a router are met. When all match criteria are met, all set actions are performed.

Examples

The following example sets the bandwidth to 10,000, the delay to 10, the reliability to 255, the loading to 1, and the MTU to 1500:

```
set metric 10000 10 255 1 1500
```

show ip eigrp interfaces

To display information about interfaces configured for Enhanced IGRP (EIGRP), use the **show ip eigrp interfaces** command in EXEC mode.

show ip eigrp interfaces [*interface-type interface-number*] [*as-number*]

Syntax Description

interface-type	(Optional) Interface type.
interface-number	(Optional) Interface number.
as-number	(Optional) Autonomous system number.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use the **show ip eigrp interfaces** command to determine on which interfaces EIGRP is active, and to learn information about EIGRP relating to those interfaces.

If an interface is specified, only that interface is displayed. Otherwise, all interfaces on which EIGRP is running are displayed.

If an autonomous system is specified, only the routing process for the specified autonomous system is displayed. Otherwise, all EIGRP processes are displayed.

Examples

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

```
Router# show ip eigrp interfaces

IP EIGRP interfaces for process 109

                    Xmit Queue    Mean   Pacing Time   Multicast   Pending
Interface   Peers   Un/Reliable   SRTT   Un/Reliable   Flow Timer  Routes
Di0           0         0/0          0      11/434          0          0
Et0           1         0/0        337       0/10           0          0
SE0:1.16      1         0/0         10       1/63         103          0
Tu0           1         0/0        330       0/16           0          0
```

Table 21 describes the significant fields shown in the display.

Table 21 show ip eigrp interfaces Field Descriptions

Field	Description
Interface	Interface over which EIGRP is configured.
Peers	Number of directly connected EIGRP neighbors.

Table 21 show ip eigrp interfaces Field Descriptions (continued)

Field	Description
Xmit Queue Un/Reliable	Number of packets remaining in the Unreliable and Reliable transmit queues.
Mean SRTT	Mean smooth round-trip time (SRTT) interval (in seconds).
Pacing Time Un/Reliable	Pacing time used to determine when EIGRP packets should be sent out the interface (unreliable and reliable packets).
Multicast Flow Timer	Maximum number of seconds in which the router will send multicast EIGRP packets.
Pending Routes	Number of routes in the packets in the transmit queue waiting to be sent.

Related Commands

Command	Description
show ip eigrp neighbors	Displays the neighbors discovered by EIGRP.

show ip eigrp neighbors

To display the neighbors discovered by Enhanced IGRP (EIGRP), use the **show ip eigrp neighbors** command in EXEC mode.

show ip eigrp neighbors [*interface-type* | *as-number* | **static**]

Syntax Description

interface-type	(Optional) Interface type.
as-number	(Optional) Autonomous system number.
static	(Optional) Static routes.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.0(7)T	The **static** keyword was added.

Usage Guidelines

Use the **show ip eigrp neighbors** command to determine when neighbors become active and inactive. It is also useful for debugging certain types of transport problems.

Examples

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

```
Router# show ip eigrp neighbors

IP-EIGRP Neighbors for process 77
Address                Interface     Holdtime Uptime   Q      Seq  SRTT  RTO
                                     (secs)   (h:m:s)  Count  Num  (ms)  (ms)
172.16.81.28           Ethernet1     13       0:00:41  0      11   4     20
172.16.80.28           Ethernet0     14       0:02:01  0      10   12    24
172.16.80.31           Ethernet0     12       0:02:02  0      4    5     20
```

Table 22 describes the significant fields shown in the display.

Table 22 show ip eigrp neighbors Field Descriptions

Field	Description
process 77	Autonomous system number specified in the **router** configuration command.
Address	IP address of the EIGRP peer.
Interface	Interface on which the router is receiving hello packets from the peer.
Holdtime	Length of time (in seconds) that the Cisco IOS software will wait to hear from the peer before declaring it down. If the peer is using the default hold time, this number will be less than 15. If the peer configures a nondefault hold time, the nondefault hold time will be displayed.

Table 22 show ip eigrp neighbors Field Descriptions (continued)

Field	Description
Uptime	Elapsed time (in hours:minutes: seconds) since the local router first heard from this neighbor.
Q Count	Number of EIGRP packets (update, query, and reply) that the software is waiting to send.
Seq Num	Sequence number of the last update, query, or reply packet that was received from this neighbor.
SRTT	Smooth round-trip time. This is the number of milliseconds required for an EIGRP packet to be sent to this neighbor and for the local router to receive an acknowledgment of that packet.
RTO	Retransmission timeout (in milliseconds). This is the amount of time the software waits before resending a packet from the retransmission queue to a neighbor.

show ip eigrp topology

To display entries in the Enhanced IGRP (EIGRP) topology table, use the **show ip eigrp topology** command in EXEC mode.

show ip eigrp topology [*as-number* | [[*ip-address*] *mask*]] [**active** | **all-links** | **pending** | **summary** | **zero-successors**]

Syntax Description

as-number	(Optional) Autonomous system number.
ip-address	(Optional) IP address. When specified with a mask, a detailed description of the entry is provided.
mask	(Optional) Subnet mask.
active	(Optional) Displays only active entries in the EIGRP topology table.
all-links	(Optional) Displays all entries in the EIGRP topology table.
pending	(Optional) Displays all entries in the EIGRP topology table that are waiting for an update from a neighbor or are waiting to reply to a neighbor.
summary	(Optional) Displays a summary of the EIGRP topology table.
zero-successors	(Optional) Displays available routes in the EIGRP topology table.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **show ip eigrp topology** command can be used without any keywords or arguments. If this command is used without any keywords or arguments, then only routes that are feasible successors are displayed. The **show ip eigrp topology** command can be used to determine Diffusing Update Algorithm (DUAL) states and to debug possible DUAL problems.

Examples

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

```
Router# show ip eigrp topology

IP-EIGRP Topology Table for process 77

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 172.16.90.0 255.255.255.0, 2 successors, FD is 0
          via 172.16.80.28 (46251776/46226176), Ethernet0
          via 172.16.81.28 (46251776/46226176), Ethernet1
          via 172.16.80.31 (46277376/46251776), Serial0
P 172.16.81.0 255.255.255.0, 1 successors, FD is 307200
          via Connected, Ethernet1
```

```
        via 172.16.81.28 (307200/281600), Ethernet1
        via 172.16.80.28 (307200/281600), Ethernet0
        via 172.16.80.31 (332800/307200), Serial0
```

Table 23 describes the significant fields shown in the display.

Table 23 show ip eigrp topology Field Descriptions

Field	Description
Codes	State of this topology table entry. Passive and Active refer to the EIGRP state with respect to this destination; Update, Query, and Reply refer to the type of packet that is being sent.
P – Passive	No EIGRP computations are being performed for this destination.
A – Active	EIGRP computations are being performed for this destination.
U – Update	Indicates that an update packet was sent to this destination.
Q – Query	Indicates that a query packet was sent to this destination.
R – Reply	Indicates that a reply packet was sent to this destination.
r – Reply status	Flag that is set after the software has sent a query and is waiting for a reply.
172.16.90.0	Destination IP network number.
255.255.255.0	Destination subnet mask.
successors	Number of successors. This number corresponds to the number of next hops in the IP routing table. If “successors” is capitalized, then the route or next hop is in a transition state.
FD	Feasible distance. The feasible distance is the best metric to reach the destination or the best metric that was known when the route went active. This value is used in the feasibility condition check. If the reported distance of the router (the metric after the slash) is less than the feasible distance, the feasibility condition is met and that path is a feasible successor. Once the software determines it has a feasible successor, it need not send a query for that destination.
replies	Number of replies that are still outstanding (have not been received) with respect to this destination. This information appears only when the destination is in Active state.
state	Exact EIGRP state that this destination is in. It can be the number 0, 1, 2, or 3. This information appears only when the destination is in the Active state.
via	IP address of the peer that told the software about this destination. The first *n* of these entries, where N is the number of successors, are the current successors. The remaining entries on the list are feasible successors.
(46251776/46226176)	The first number is the EIGRP metric that represents the cost to the destination. The second number is the EIGRP metric that this peer advertised.
Ethernet0	Interface from which this information was learned.
Serial0	Interface from which this information was learned.

show ip eigrp traffic

To display the number of Enhanced IGRP (EIGRP) packets sent and received, use the **show ip eigrp traffic** command in EXEC mode.

show ip eigrp traffic [*as-number*]

Syntax Description

as-number	(Optional) Autonomous system number.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

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

```
Router# show ip eigrp traffic

IP-EIGRP Traffic Statistics for process 77
  Hellos sent/received: 218/205
  Updates sent/received: 7/23
  Queries sent/received: 2/0
  Replies sent/received: 0/2
  Acks sent/received: 21/14
```

Table 24 describes the significant fields shown in the display.

Table 24 show ip eigrp traffic Field Descriptions

Field	Description
process 77	Autonomous system number specified in the **ip router** command.
Hellos sent/received	Number of hello packets sent and received.
Updates sent/received	Number of update packets sent and received.
Queries sent/received	Number of query packets sent and received.
Replies sent/received	Number of reply packets sent and received.
Acks sent/received	Number of acknowledgment packets sent and received.

timers active-time

To adjust routing wait time, use the **timers active-time** command in router configuration mode. To disable this function, use the **no** form of the command.

timers active-time [*time-limit* | **disabled**]

no timers active-time

Syntax Description

time-limit	EIGRP active-time limit (in minutes). The time range is from 1to 4294967295 minutes.
disabled	Disables the timers and permits the routing wait time to remain active indefinitely.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

In EIGRP, there are timers that control the time the router waits (after sending a query) before declaring the route to be in the stuck in active (SIA) state.

Examples

In the following example, the routing wait time is 200 minutes on the specified route:

```
router igrp 5
 timers active-time 200
```

In the following example, the routing wait time is indefinite on the specified route:

```
router igrp 5
 timers active-time disabled
```

Related Commands

Command	Description
show ip eigrp topology	Displays the EIGRP topology table.

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** command in router configuration mode. 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.

Defaults

Traffic is distributed proportionately to the ratios of the metrics.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command applies to IGRP and EIGRP routing protocols only. With the default setting, routes that have higher metrics represent less-preferable routes and get less traffic.

Examples

In the following example, traffic is balanced across multiple routes:

```
router eigrp 5
 traffic-share balanced
 variance 1
```

Related Commands

Command	Description
variance (Enhanced IGRP)	Controls load balancing in an EIGRP and IGRP internetwork.

variance (Enhanced IGRP)

To control load balancing in an Enhanced IGRP-based internetwork, use the **variance** command in router configuration mode. To reset the variance to the default value, use the **no** form of this command.

variance *multiplier*

no variance

Syntax Description

multiplier	Metric value used for load balancing. It can be a value from 1 to 128. The default is 1, which means equal-cost load balancing.

Defaults

1 (equal-cost load balancing)

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Setting a variance value lets the Cisco IOS software determine the feasibility of a potential route. A route is feasible if the next router in the path is closer to the destination than the current router and if the metric for the entire path is within the variance. Only paths that are feasible can be used for load balancing and included in the routing table.

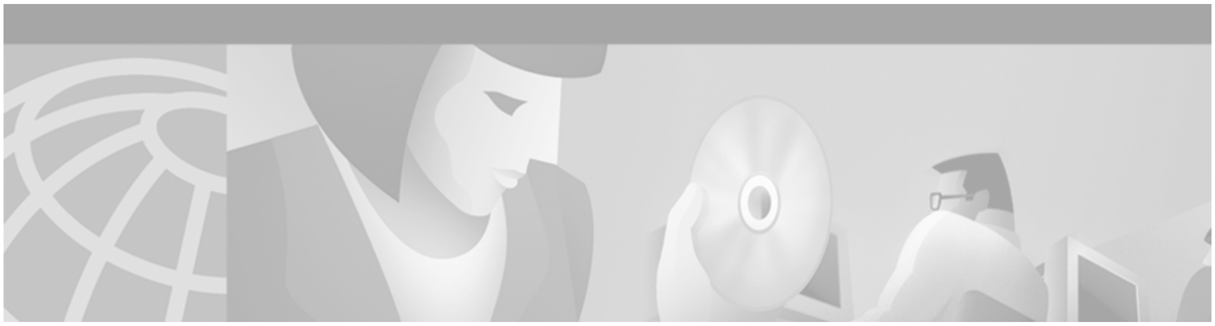
If the following two conditions are met, the route is deemed feasible and can be added to the routing table:

- The local best metric must be greater than the metric learned from the next router.
- The multiplier times the local best metric for the destination must be greater than or equal to the metric through the next router.

Examples

The following example sets a variance value of 4:

```
router igrp 109
 variance 4
```



Integrated IS-IS Commands

Use the commands in this chapter to configure and monitor the Intermediate System-to-Intermediate System (IS-IS) protocol. For IS-IS configuration information and examples, refer to the "Configuring Integrated IS-IS" chapter of the *Cisco IOS IP Configuration Guide*.

area-password

To configure the IS-IS area authentication password, use the **area-password** command in router configuration mode. To disable the password, use the **no** form of this command.

area-password *password*

no area-password [*password*]

Syntax Description

password	Password you assign.

Defaults

No area password is defined, and area password authentication is disabled.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Using the **area-password** command on all routers in an area will prevent unauthorized routers from injecting false routing information into the link-state database.

This password is exchanged as plain text and thus this feature provides only limited security.

This password is inserted in Level 1 (station router level) protocol data unit (PDU) link-state packets (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNP).

Examples

The following example assigns an area authentication password:

```
router isis
 area-password angel
```

Related Commands

Command	Description
domain-password	Configures the IS-IS routing domain authentication password.
isis password	Configures the authentication password for an interface.

default-information originate (IS-IS)

To generate a default route into an IS-IS routing domain, use the **default-information originate** command in router configuration mode. 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.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

If a router configured with this command has a route to 0.0.0.0 in the routing table, IS-IS will originate an advertisement for 0.0.0.0 in its link-state packets (LSPs).

Without a route map, the default is only advertised in Level 2 LSPs. For Level 1 routing, there is another mechanism to find the default route, which is to look for the closest Level 1 or Level 2 router. The closest Level 1 or Level 2 router can be found by looking at the attached-bit (ATT) in Level 1 LSPs.

A route map can be used for two purposes:

- Make the router generate default in its Level 1 LSPs.
- Advertise 0/0 conditionally.

With a **match ip address** *standard-access-list* command, you can specify one or more IP routes that must exist before the router will advertise 0/0.

Examples

The following example forces the software to generate a default external route into an IS-IS domain:

```
router isis
! BGP routes will be distributed into IS-IS
redistribute bgp 120
! access list 2 is applied to outgoing routing updates
distribute-list 2 out
default-information originate
! access list 2 defined as giving access to network 10.105.0.0
access-list 2 permit 10.105.0.0 0.0.255.255
```

Related Commands

Command	Description
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
show isis database	Displays the IS-IS link-state database.

domain-password

To configure the IS-IS routing domain authentication password, use the **domain-password** command in router configuration mode. To disable a password, use the **no** form of this command.

domain-password *password*

no domain-password [*password*]

Syntax Description

password	Password you assign.

Defaults

No password is specified and no authentication is enabled for exchange of Level 2 routing information.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This password is exchanged as plain text and thus this feature provides only limited security.

This password is inserted in Level 2 (area router level) protocol data unit (PDU) link-state packets (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs).

Examples

The following example assigns an authentication password to the routing domain:

```
router isis
 domain-password flower
```

Related Commands

Command	Description
area-password	Configures the IS-IS area authentication password.
isis password	Configures the authentication password for an interface.

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** command in interface configuration mode. 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

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. **Note** Each area in a multiarea configuration should have a nonnull area tag to facilitate identification of the area.

Defaults

No routing processes are specified.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	Multiarea functionality was added, changing the way the *tag* argument (now *area-tag*) is used.

Usage Guidelines

Before the IS-IS routing process is useful, a network entity title (NET) must be assigned with the **net** command and some interfaces must have IS-IS enabled.

If you have IS-IS running and at least one International Organization for Standardization Interior Gateway Routing Protocol (ISO-IGRP) process, the IS-IS process and the ISO-IGRP process cannot both be configured without an area tag. The null tag can be used by only one process. If you run ISO-IGRP and IS-IS, a null tag can be used for IS-IS, but not for ISO-IGRP at the same time. However, each area in an IS-IS multiarea configuration should have a nonnull area tag to facilitate identification of the area.

You can configure only one process to perform Level 2 (interarea) routing. If Level 2 routing is configured on any process, all additional processes are automatically configured as Level 1. You can configure this process to perform intra-area (Level 1) routing at the same time. You can configure up to 29 additional processes as Level 1-only processes. Use the **is-type** command to remove Level 2 routing from a router instance. You can then use the **is-type** command to enable Level 2 routing on some other IS-IS router instance.

An interface cannot be part of more than one area, except in the case where the associated routing process is performing both Level 1 and Level 2 routing. On media such as WAN media where subinterfaces are supported, different subinterfaces could be configured for different areas.

Examples

The following example specifies IS-IS as an IP routing protocol for a process named Finance, and specifies that the Finance process will be routed on Ethernet interface 0 and serial interface 0:

```
router isis Finance
 net 49.0001.aaaa.aaaa.aaaa.00
interface Ethernet 0
 ip router isis Finance
interface serial 0
 ip router isis Finance
```

The following example shows an IS-IS configuration with two Level 1 areas and one Level 1-2 area:

```
ip routing

.
.
.

interface Tunnel529
 ip address 10.0.0.5 255.255.255.0
 ip router isis BB

interface Ethernet1
 ip address 10.1.1.5 255.255.255.0
 ip router isis A3253-01
1
!
interface Ethernet2
 ip address 10.2.2.5 255.255.255.0
 ip router isis A3253-02


.
.
.

! Defaults to "is-type level-1-2"
router isis BB
 net 49.2222.0000.0000.0005.00
!
router isis A3253-01
 net 49.0553.0001.0000.0000.0005.00
 is-type level-1
!
router isis A3253-02
 net 49.0553.0002.0000.0000.0005.00
 is-type level-1
```

Related Commands

Command	Description
is-type	Configures the routing level for an IS-IS routing process.
net	Configures an IS-IS NET for a CLNS routing process.
router isis	Enables the IS-IS routing protocol.

isis circuit-type

To configure the type of adjacency, use the **isis circuit-type** command in interface configuration mode. To reset the circuit type to Level l 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 Level 2 adjacency only.

Defaults

A Level 1 and Level 2 adjacency is established.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Normally, this command need not be configured. The proper way is to configure a router as a Level 1-only, Level 1-2, or Level 2-only system. Only on routers that are between areas (Level 1-2 routers) should you configure some interfaces to be Level 2-only to prevent wasting bandwidth by sending out unused Level 1 hello packets. Note that on point-to-point interfaces, the Level 1 and Level 2 hellos are in the same packet.

A Level 1 adjacency may be established if there is at least one area address in common between this system and its neighbors. Level 2 adjacencies will never be established over this interface.

A Level 1 and Level 2 adjacency is established if the neighbor is also configured as **level-1-2** and there is at least one area in common. If there is no area in common, a Level 2 adjacency is established. This is the default.

Level 2 adjacencies are established if the other routers are Level 2 or Level 1-2 routers and their interfaces are configured for Level 1-2 or Level 2. Level 1 adjacencies will never be established over this interface.

Examples

In the following example, other routers on Ethernet interface 0 are in the same area. Other routers on Ethernet interface 1 are in other areas, so the router will stop sending Level 1 hellos.

```
interface ethernet 0
ip router isis
interface ethernet 1
 isis circuit-type level-2-only
```

isis csnp-interval

To configure the IS-IS complete sequence number PDUs (CSNPs) interval, use the **isis csnp-interval** command in interface configuration mode. 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

seconds	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.

Defaults

10 seconds
Level 1 and Level 2

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

It is very unlikely you will need to change the default value of this command.

This command applies only for the designated router (DR) for a specified interface. Only DRs send CSNP packets in order to maintain database synchronization. The CSNP interval can be configured independently for Level 1 and Level 2. Configuring the CSNP interval does not apply to serial point-to-point interfaces. It does apply to WAN connections if the WAN is viewed as a multiaccess meshed network.

For multiaccess WAN interfaces such as ATM, Frame Relay, and X.25, we highly recommend that you configure the nonbroadcast multiaccess (NBMA) cloud as multiple point-to-point subinterfaces. Doing so will make routing much more robust if one or more permanent virtual circuits (PVCs) fails.

The **isis csnp-interval** command on point-to-point subinterfaces should be used only in combination with the IS-IS mesh-group feature.

Examples

The following example configures Ethernet interface 0 for sending CSNPs every 30 seconds:

```
interface ethernet 0
 isis csnp-interval 30 level-1
```

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** command in global configuration mode. 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.
count	(Optional) Number of carriage returns or length of string to use for the delimiter.
character	(Optional) Character to use for the delimiter string.

Defaults

The **isis display delimiter** command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use this command to customize display output when the IS-IS multiarea feature is used. The **isis display delimiter** command displays the output from different areas as a string or additional white space.

Examples

The following command causes different areas in multiarea displays (such as **show** command output) to be delimited by a string of dashes (-):

```
isis display delimiter - 14
```

With three IS-IS neighbors configured, this command displays the following output from the **show clns neighbors** command:

```
Router# show clns neighbors
--------------
Area L2BB:
System Id      Interface   SNPA                State  Holdtime  Type Protocol
0000.0000.0009 Tu529       172.21.39.9         Up     25        L1L2 IS-IS
--------------
Area A3253-01:
System Id      Interface   SNPA                State  Holdtime  Type Protocol
0000.0000.0053 Et1         0060.3e58.ccdb      Up     22        L1   IS-IS
0000.0000.0003 Et1         0000.0c03.6944      Up     20        L1   IS-IS
```

```
--------------
Area A3253-02:
System Id      Interface   SNPA                State  Holdtime  Type Protocol
0000.0000.0002 Et2         0000.0c03.6bc5      Up     27        L1   IS-IS
0000.0000.0053 Et2         0060.3e58.ccde      Up     24        L1   IS-IS
```

Related Commands

Command	Description
show clns es-neighbors	Lists the ES neighbors that this router knows.
show clns is-neighbors	Displays IS-IS related information for IS-IS router adjacencies.
show clns neighbors	Displays both ES and IS neighbors.
show clns protocol	Lists the protocol-specific information for each ISO IGRP routing process in the router.
show clns traffic	Lists the CLNS packets this router has seen.
show isis database	Displays the IS-IS link-state database.
show isis routes	Displays the IS-IS Level 1 forwarding table for IS-IS learned routes.
show isis spf-log	Displays how often and why the router has run a full SPF calculation.
show isis topology	Displays a list of all connected routers in all areas.

isis hello-interval

To specify the length of time between hello packets that the Cisco IOS software sends, use the **isis hello-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

isis hello-interval {*seconds* | **minimal**} [**level-1** | **level-2**]

no isis hello-interval [**level-1** | **level-2**]

Syntax Description

seconds	An integer value. By default, a value three times the hello interval *seconds* is advertised as the hold time in the hello packets sent. (Change the 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.
minimal	Causes the system to compute the hello interval based on the hello multiplier (specified by the **isis hello-multiplier** command) so that the resulting hold time is 1 second.
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.

Defaults

10 seconds
Level 1 and Level 2

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	The **minimal** keyword was added.

Usage Guidelines

The hello interval multiplied by the hello multiplier equals the hold time. If the **minimal** keyword is specified, the hold time is 1 second and the system computes the hello interval based on the hello multiplier.

The hello interval can be configured independently for Level 1 and Level 2, except on serial point-to-point interfaces. (Because only a single type of hello packet is sent on serial links, it is independent of Level 1 or Level 2.) The **level-1** and **level-2** keywords are used on X.25, SMDS, and Frame Relay multiaccess networks or LAN interfaces.

A faster hello interval gives faster convergence, but increases bandwidth and CPU usage. It might also add to instability in the network. A slower hello interval saves bandwidth and CPU. Especially when used in combination with a higher hello multiplier, this configuration may increase overall network stability.

It makes more sense to tune the hello interval and hello multiplier on point-to-point interfaces than on LAN interfaces.

Examples

The following example configures serial interface 0 to advertise hello packets every 5 seconds. The router is configured to act as a station router. This configuration will cause more traffic than configuring a longer interval, but topological changes will be detected earlier.

```
interface serial 0
 isis hello-interval 5 level-1
```

Related Commands

Command	Description
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the router should declare the adjacency as down.

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** command in interface configuration mode. 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

multiplier	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.

Defaults

multiplier: 3
Level 1 and Level 2

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The "holding time" carried in an IS-IS hello packet determines how long a neighbor waits for another hello packet before declaring the neighbor to be down. This time determines how quickly a failed link or neighbor is detected so that routes can be recalculated.

Use the **isis hello-multiplier** command in circumstances where hello packets are lost frequently and IS-IS adjacencies are failing unnecessarily. You can raise the hello multiplier and lower the hello interval (**isis hello-interval** command) correspondingly to make the hello protocol more reliable without increasing the time required to detect a link failure.

On point-to-point links, there is only one hello for both Level 1 and Level 2, so different hello multipliers should be configured only for multiaccess networks such as Ethernet and FDDI. Separate Level 1 and Level 2 hello packets are also sent over nonbroadcast multiaccess (NBMA) networks in multipoint mode, such as X.25, Frame Relay, and ATM. However, we recommend that you run IS-IS over point-to-point subinterfaces over WAN NBMA media.

Examples

In the following example, the network administrator wants to increase network stability by making sure an adjacency will go down only when many (ten) hello packets are missed. The total time to detect link failure is 60 seconds. This configuration will ensure that the network remains stable, even when the link is fully congested.

```
interface serial 1
 ip router isis
 isis hello-interval 6 level-1
 isis hello-multiplier 10 level-1
```

Related Commands

Command	Description
isis hello-interval	Specifies the length of time between hello packets that the Cisco IOS software sends.

isis lsp-interval

To configure the time delay between successive IS-IS link-state packet (LSP) transmissions, use the **isis lsp-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

isis lsp-interval *milliseconds*

no isis lsp-interval

Syntax Description

milliseconds	Time delay between successive LSPs (in milliseconds).

Defaults

The default time delay is 33 milliseconds.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

In topologies with a large number of IS-IS neighbors and interfaces, a router may have difficulty with the CPU load imposed by LSP transmission and reception. This command allows the LSP transmission rate (and by implication the reception rate of other systems) to be reduced.

Examples

The following example causes the system to send LSPs every 100 milliseconds (10 packets per second) on serial interface 0:

```
interface serial 0
 isis lsp-interval 100
```

Related Commands

Command	Description
isis retransmit-interval	Configures the time between retransmission of each LSP (IS-IS link-state PDU) over point-to-point links.

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** command in interface configuration mode. 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

number	(Optional) A number identifying the mesh group of which this interface is a member.
blocked	(Optional) Specifies that no LSP flooding will take place on this subinterface.

Defaults

The interface performs normal flooding.

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

LSPs that are first received on subinterfaces that are not part of a mesh group are flooded to all other subinterfaces in the usual way.

LSPs that are first received on subinterfaces that are part of a mesh group are flooded to all interfaces except those in the same mesh group. If the **blocked** keyword is configured on a subinterface, then a newly received LSP is not flooded out over that interface.

To minimize the possibility of incomplete flooding, you should allow unrestricted flooding over at least a minimal set of links in the mesh. Selecting the smallest set of logical links that covers all physical paths results in very low flooding, but less robustness. Ideally, you should select only enough links to ensure that LSP flooding is not detrimental to scaling performance, but enough links to ensure that under most failure scenarios no router will be logically disconnected from the rest of the network. In other words, blocking flooding on all links permits the best scaling performance, but there is no flooding. Permitting flooding on all links results in very poor scaling performance.

Examples

In the following example six interfaces are configured in three mesh groups. LSPs received are handled as follows:

- LSPs received first via ATM 1/0.1 are flooded to all interfaces except ATM 1/0.2 (which is part of the same mesh group) and ATM 1/2.1, which is blocked.
- LSPs received first via ATM 1/1.2 are flooded to all interfaces except ATM 1/1.1 (which is part of the same mesh group) and ATM 1/2.1, which is blocked.
- LSPs received first via ATM 1/2.1 are not ignored, but flooded as usual to all interfaces. LSPs received first via ATM 1/2.2 are flooded to all interfaces, except ATM 1/2.1, which is blocked.

```
interface atm 1/0.1
ip router isis
isis mesh-group 10

interface atm 1/0.2
ip router isis
isis mesh-group 10

interface atm 1/1.1
ip router isis
isis mesh-group 11

interface atm 1/1.2
ip router isis
isis mesh-group 11

interface atm 1/2.1
ip router isis
isis mesh-group blocked

interface atm 1/2.2
ip router isis
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

isis metric

To configure the metric for an interface, use the **isis metric** command in interface configuration mode. 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

default-metric	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.
level-1	(Optional) This metric should be used only in the shortest path first (SPF) calculation for Level 1 (intra-area) routing.
level-2	(Optional) This metric should be used only in the SPF calculation for Level 2 (interarea) routing.

Defaults

Level 1 and Level 2

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Specifying the **level-1** or **level-2** keyword resets the metric only for Level 1 or Level 2 routing, respectively.

We highly recommend that you configure metrics on all interfaces. If you do not do so, the IS-IS metrics are similar to hop count metrics.

Examples

The following example configures serial interface 0 for a default link-state metric cost of 15 for Level 1:

```
interface serial 0
 isis metric 15 level-1
```

isis password

To configure the authentication password for an interface, use the **isis password** command in interface configuration mode. 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

password	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.

Defaults

This command is disabled by default.

If no keyword is specified, the default is Level 1 and Level 2.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command enables you to prevent unauthorized routers from forming adjacencies with this router, and thus protects the network from intruders.

The password is exchanged as plain text and thus provides only limited security.

Different passwords can be assigned for different routing levels using the **level-1** and **level-2** kewords.

Specifying the **level-1** or **level-2** keyword disables the password only for Level 1 or Level 2 routing, respectively.

Examples

The following example configures a password for Ethernet interface 0 at Level 1:

```
interface ethernet 0
 isis password frank level-1
```

isis priority

To configure the priority of designated routers, use the **isis priority** command in interface configuration mode. 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

number-value	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.

Defaults

Priority of 64
Level 1 and Level 2

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Priorities can be configured for Level 1 and Level 2 independently. Specifying the **level-1** or **level-2** keyword resets priority only for Level 1 or Level 2 routing, respectively.

The priority is used to determine which router on a LAN will be the designated router or Designated Intermediate System (DIS). The priorities are advertised in the hello packets. The router with the highest priority will become the DIS.

In IS-IS, there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a router with a higher priority comes on line, it will take over the role from the current DIS. In the case of equal priorities, the highest MAC address breaks the tie.

Examples

The following example shows Level 1 routing given priority by setting the priority level to 80. This router is now more likely to become the DIS.

```
interface ethernet 0
 isis priority 80 level-1
```

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** command in interface configuration mode. To restore the default value, use the **no** form of this command.

isis retransmit-interval *seconds*

no isis retransmit-interval *seconds*

Syntax Description

seconds	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.

Defaults

5 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The setting of the *seconds* argument should be conservative, or needless retransmission will result.

This command has no effect on LAN (multipoint) interfaces. On point-to-point links, the value can be increased to enhance network stability.

Retransmissions occur only when LSPs are dropped. So setting the *seconds* argument to a higher value has little effect on reconvergence. The more neighbors routers have, and the more paths over which LSPs can be flooded, the higher this value can be made.

The value should be higher for serial lines.

Examples

The following example configures serial interface 0 for retransmission of IS-IS LSP, every 60 seconds for a large serial line:

```
interface serial 0
 isis retransmit-interval 60
```

Related Commands

Command	Description
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of any IS-IS LSPs on a point-to-point interface.

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** command in interface configuration mode. To restore the default value, use the **no** form of this command.

isis retransmit-throttle-interval *milliseconds*

no isis retransmit-throttle-interval

Syntax Description

milliseconds	Minimum delay (in milliseconds) between LSP retransmissions on the interface.

Defaults

The delay is determined by the **isis lsp-interval** command.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command may be useful in very large networks with many LSPs and many interfaces as a way of controlling LSP retransmission traffic. This command controls the rate at which LSPs can be re-sent on the interface.

The **isis retransmit-throttle-interval** command is distinct from the rate at which LSPs are sent on the interface (controlled by the **isis lsp-interval** command) and the period between retransmissions of a single LSP (controlled by the **isis retransmit-interval** command). These commands may all be used in combination to control the offered load of routing traffic from one router to its neighbors.

Examples

The following example configures serial interface 0 to limit the rate of LSP retransmissions to one every 300 milliseconds:

```
interface serial 0
 isis retransmit-throttle-interval 300
```

Related Commands

Command	Description
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSPs over a point-to-point link.

is-type

To configure the routing level for an instance of the IS-IS routing process, use the **is-type** command in router configuration mode. 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 learns only 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 a 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.

Defaults

In conventional IS-IS configurations, the router acts as both a Level 1 (intra-area) and a Level 2 (interarea) router.

In multiarea IS-IS configurations, the first instance of the IS-IS routing process configured is by default a Level 1-2 (intra-area and interarea) router. The remaining instances of the IS-IS process configured by default are Level 1 routers.

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	This command was modified to include multiarea IS-IS routing.

Usage Guidelines

We highly recommend that you configure the type of IS-IS routing process. If you are configuring multiarea IS-IS, you *must* configure the type of the router, or allow it to be configured by default. By default, the first instance of the IS-IS routing process that you configure using the **router isis** command is a Level 1-2 router.

If only one area is in the network, there is no need to run both Level 1 and Level 2 routing algorithms. If IS-IS is used for Connectionless Network Service (CLNS) routing (and there is only one area), Level 1 only must be used everywhere. If IS-IS is used for IP routing only (and there is only one area), you can run Level 2 only everywhere. Areas you add after the Level 1-2 area exists are by default Level 1 areas.

If the router instance has been configured for Level 1-2 (the default for the first instance of the IS-IS routing process in a Cisco device), you can remove Level 2 (interarea) routing for the area using the **is-type** command. You can also use the **is-type** command to configure Level 2 routing for an area, but it must be the only instance of the IS-IS routing process configured for Level 2 on the Cisco device.

Examples

The following example specifies an area router:

```
router isis
 is-type level-2-only
```

Related Commands

Command	Description
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.
show clns neighbor areas	Displays information about IS-IS neighbors and the areas to which they belong.

lsp-gen-interval

To customize IS-IS throttling of LSP generation, use the **lsp-gen-interval** command in router configuration mode. To restore default values, use the **no** form of this command.

lsp-gen-interval [level-1 | level-2] *lsp-max-wait* [*lsp-initial-wait lsp-second-wait*]

no lsp-gen-interval

Syntax Description

level-1	(Optional) Apply intervals to Level-1 areas only.
level-2	(Optional) Apply intervals to Level-2 areas only.
lsp-max-wait	Indicates the maximum interval (in seconds) between two consecutive ocurrences of an LSP being generated. The range is 1 to 120 seconds. The default is 5 seconds.
lsp-initial-wait	(Optional) Indicates the initial LSP generation delay (in milliseconds). The range is 1 to 120,000 milliseconds. The default is 50 milliseconds.
lsp-second-wait	(Optional) Indicates the hold time between the first and second LSP generation (in milliseconds). The range is 1 to 120,000 milliseconds. The default is 5000 milliseconds (5 seconds).

Defaults

lsp-max-wait: 5 seconds
lsp-initial-wait: 50 milliseconds
lsp-second-wait: 5000 milliseconds

Command Modes

Router configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

The following description will help you determine whether to change the default values of this command:

- The *lsp-initial-wait* argument indicates the initial wait time (in milliseconds) before generating the first LSP.
- The third argument indicates the amount of time to wait (in milliseconds) between the first and second LSP generation.
- Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the *lsp-max-wait* interval specified, so this value causes the throttling or slowing down of the LSP generation after the initial and second intervals. Once this interval is reached, the wait interval continues at this interval until the network calms down.
- After the network calms down and there are no triggers for 2 times the *lsp-max-wait* interval, fast behavior is restored (the initial wait time).

Notice that the **lsp-gen-interval** command controls the delay between LSPs being *generated*, as opposed to the following related commands:

- The **isis lsp-interval** command sets the delay (in milliseconds) between successive LSPs being *transmitted* (including LSPs generated by another system and forwarded by the local system).
- The **isis retransmit-interval** command sets the amount of time (in seconds) between retransmissions *of the same LSP* on a point-to-point link.
- The **isis retransmit-throttle-interval** command sets the minimum delay (in milliseconds) between retransmitted LSPs on a point-to-point interface.

These commands can be used in combination to control the rate of LSP packets being generated, transmitted, and retransmitted.

Examples

The following example configures intervals for SPF calculations, PRC, and LSP generation:

```
router isis
 spf-interval 5 10 20
 prc-interval 5 10 20
 lsp-gen-interval 2 50 100
```

Related Commands

Command	Description
isis lsp-interval	Sets the time delay between successive IS-IS LSP transmissions.
isis retransmit-interval	Sets the amount of time between retransmission of each IS-IS LSP on a point-to-point link.
isis retransmit-throttle-interval	Sets the minimum delay between retransmissions on each LSP on a point-to-point interface.

lsp-refresh-interval (IS-IS)

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

Syntax Description

seconds	Interval (in seconds) at which LSPs are refreshed.The range is 1 to 65535 seconds. The default value is 900 seconds (15 minutes).

Defaults

900 seconds (15 minutes)

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The refresh interval determines the rate at which Cisco IOS software periodically transmits in LSPs the route topology information that it originates. This is done to keep the database information from becoming too old.

LSPs must be periodically refreshed before their lifetimes expire. The value set for the **lsp-refresh-interval** command should be less than the value set for the **max-lsp-lifetime** command; otherwise, LSPs will time out before they are refreshed. If you misconfigure the LSP lifetime to be too low compared to the LSP refresh interval, the software will reduce the LSP refresh interval to prevent the LSPs from timing out.

Reducing the refresh interval reduces the amount of time that undetected link state database corruption can persist at the cost of increased link utilization. (This is an extremely unlikely event, however, because there are other safeguards against corruption.) Increasing the interval reduces the link utilization caused by the flooding of refreshed packets (although this utilization is very small).

Examples

The following example configures the IS-IS LSP refresh interval to be 1080 seconds (18 minutes):

```
router isis
 lsp-refresh-interval 1080
```

Related Commands

Command	Description
max-lsp-lifetime (IS-IS)	Sets the maximum time that link-state packets (LSPs) can remain in a router's database without being refreshed.

max-lsp-lifetime (IS-IS)

To set the maximum time that link-state packets (LSPs) can remain in a router's database without being refreshed, use the **max-lsp-lifetime** command in router configuration mode. To restore the default lifetime, use the **no** form of this command.

max-lsp-lifetime *seconds*

no max-lsp-lifetime

Syntax Description

seconds	Lifetime of the LSP in seconds. The range is 1 to 65535 seconds; the default is 1200 seconds (20 minutes).

Defaults

1200 seconds (20 minutes)

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

If the lifetime is exceeded before a refresh LSP arrives, the LSP is dropped from the database.

You might need to adjust the maximum LSP lifetime if you change the LSP refresh interval with the **lsp-refresh-interval** (IP) command. LSPs must be periodically refreshed before their lifetimes expire. The value set for the **lsp-refresh-interval** command should be less than the value set for the **max-lsp-lifetime** command; otherwise, LSPs will time out before they are refreshed. If you misconfigure the LSP lifetime to be too low compared to the LSP refresh interval, the software will reduce the LSP refresh interval to prevent the LSPs from timing out.

You might prefer higher values for each command in order to reduce control traffic, at the expense of holding stale LSPs from a crashed or unreachable router in the database longer (thus wasting memory) or increasing the risk of undetected bad LSPs staying active (very rare).

Examples

The following example configures an LSP lifetime of 40 minutes:

```
router isis
 max-lsp-lifetime 2400
```

Related Commands

Command	Description
lsp-refresh-interval (IS-IS)	Sets the link-state packet (LSP) refresh interval.

net

To configure an IS-IS network entity title (NET) for a Connectionless Network Service (CLNS) routing process, use the **net** command in router configuration mode. 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.

Defaults

No NET is configured and the CLNS process will not start. A NET is mandatory.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	This command was modified to include multiarea IS-IS routing.

Usage Guidelines

Under most circumstances, one and only one NET must be configured.

A NET is a network service access point (NSAP) where the last byte is always zero. On a Cisco router running IS-IS, a NET can be 8 to 20 bytes. The last byte is always the n-selector and must be zero.

The six bytes directly in front of the n-selector are the system ID. The system ID length is a fixed size and cannot be changed. The system ID must be unique throughout each area (Level 1) and throughout the backbone (Level 2).

All bytes in front of the system ID are the area ID.

Even when IS-IS is used to perform IP routing only (no CLNS routing enabled), a NET must still be configured to define the router system ID and area ID.

A maximum of three NETs per router are allowed. In rare circumstances, it is possible to configure two or three NETs. In such a case, the area this router is in will have three area addresses. There will still be only one area, but it will have an additional maximum of three area addresses.

Configuring multiple NETs can be temporarily useful in the case of network reconfiguration where multiple areas are merged, or where one area is split into additional areas. Multiple area addresses enable you to renumber an area individually as needed.

If you are configuring multiarea IS-IS, the area ID must be unique, but the system ID portion of the NET must be the same for all IS-IS routing process instances.

Examples

The following example configures a router with system ID 0000.0c11.1111.00 and area ID 47.0004.004d.0001:

```
router isis CHESNUT
 net 47.0004.004d.0001.0001.0c11.1111.00
```

The following example shows three IS-IS routing processes with three areas configured. Each area has a unique identifier, but the system ID is the same for all areas.

```
clns routing

.
.
.

interface Tunnel529
 ip address 10.0.0.5 255.255.255.0
 ip router isis BB
 clns router isis BB

interface Ethernet1
 ip address 10.1.1.5 255.255.255.0
 ip router isis A3253-01
 clns router isis A3253-01
!
interface Ethernet2
 ip address 10.2.2.5 255.255.255.0
 ip router isis A3253-02
 clns router isis A3253-02

.
.
.

router isis BB                          ! Defaults to "is-type level-1-2"
 net 49.2222.0000.0000.0005.00
!
router isis A3253-01
 net 49.0553.0001.0000.0000.0005.00
 is-type level-1
!
router isis A3253-02
 net 49.0553.0002.0000.0000.0005.00
 is-type level-1
```

Related Commands

Command	Description
is-type	Configures the routing level for an instance of the IS-IS routing process.
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

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** command in router configuration mode. 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.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

When the **partition avoidance** command is enabled, a multiarea router withdraws a Level 1 area prefix from the Level 2 backbone when it no longer has any active adjacencies to that Level 1 area. This withdrawal prevents the Level 1 area from appearing to be partitioned within the Level 2 backbone.

In International Standards Organization (ISO) CLNS networks using a redundant topology, it is possible for an area to become “partitioned” when full connectivity is lost between a Level 1-2 border router, all adjacent Level 1 routers, and end hosts. In such a case, multiple Level 1-2 border routers advertise the Level 1 area prefix into the backbone area, even though any one router can reach only a subset of the end hosts in the Level 1 area.

When enabled, the **partition avoidance** command prevents this partitioning by causing the border router to stop advertising the Level 1 area prefix into the Level 2 backbone. This command displays the output from different areas as a string or additional white space.

Other cases of connectivity loss within the Level 1 area itself are not detected or corrected by the border router, and this command will have no effect.

Examples

The following example causes the routing process named Finance to stop advertising the prefix for the area named area1 when the router no longer has any active adjacencies to area1:

```
router isis Finance
 partition avoidance area1
```

Related Commands

Command	Description
is-type	Configures the routing level for an instance of the IS-IS routing process.
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process.

prc-interval

To customize IS-IS throttling of partial route calculations (PRC), use the **prc-interval** command in router configuration mode. To restore default values, use the **no** form of this command.

prc-interval *prc-max-wait* [*prc-initial-wait prc-second-wait*]

no prc-interval

Syntax Description

prc-max-wait	Indicates the maximum interval (in seconds) between two consecutive PRC calculations. Value range is 1 to 120 seconds. The default is 5 seconds.
prc-initial-wait	(Optional) Indicates the initial PRC calculation delay (in milliseconds) after a topology change. The range is 1 to 120,000 milliseconds. The default is 2000 milliseconds.
prc-second-wait	(Optional) Indicates the hold time between the first and second PRC calculation (in milliseconds). The range is 1 to 120,000 milliseconds. The default is 5000 milliseconds (5 seconds).

Defaults

prc-max-wait: 5 seconds
prc-initial-wait: 2000 milliseconds
prc-second-wait: 5000 milliseconds

Command Modes

Router configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

PRC is the software's process of calculating routes without performing an SPF calculation. This is possible when the topology of the routing system itself has not changed, but a change is detected in the information announced by a particular IS or when it is necessary to attempt to reinstall such routes in the RIB.

The following description will help you determine whether to change the default values of this command:

- The *prc-initial-wait* argument indicates the initial wait time (in milliseconds) before generating the first LSP.
- The *prc-second-wait* argument indicates the amount of time to wait (in milliseconds) between the first and second LSP generation.
- Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the *prc-max-wait* interval specified, so this value causes the throttling or slowing down of the PRC calculation after the initial and second intervals. Once this interval is reached, the wait interval continues at this interval until the network calms down.

- After the network calms down and there are no triggers for 2 times the *prc-max-wait* interval, fast behavior is restored (the initial wait time).

Examples

The following example configures intervals for SPF calculations, PRC, and LSP generation:

```
router isis
 spf-interval 5 10 20
 prc-interval 5 10 20
 lsp-gen-interval 2 50 100
```

router isis

To enable the IS-IS routing protocol and to specify an IS-IS process, use the **router isis** command in global configuration mode. 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.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	Multiarea functionality was added, changing the way the *tag* argument (now *area-tag*) is used.

Usage Guidelines

This command is used to enable routing for an area. An appropriate network entity title (NET) must be configured to specify the area address of the area and system ID of the router. Routing must be enabled on one or more interfaces before adjacencies may be established and dynamic routing is possible.

If you have IS-IS running and at least one International Standards Organization Interior Gateway Routing Protocol (ISO-IGRP) process, the IS-IS process and the ISO-IGRP process cannot both be configured without an area tag. The null tag can be used by only one process. If you run ISO-IGRP and IS-IS, a null tag can be used for IS-IS, but not for ISO-IGRP at the same time. However, each area in an IS-IS multiarea configuration should have a nonnull area tag to facilitate identification of the area.

You can configure only one IS-IS routing process to perform Level 2 (interarea) routing. You can configure this process to perform Level 1 (intra-area) routing at the same time. You can configure up to 29 additional processes as Level 1-only processes. If Level 2 routing is configured on any process, all additional processes are automatically configured as Level 1.

An interface cannot be part of more than one area, except in the case where the associated routing process is performing both Level 1 and Level 2 routing. On media such as WAN media where subinterfaces are supported, different subinterfaces could be configured for different areas.

If Level 2 routing is not desired for a given area, use the **is-type** command to remove Level 2. Level 2 routing can then be enabled on some other router instance.

Explicit redistribution between IS-IS instances is prohibited (prevented by the parser). In other words, you cannot issue a **redistribute isis** *area-tag* command in the context of another IS-IS router instance (**router isis** *area-tag*). Redistribution from any other routing protocol into a particular area is possible, and is configured per router instance, as in Cisco IOS software Release 12.0, using the **redistribute** and **route map** commands. By default, redistribution is into Level 2.

If multiple Level 1 areas are defined, the Target Address Resolution Protocol (TARP) behaves in the following way:

- The locally assigned target identifier gets the network service access point (NSAP) of the Level 2 area, if present.
- If only Level 1 areas are configured, the router uses the NSAP of the first active Level 1 area as shown in the configuration at the time of TARP configuration ("tarp run"). (Level 1 areas are sorted alphanumerically by tag name, with capital letters coming before lowercase letters. For example, AREA-1 precedes AREA-2, which precedes area-1.) Note that the target identifier NSAP could change following a reload if a new Level 1 area is added to the configuration after TARP is running.
- The router continues to process all Type 1 and 2 protocol data units (PDUs) that are for this router. Type 1 PDUs are processed locally if the specified target identifier is in the local target identifier cache. If not, they are "propagated" (routed) to all interfaces in the *same* Level 1 area. (The same area is defined as the area configured on the input interface.)
- Type 2 PDUs are processed locally if the specified target identifier is in the local target identifier cache. If not, they are propagated via all interfaces (all Level 1 or Level 2 areas) with TARP enabled. If the source of the PDU is from a different area, the information is also added to the local target identifier cache. Type 2 PDUs are propagated via all static adjacencies.
- Type 4 PDUs (for changes originated locally) are propagated to all Level 1 and Level 2 areas (because internally they are treated as "Level 1-2").
- Type 3 and 5 PDUs continue to be routed.
- Type 1 PDUs are propagated only via Level 1 static adjacencies if the static NSAP is in one of the Level 1 areas in this router.

Examples

The following example configures IS-IS for IP routing, with system ID 0000.0000.0002 and area ID 01.0001, and enables IS-IS to form adjacencies on Ethernet interface 0 and serial interface 0. The IP prefix assigned to Ethernet interface 0 will be advertised to other IS-IS routers.

```
router isis
 net 01.0001.0000.0000.0002
 is-type level-1
!
interface ethernet 0
 ip address 10.1.1.1 255.255.255.0
 ip router isis
!
interface serial 0
 ip unnumbered ethernet0
 ip router isis
```

The following example starts IS-IS routing with the optional *area-tag* argument, where CHESNUT is the value for the *area-tag* argument:

```
router isis CHESNUT
```

The following example specifies IS-IS as an IP routing protocol for a process named Finance, and specifies that the Finance process will be routed on Ethernet interface 0 and serial interface 0:

```
router isis Finance
 net 49.0001.aaaa.aaaa.aaaa.00
interface Ethernet 0
 ip router isis Finance
interface serial 0
 ip router isis Finance
```

Related Commands

Command	Description
clns router isis	Enables IS-IS routing for ISO CLNS on an interface and attaches an area designator to the routing process.
ip router isis	Configures an IS-IS routing process for IP on an interface and attaches an area designator to the routing process.
net	Configures an IS-IS NET for the routing process.
redistribute (IP)	Redistribute routes from one routing domain into another routing domain.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.

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** command in router configuration mode. To remove the designation, use the **no** form of this command.

set-overload-bit [**on-startup** {*seconds* | **wait-for-bgp**}] [**suppress** {[**interlevel**] [**external**]}]

no set-overload-bit

Syntax Description

on-startup	(Optional) Sets the overload bit upon the system starting up. The overload bit remains set for the number of *seconds* configured or until BGP has converged, depending on the subsequent argument or keyword specified.
seconds	(Optional) When the **on-startup** keyword is configured, causes the overload bit to be set upon system startup and remain set for this number of seconds.
wait-for-bgp	(Optional) When the **on-startup** keyword is configured, causes the overload bit to be set upon system startup and remain set until BGP has converged. If BGP does not signal IS-IS that it is converged, IS-IS will turn off the overload bit after 10 minutes.
suppress	(Optional) Causes the type of prefix identified by the subsequent keyword or keywords to be suppressed.
interlevel	(Optional) When the **suppress** keyword is configured, prevents the IP prefixes learned from another IS-IS level from being advertised.
external	(Optional) When the **suppress** keyword is configured, prevents the IP prefixes learned from other protocols from being advertised.

Defaults

The overload bit is not set.

Command Modes

Router configuration

Command History

Release	Modification
11.2	This command was introduced.
11.3(2)	The **on-startup** keyword and the *seconds* argument were added.
12.0(7)S	The **wait-for-bgp** keyword was added.
12.1(9)	The **wait-for-bgp** keyword was added.
12.2(2)	The **wait-for-bgp** keyword was added.
12.0(21)ST	The **suppress**, **interlevel**, and **external** keywords were added.
12.2(8)	The **suppress**, **interlevel**, and **external** keywords were added.

Usage Guidelines

This command forces the router to set the overload bit (also known as the hippity bit) in its nonpseudonode link-state packets (LSPs). Normally, the setting of the overload bit is allowed only when a router runs into problems. For example, when a router is experiencing a memory shortage, it might be that the link-state database is not complete, resulting in an incomplete or inaccurate routing table. By setting the overload bit in its LSPs, other routers can ignore the unreliable router in their SPF calculations until the router has recovered from its problems.

The result will be that no paths through this router are seen by other routers in the IS-IS area. However, IP and Connectionless Network Service (CLNS) prefixes directly connected to this router will still be reachable.

This command can be useful when you want to connect a router to an IS-IS network but do not want real traffic flowing through it under any circumstances. Examples situations are as follows:

- A test router in the lab, connected to a production network.
- A router configured as an LSP flooding server, for example, on a nonbroadcast multiaccess (NBMA) network, in combination with the mesh group feature.
- A router that is aggregating virtual circuits (VCs) used only for network management. In this case, the network management stations must be on a network directly connected to the router with the **set-overload-bit** command configured.

Unless you specify the **on-startup** keyword, this command sets the overload bit immediately.

In addition to setting the overload bit, you might want to suppress certain types of IP prefix advertisements from LSPs. For example, allowing IP prefix propagation between Level 1 and Level 2 effectively makes a node a transit node for IP traffic, which might be undesirable. The **suppress** keyword used with the **interlevel** or **external** keyword (or both) accomplishes that suppression while the overload bit is set.

Examples

The following example sets the overload bit upon startup and until BGP has converged, and suppresses redistribution between IS-IS levels and suppresses redistribution from external routing protocols while the overload bit is set:

```
interface Ethernet0
 ip address 10.1.1.1 255.255.255.0
 ip router isis
router isis
 net 49.0001.0000.0000.0001.00
 set-overload-bit on-startup wait-for-bgp suppress interlevel external
router bgp 100
```

show isis database

To display the IS-IS link-state database, use the **show isis database** command in EXEC mode.

show isis *area-tag* **database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**]

Syntax Description

area-tag	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.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Each of the options for this command can be entered in an arbitrary string within the same command entry. For example, the following are both valid command specifications and provide the same output: **show isis database detail l2** and **show isis database l2 detail**.

Examples

The following is sample output from the **show isis database** command when it is specified with no options or as **show isis database l1 l2**:

```
Router# show isis database

IS-IS Level-1 Link State Database
LSPID                 LSP Seq Num    LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.0C35.00-00  0x0000000C     0x5696        792           0/0/0
0000.0C00.40AF.00-00* 0x00000009     0x8452        1077          1/0/0
0000.0C00.62E6.00-00  0x0000000A     0x38E7        383           0/0/0
0000.0C00.62E6.03-00  0x00000006     0x82BC        384           0/0/0
0800.2B16.24EA.00-00  0x00001D9F     0x8864        1188          1/0/0
0800.2B16.24EA.01-00  0x00001E36     0x0935        1198          1/0/0

IS-IS Level-2 Link State Database
LSPID                 LSP Seq Num    LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.0C35.03-00  0x00000005     0x04C8        792           0/0/0
0000.0C00.3E51.00-00  0x00000007     0xAF96        758           0/0/0
0000.0C00.40AF.00-00* 0x0000000A     0x3AA9        1077          0/0/0
```

Table 25 describes the significant fields shown in the display.

Table 25 show isis database Field Descriptions

Field	Description
LSPID	The LSP identifier. The first six octets form the system ID of the router that originated the LSP. The next octet is the pseudonode ID. When this byte is zero, the LSP describes links from the system. When it is nonzero, the LSP is a so-called nonpseudonode LSP. This is similar to a router link-state advertisement (LSA) in Open Shortest Path First (OSPF). The LSP will describe the state of the originating router. For each LAN, the designated router for that LAN will create and flood a pseudonode LSP, describing all systems attached to that LAN. The last octet is the LSP number. If there is more data than can fit in a single LSP, the LSP will be divided into multiple LSP fragments. Each fragment will have a different LSP number. An asterisk (*) indicates that the LSP was originated by the system on which this command is issued.
LSP Seq Num	Sequence number for the LSP that allows other systems to determine if they have received the latest information from the source.
LSP Checksum	Checksum of the entire LSP packet.
LSP Holdtime	Amount of time the LSP remains valid (in seconds). An LSP hold time of zero indicates that this LSP was purged and is being removed from the link-state database (LSDB) of all routers. The value indicates how long the purged LSP will stay in the LSDB before being completely removed.
ATT	The Attach bit. This indicates that the router is also a Level 2 router, and it can reach other areas. Level 1-only routers and Level 1-2 routers that have lost connection to other Level 2 routers will use the attach bit to find the closest Level 2 router. They will point a default route to the closest Level 2 router.

Table 25 show isis database Field Descriptions (continued)

Field	Description
P	The P bit. Detects if the IS is area partition repair capable. Cisco and other vendors do not support area partition repair.
OL	The Overload bit. Determines if the IS is congested. If the Overload bit is set, other routers will not use this system as a transit router when calculating routers. Only packets for destinations directly connected to the overloaded router will be sent to this router.

The following is sample output from the **show isis database detail** command:

```
Router# show isis database detail

IS-IS Level-1 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.0C35.00-00  0x0000000C   0x5696        325           0/0/0
  Area Address: 47.0004.004D.0001
  Area Address: 39.0001
  Metric: 10   IS 0000.0C00.62E6.03
  Metric: 0    ES 0000.0C00.0C35
 --More--
0000.0C00.40AF.00-00* 0x00000009   0x8452        608           1/0/0
  Area Address: 47.0004.004D.0001
  Metric: 10   IS 0800.2B16.24EA.01
  Metric: 10   IS 0000.0C00.62E6.03
  Metric: 0    ES 0000.0C00.40AF

IS-IS Level-2 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.0C35.03-00  0x00000005   0x04C8        317           0/0/0
  Metric: 0    IS 0000.0C00.0C35.00
 --More--
0000.0C00.3E51.00-00  0x00000009   0xAB98        1182          0/0/0
  Area Address: 39.0004
  Metric: 10   IS 0000.0C00.40AF.00
  Metric: 10   IS 0000.0C00.3E51.05
```

As the output shows, in addition to the information displayed with the **show isis database** command, the **show isis database detail** command displays the contents of each LSP.

Table 26 describes the significant fields shown in the display.

Table 26 show isis database detail Field Descriptions

Field	Description
Area Address:	Reachable area addresses from the router. For Level 1 LSPs, these are the area addresses configured manually on the originating router. For Level 2 LSPs, these are all the area addresses for the area to which this route belongs.
Metric:	IS-IS metric for the cost of the adjacency between the originating router and the advertised neighbor, or the metric of the cost to get from the advertising router to the advertised destination (which can be an IP address, an end system [ES], or a CLNS prefix).

The following is additional sample output from the **show isis database detail** command.This is a Level 2 LSP. The area address 39.0001 is the address of the area in which the router resides.

```
Router# show isis database detail l2

IS-IS Level-2 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.1111.00-00* 0x00000006   0x4DB3        1194          0/0/0
  Area Address: 39.0001
  NLPID:        0x81 0xCC
  IP Address:  160.89.64.17
  Metric: 10   IS 0000.0C00.1111.09
  Metric: 10   IS 0000.0C00.1111.08
  Metric: 10   IP 172.16.65.0 255.255.255.0
  Metric: 10   IP 172.16.64.0 255.255.255.0
  Metric: 0    IP-External 10.0.0.0 255.0.0.0
```

Table 27 describes the significant field shown in the display.

Table 27 show isis database detail Field Descriptions Displaying IP Addresses

Field	Description
Various addresses	The IP entries are the directly connected IP subnets the router is advertising (with associated metrics). The IP-External entry is a redistribute route.

show isis lsp-log

To display the Level 1 and Level 2 Intermediate System-to-Intermediate System (IS-IS) link-state packet (LSP) log of the interfaces that triggered the new LSP, use the **show isis lsp-log** command in EXEC mode.

show isis lsp-log

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0	This command was introduced.

Examples

The following is sample output from the **show isis lsp-log** command:

```
Router# show isis lsp-log

   Level 1 LSP log
  When        Count      Interface   Triggers
07:05:18        3                    CONFIG NEWADJ DIS
07:05:13        2        Ethernet0   NEWADJ DIS
07:04:43        1                    ATTACHFLAG
07:01:38        2        Ethernet0   IPUP
07:01:33        2        Loopback0   CONFIG
07:01:24        1        Ethernet0   DELADJ
07:01:17        2        Ethernet0   DIS ES
07:01:02        1        Ethernet0   NEWADJ
07:00:57        2        Ethernet0   NEWADJ DIS


   Level 2 LSP log
  When        Count      Interface   Triggers
07:05:24        2                    CONFIG NEWADJ
07:05:23        1        Ethernet0   NEWADJ
07:05:18        1        Ethernet0   DIS
07:05:00        1          Serial0   NEWADJ
07:01:44        2        Ethernet0   IPUP
07:01:39        3        Loopback0   CONFIG DELADJ
07:01:30        1        Ethernet0   DELADJ
07:01:25        1          Serial0   NEWADJ
07:00:56        1                    IPIA
07:00:47        2                    AREASET IPIA
```

Table 28 describes the fields shown in the display.

Table 28 show isis lsp-log Field Descriptions

Field	Description
When	Time elapsed since the LSP was generated.
Count	Number of events that took place at this time.
Interface	Interface that caused the LSP regeneration.
Triggers	Event that triggered the LSP to be flooded. Possible triggers for an LSP are as follows: • AREASET—Active area set changed. • ATTACHFLAG—Attached bit changed state. • CLEAR—Some form of manual **clear** command was issued. • CONFIG—Any configuration change. • DELADJ—Adjacency went down. • DIS—DIS changed or pseudonode changed. • ES—End System adjacency changed. • HIPPITY—LSPDB overload bit changed state. • IF_DOWN—Needs a new LSP. • IP_DEF_ORIG—Default information originate changed. • IPDOWN—Directly connected IP prefix down. • IP_EXTERNAL—Redistributed IP route appeared or gone. • IPIA—Interarea IP route appeared or gone. • IPUP—Directly connected IP prefix up. • NEWADJ—New adjacency came up. • REDIST—Redistributed level-2 CLNS route changed. • RRR_INFO—RRR bandwidth resource information.

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 command in EXEC mode.

show isis *area-tag* **spf-log**

Syntax Description

area-tag	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.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show isis spf-log** command:

```
Router# show isis spf-log

                   Level 1 SPF log
When   Duration  Nodes  Count     Last trigger LSP   Triggers
00:15:46    3124     40      1          milles.00-00  TLVCODE
00:15:24    3216     41      5          milles.00-00  TLVCODE NEWLSP
00:15:19    3096     41      1          deurze.00-00  TLVCODE
00:14:54    3004     41      2          milles.00-00  ATTACHFLAG LSPHEADER
00:14:49    3384     41      1          milles.00-01  TLVCODE
00:14:23    2932     41      3          milles.00-00  TLVCODE
00:05:18    3140     41      1                        PERIODIC
00:03:54    3144     41      1          milles.01-00  TLVCODE
00:03:49    2908     41      1          milles.01-00  TLVCODE
00:03:28    3148     41      3           bakel.00-00  TLVCODE TLVCONTENT
00:03:15    3054     41      1          milles.00-00  TLVCODE
00:02:53    2958     41      1          mortel.00-00  TLVCODE
00:02:48    3632     41      2          milles.00-00  NEWADJ TLVCODE
00:02:23    2988     41      1          milles.00-01  TLVCODE
00:02:18    3016     41      1          gemert.00-00  TLVCODE
00:02:14    2932     41      1           bakel.00-00  TLVCONTENT
00:02:09    2988     41      2           bakel.00-00  TLVCONTENT
00:01:54    3228     41      1          milles.00-00  TLVCODE
00:01:38    3120     41      3            rips.03-00  TLVCONTENT
```

Table 29 describes the significant fields shown in the display.

Table 29 show isis spf-log Field Descriptions

Field	Description
When	How long ago (in hours: minutes: seconds) a full SPF calculation occurred. The last 20 occurrences are logged.
Duration	Number of milliseconds required to complete this SPF run. Elapsed time is wall clock time, not CPU time.
Nodes	Number of routers and pseudonodes (LANs) that make up the topology calculated in this SPF run.
Count	Number of events that triggered this SPF run. When there is a topology change, often multiple link-state packets (LSPs) are received in a short time. A router waits 5 seconds before running a full SPF run, so it can include all new information. This count denotes the number of events (such as receiving new LSPs) that occurred while the router was waiting its 5 seconds before running full SPF.
Last trigger LSP	Whenever a full SPF calculation is triggered by the arrival of a new LSP, the router stores the LSP ID. The LSP ID can provide a clue as to the source of routing instability in an area. If multiple LSPs are causing an SPF run, only the LSP ID of the last received LSP is remembered.
Triggers	A list of all reasons that triggered a full SPF calculation. For a list of possible triggers, see Table 30.

Table 30 lists possible triggers of a full SPF calculation.

Table 30 Possible Triggers of Full SPF Calculation

Trigger	Description
ATTACHFLAG	This router is now attached to the Level 2 backbone or it has just lost contact to the Level 2 backbone.
ADMINDIST	Another administrative distance was configured for the IS-IS process on this router.
AREASET	Set of learned area addresses in this area changed.
BACKUPOVFL	An IP prefix disappeared. The router knows there is another way to reach that prefix but has not stored that backup route. The only way to find the alternative route is through a full SPF run.
DBCHANGED	A **clear isis *** command was issued on this router.
IPBACKUP	An IP route disappeared, which was not learned via IS-IS, but via another protocol with better administrative distance. IS-IS will run a full SPF to install an IS-IS route for the disappeared IP prefix.
IPQUERY	A **clear ip route** command was issued on this router.
LSPEXPIRED	Some LSP in the link-state database (LSDB) has expired.
LSPHEADER	ATT/P/OL bits or is-type in an LSP header changed.
NEWADJ	This router has created a new adjacency to another router.
NEWAREA	A new area (via NET) was configured on this router.

Table 30 Possible Triggers of Full SPF Calculation (continued)

Trigger	Description
NEWLEVEL	A new level (via is-type) was configured on this router.
NEWLSP	A new router or pseudonode appeared in the topology.
NEWMETRIC	A new metric was configured on an interface of this router.
NEWSYSID	A new system ID (via network entity title (NET)) was configured on this router.
PERIODIC	Typically, every 15 minutes a router runs a periodic full SPF calculation.
RTCLEARED	A **clear clns route** command was issued on this router.
TLVCODE	TLV code mismatch, indicating that different TLVs are included in the newest version of an LSP.
TLVCONTENT	TLV contents changed. This normally indicates that an adjacency somewhere in the area has come up or gone down. Look at the "Last trigger LSP" column to get an indication of where the instability may have occurred.

show isis topology

To display a list of all connected routers in all areas, use the **show isis topology** command in EXEC mode.

show isis *area-tag* **topology** [**level-1**] [**level-2**] [*host-nsap*]

Syntax Description

area-tag	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) Paths to all Level 1 routers in the area or areas in which this router resides. The abbreviated keyword **l1** may be used in place of **level-1**.
level-2	(Optional) Paths to all Level 2 routers in the domain. The abbreviated keyword **l2** may be used in place of **level-2**.
host-nsap	(Optional) Host name or network service access point (NSAP) of a router for which you would like to check reachability.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.1	The **level-1** and **level-2** keywords and the *host-nsap* argument were added.

Usage Guidelines

Use the **show isis topology** EXEC command to verify the presence and connectivity between all routers in all areas.

Examples

The following is sample output from the **show isis topology** command:

```
Router# show isis topology

IS-IS paths to level-1 routers
System Id       Metric  Next-Hop        Interface       SNPA
Router_A        --
Router_B        10      Router_B        Et0             00e0.b064.46ec
```

```
IS-IS paths to level-2 routers
System Id       Metric  Next-Hop        Interface       SNPA
Router_A        --
Router_B        10      Router_B        Et0             00e0.b064.46ec
Router_C        20      Router_B        Et0             00e0.b064.46ec
                        Router_D        Se0             DLCI 100
                        Router_D        Se1             *HDLC*
Router_D        10      Router_D        Se0             DLCI 100
                        Router_D        Se1             *HDLC*
```

Table 31 describes the fields shown in the display.

Table 31 show isis topology Field Descriptions

Field	Description
System Id	Identification value of the system listed in the Level 1 or Level 2 forwarding table.
Metric	IS-IS metric for the route.
Next-Hop	System ID of best-cost next-hop to listed address.
Interface	Interface through which the next-hop system is known.
SNPA	Subnetwork point of attachment (MAC address) of next-hop.

Related Commands

Command	Description
show clns es-neighbors	Lists the ES neighbors that this router knows.
show clns is-neighbors	Displays IS-IS related information for IS-IS router adjacencies.
show clns neighbors	Displays both ES and IS neighbors.
show clns neighbor areas	Displays information about IS-IS neighbors and the areas to which they belong.
show clns route	Displays one or all of the destinations to which the router knows how to route CLNS packets.

spf-interval

To customize IS-IS throttling of shortest path first (SPF) calculations, use the **spf-interval** command in router configuration mode. To restore default values, use the **no** form of this command.

spf-interval [level-1 | level-2] *spf-max-wait* [*spf-initial-wait spf-second-wait*]

no spf-interval

Syntax Description

level-1	(Optional) Apply intervals to Level-1 areas only.
level-2	(Optional) Apply intervals to Level-2 areas only.
spf-max-wait	Indicates the maximum interval (in seconds) between two consecutive SPF calculations. The range is 1 to 120 seconds. The default is 10 seconds.
spf-initial-wait	(Optional) Indicates the initial SPF calculation delay (in milliseconds) after a topology change. The range is 1 to 120,000 milliseconds. The default is 5500 milliseconds (5.5 seconds).
spf-second-wait	(Optional) Indicates the hold time between the first and second SPF calculation (in milliseconds). The range is 1 to 120,000 milliseconds. The default is 5500 milliseconds (5.5 seconds).

Defaults

spf-max-wait: 10 seconds
spf-initial-wait: 5500 milliseconds
spf-second-wait: 5500 milliseconds

Command Modes

Router configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

The following description will help you determine whether to change the default values of this command:

- The *spf-initial-wait* argument indicates the initial wait time (in milliseconds) before the first SPF calculation.
- The *spf-second-wait* argument indicates the amount of time to wait (in milliseconds) between the first and second SPF calculation.
- Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the *spf-max-wait* interval specified, so this value causes the throttling or slowing down of the SPF calculations after the initial and second intervals. Once this interval is reached, the wait interval continues at this interval until the network calms down.
- After the network calms down and there are no triggers for 2 times the *spf-max-wait* interval, fast behavior is restored (the initial wait time).

SPF throttling is not a dampening mechanism; that is, SPF throttling does not prevent SPF calculations or mark any route, interface, or router as down. SPF throttling simply increases the intervals between SPF calculations.

Examples

The following example configures intervals for SPF calculations, PRC, and LSP generation:

```
router isis
 spf-interval 5 10 20
 prc-interval 5 10 20
 lsp-gen-interval 2 50 100
```

summary-address (IS-IS)

To create aggregate addresses for IS-IS or Open Shortest Path First (OSPF), use the **summary-address** command in router configuration mode. To restore the default, use the **no** form of this command.

summary-address *address mask* {**level-1** | **level-1-2** | **level-2**}

no summary-address *address mask* {**level-1** | **level-1-2** | **level-2**}

Syntax Description

address	Summary address designated for a range of addresses.
mask	IP subnet mask used for the summary route.
level-1	Only routes redistributed into Level 1 are summarized with the configured address and 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 advertises Level 1 routes as reachable in its area.
level-2	Routes learned by Level 1 routing are summarized into the Level 2 backbone with the configured address and mask value. Redistributed routes into Level 2 IS-IS will be summarized also.

Defaults

All redistributed routes are advertised individually.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Multiple groups of addresses can be summarized for a given level. Routes learned from other routing protocols can also be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. This command helps reduce the size of the routing table.

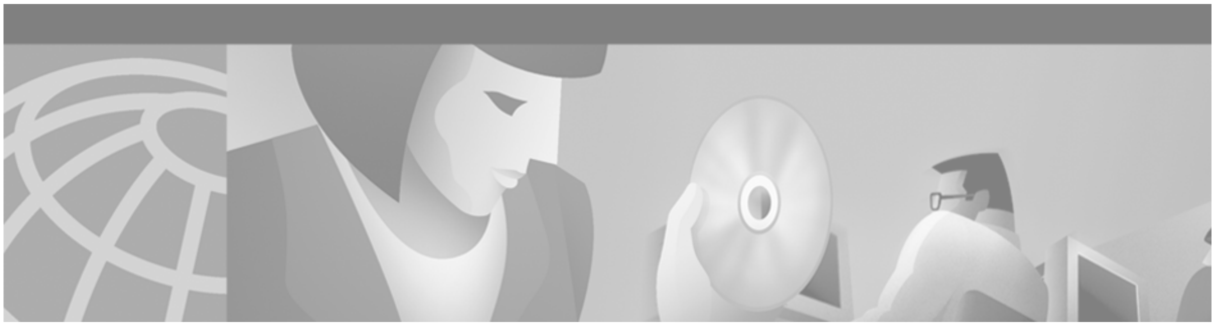
This command also reduces the size of the link-state packets (LSPs) and thus the link-state database (LSDB). It also helps stability because a summary advertisement is depending on many more specific routes. A single route flap does not cause the summary advertisement to flap in most cases.

The drawback of summary addresses is that other routes might have less information to calculate the most optimal routing table for all individual destinations.

Examples

The following example redistributes Routing Information Protocol (RIP) routes into IS-IS. In a RIP network, there are IP routes for 10.1.1, 10.1.2, 10.1.3, 10.1.4, and so on. This example advertises only 10.1.0.0 into the IS-IS Level 1 link-state PDU.

```
router isis
net 01.0000.0000.0001.00
redistribute rip level-1 metric 40
summary-address 10.1.0.0 255.255.0.0 level-1
```



BGP Commands

Use the commands in this chapter to configure and monitor Border Gateway Protocol (BGP). For BGP configuration information and examples, refer to the "Configuring BGP" chapter of the *Cisco IOS IP Configuration Guide*. For multiprotocol BGP configuration information and examples, refer to the "Configuring Multiprotocol BGP Extensions for IP Multicast" chapter of the *Cisco IOS IP Configuration Guide*. For multiprotocol BGP command descriptions, refer to the "Multiprotocol BGP Extensions for IP Multicast Commands" chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*.

aggregate-address

To create an aggregate entry in a Border Gateway Protocol (BGP) or multiprotocol 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

address	Aggregate address.
mask	Aggregate mask.
as-set	(Optional) Generates autonomous system set path information.
summary-only	(Optional) Filters all more-specific routes from updates.
suppress-map *map-name*	(Optional) Name of the route map used to select the routes to be suppressed.
advertise-map *map-name*	(Optional) Name of the route map used to select the routes to create AS_SET origin communities.
attribute-map *map-name*	(Optional) Name of the route map used to set the attribute of the aggregate route.

Defaults

This command is disabled by default.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.1(20)CC	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were added.
12.0(2)S	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were added.
12.0(7)T	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were removed. Address family configuration mode was added.

Usage Guidelines

You can implement aggregate routing in BGP and multiprotocol BGP either by redistributing an aggregate route into BGP or multiprotocol BGP, or by using this conditional aggregate routing feature.

Using the **aggregate-address** command with no keywords will create an aggregate entry in the BGP or multiprotocol BGP routing table if any more-specific BGP or multiprotocol BGP routes are available that fall in the specified range. The aggregate route will be advertised as coming from your autonomous system and will have the atomic aggregate attribute set to show that information might be missing. (By default, the atomic aggregate attribute is set unless you specify the **as-set** keyword.)

Using the **as-set** keyword creates an aggregate entry using the same rules that the command follows without this keyword, but the path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized. Do not use this form of the **aggregate-address** command when aggregating many paths, because this route must be continually withdrawn and reupdated as autonomous system path reachability information for the summarized routes changes.

Using the **summary-only** keyword not only creates the aggregate route (for example, 193.*.*.*) but also suppresses advertisements of more-specific routes to all neighbors. If you want to suppress only advertisements to certain neighbors, you may use the **neighbor distribute-list** command, with caution. If a more-specific route leaks out, all BGP or multiprotocol BGP routers will prefer that route over the less-specific aggregate you are generating (using longest-match routing).

Using the **suppress-map** keyword creates the aggregate route but suppresses advertisement of specified routes. You can use the **match** clauses of route maps to selectively suppress some more-specific routes of the aggregate and leave others unsuppressed. IP access lists and autonomous system path access lists match clauses are supported.

Using the **advertise-map** keyword selects specific routes that will be used to build different components of the aggregate route, such as AS_SET or community. This form of the **aggregate-address** command is useful when the components of an aggregate are in separate autonomous systems and you want to create an aggregate with AS_SET, and advertise it back to some of the same autonomous systems. You must remember to omit the specific autonomous system numbers from the AS_SET to prevent the aggregate from being dropped by the BGP loop detection mechanism at the receiving router. IP access lists and autonomous system path access lists **match** clauses are supported.

Using the **attribute-map** keyword allows attributes of the aggregate route to be changed. This form of the **aggregate-address** command is useful when one of the routes forming the AS_SET is configured with an attribute such as the community no-export attribute, which would prevent the aggregate route from being exported. An attribute map route map can be created to change the aggregate attributes.

Examples

In the following example, a BGP aggregate address is created in router configuration mode. The path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized.

```
router bgp 65000
aggregate-address 10.0.0.0 255.0.0.0 as-set
```

In the following example, a multiprotocol BGP aggregate address is created in address family configuration mode and applied to the multicast database only using an IP Version 4 address family. More-specific routes are filtered from updates.

```
router bgp 65000
address-family ipv4 multicast
aggregate-address 10.0.0.0 255.0.0.0 summary-only
```

In the following example, a route map called map-one is created matching on an as-path access list. The path advertised for this route will be an AS_SET consisting of elements contained in paths that are matched in the route map.

```
ip as-path access-list 1 deny ^1234_
ip as-path access-list 1 permit .*
!
route-map map-one
match ip as-path 1
!
router bgp 65000
aggregate-address 10.0.0.0 255.0.0.0 as-set advertise-map map-one
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
neighbor distribute-list	Distribute BGP neighbor information in an access list.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

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.

Defaults

The behavior of this command is enabled by default (the software summarizes subprefixes to the classful network boundary when crossing classful network boundaries).

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

Route summarization reduces the amount of routing information in the routing tables.

By default, BGP does not accept subnets redistributed from Interior Gateway Protocol (IGP). To advertise and carry subnet routes in BGP, use an explicit **network** command or the **no auto-summary** command. If you disable automatic summarization and have not entered a **network** command, you will not advertise network routes for networks with subnet routes unless they contain a summary route.

Examples

In the following router configuration mode example, network numbers are not summarized automatically:

```
router bgp 6
 no auto-summary
```

In the following address family configuration mode example, network numbers are not summarized automatically:

```
router bgp 6
address-family ipv4 unicast
 no auto-summary
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.

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** command in router configuration mode. 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.

Defaults

The Cisco IOS software does not compare MEDs for paths from neighbors in different autonomous systems.

Command Modes

Router configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

The MED is one of the parameters that is considered when selecting the best path among many alternative paths. The path with a lower MED is preferred over a path with a higher MED.

By default, during the best-path selection process, MED comparison is done only among paths from the same autonomous system. This command changes the default behavior by allowing comparison of MEDs among paths regardless of the autonomous system from which the paths are received.

Examples

The following example configures the BGP speaker in autonomous system 109 to compare MEDs among alternative paths, regardless of the autonomous system from which the paths are received:

```
router bgp 109
 bgp always-compare-med
```

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** command in router configuration mode. 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.

Defaults

The router considers as-path in choosing a route.

Command Modes

Router configuration

Command History

Release	Modification
12.0	This command was introduced.

Examples

The following example prevents the BGP router from considering as-path as a factor in choosing a route:

```
router bgp 210
 bgp bestpath as-path ignore
```

Related Commands

Command	Description
show ip bgp ipv4	Displays information about the TCP and BGP connections to neighbors.

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.

Defaults

Border Gateway Protocol (BGP) does not compare similar paths received from eBGP peers during the best path selection process and switch the best path to the route with the lowest router ID.

Command Modes

Router configuration

Command History

Release	Modification
12.0	This command was introduced.
12.0 S	This command was introduced.
12.0 ST	This command was introduced.

Usage Guidelines

By default, during the best path selection process, when BGP receives similar routes from eBGP peers (all the attributes are the same except for the router ID), the best path is not switched to the route with the lowest router ID if that route was not the first route received. If the **bgp bestpath compare-routerid** command is enabled, then similar routes are compared and the best path is switched to the route with the lowest router ID.

Examples

The following example shows the BGP speaker in autonomous system 500 configured to compare the router IDs of similar paths, regardless of the autonomous system from which the paths are received:

```
router bgp 500
 bgp bestpath compare-routerid
```

Related Commands

Command	Description
show ip bgp	Displays entries in the BGP routing table.

bgp bestpath med confed

To enable Multi Exit Discriminator (MED) comparison among paths learned from confederation peers, use the **bgp bestpath med confed** command in router configuration mode. 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.

Defaults

The software does not consider the MED attribute when choosing among paths learned from confederation peers.

Command Modes

Router configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The comparison between MEDs is made only if no external autonomous systems are in the path (an external autonomous system is an autonomous system that is not within the confederation). If an external autonomous system in the path, then the external MED is passed transparently through the confederation, and the comparison is not made.

For example, assume that autonomous system 65000, 65001, 65002, and 65004 are part of the confederation; autonomous system 1 is not; and we are comparing route A with four paths. If the **bgp bestpath med confed** command is enabled, path 1 would be chosen. The fourth path has a lower MED, but it is not involved in the MED comparison because there is an external autonomous system in this path. The following list displays the MED for each autonomous system.

path = 65000 65004, med = 2

path = 65001 65004, med = 3

path = 65002 65004, med = 4

path = 65003 1, med = 1

Examples

The following command enables the BGP router to compare MED values for paths learned from confederation peers:

```
router bgp 210
 bgp bestpath med confed
```

Related Commands

Command	Description
show ip bgp	Displays entries in the BGP routing table.
show ip bgp ipv4	Displays information about the TCP and BGP connections to neighbors.

bgp bestpath med missing-as-worst

To have Cisco IOS software consider a missing Multi 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** command in router configuration mode. 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.

Defaults

The software assigns a value of 0 to the missing MED, causing the path with the missing MED attribute to be considered the best path.

Command Modes

Router configuration

Command History

Release	Modification
12.0	This command was introduced.

Examples

The following example specifies the BGP router to consider a missing MED attribute in a path as having a value of infinity, making this path the least desirable path:

```
router bgp 210
 bgp bestpath med missing-as-worst
```

Related Commands

Command	Description
show ip bgp	Displays entries in the BGP routing table.
show ip bgp ipv4	Displays information about the TCP and BGP connections to neighbors.

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.

Defaults

When a route reflector is configured, the route reflector reflects routes from a client to other clients.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
11.1	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

By default, the clients of a route reflector are not required to be fully meshed and the routes from a client are reflected to other clients. However, if the clients are fully meshed, route reflection is not required. Use the **no bgp client-to-client reflection** command to disable client-to-client reflection.

Examples

In the following router configuration mode example, the local router is a route reflector. The three neighbors are fully meshed, so client-to-client reflection is disabled.

```
router bgp 5
 neighbor 10.24.95.22 route-reflector-client
 neighbor 10.24.95.23 route-reflector-client
 neighbor 10.24.95.24 route-reflector-client
 no bgp client-to-client reflection
```

In the following address family configuration mode example, the local router is a route reflector. The three neighbors are fully meshed, so client-to-client reflection is disabled.

```
router bgp 5
address-family ipv4 unicast
 neighbor 10.24.95.22 route-reflector-client
 neighbor 10.24.95.23 route-reflector-client
 neighbor 10.24.95.24 route-reflector-client
 no bgp client-to-client reflection
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
bgp cluster-id	Configures the cluster ID if the BGP cluster has more than one route reflector.
neighbor route-reflector-client	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
show ip bgp	Displays entries in the BGP routing table.

bgp cluster-id

To configure the cluster ID if the BGP cluster has more than one route reflector, use the **bgp cluster-id** command in router configuration mode. 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.

Defaults

The router ID of the single route reflector in a cluster

Command Modes

Router configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Together, a route reflector and its clients form a *cluster*.

Usually a cluster of clients will have a single route reflector. In that case, the cluster is identified by the router ID of the route reflector. In order to increase redundancy and avoid a single point of failure, a cluster might have more than one route reflector. In this case, all route reflectors in the cluster must be configured with the 4-byte cluster ID so that a route reflector can recognize updates from route reflectors in the same cluster.

If the cluster has more than one route reflector, use this command to configure the cluster ID.

Examples

In the following example, the local router is one of the route reflectors serving the cluster. It is configured with the cluster ID to identify the cluster.

```
router bgp 5
 neighbor 198.92.70.24 route-reflector-client
 bgp cluster-id 50000
```

Related Commands

Command	Description
bgp client-to-client reflection	Restores route reflection from a BGP route reflector to clients.
neighbor route-reflector-client	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
show ip bgp	Displays entries in the BGP routing table.

bgp confederation identifier

To specify a BGP confederation identifier, use the **bgp confederation identifier** command in router configuration mode. 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.

Defaults

No confederation identifier is configured.

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

One way to reduce the internal BGP (iBGP) mesh is to divide an autonomous system into multiple autonomous systems and group them into a single confederation. Each autonomous system is fully meshed within itself and has a few connections to another autonomous system in the same confederation. Even though the peers in different autonomous systems have external BGP (eBGP) sessions, they exchange routing information as if they are iBGP peers. Specifically, the next hop, Multi Exit Discriminator (MED), and local preference information is preserved. The preservation of this information enables to you to retain a single Interior Gateway Protocol (IGP) for all the autonomous systems. To the outside world, the confederation looks like a single autonomous system.

Examples

In the following example, the autonomous system is divided into autonomous systems 4001, 4002, 4003, 4004, 4005, 4006, and 4007 and identified by the confederation identifier 5. Neighbor 10.2.3.4 is someone inside your routing domain confederation. Neighbor 10.4.5.6 is someone outside your routing domain confederation. To the outside world, there appears to be a single autonomous system with the number 5.

```
router bgp 4001
 bgp confederation identifier 5
 bgp confederation peers 4002 4003 4004 4005 4006 4007
 neighbor 10.2.3.4 remote-as 4002
 neighbor 10.4.5.6 remote-as 510
```

Related Commands

Command	Description
bgp confederation peers	Configures the autonomous systems that belong to the confederation.

bgp confederation peers

To configure the autonomous systems that belong to the confederation, use the **bgp confederation peers** command in router configuration mode. 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

as-number	Autonomous system numbers for BGP peers that will belong to the confederation.

Defaults

No BGP peers are identified as belonging to the confederation.

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *as-number* argument.

The autonomous systems specified in this command are visible internally to a confederation. Each autonomous system is fully meshed within itself. The **bgp confederation identifier** command specifies the confederation to which the autonomous systems belong.

Examples

The following example specifies that autonomous systems 1090, 1091, 1092, and 1093 belong to a single confederation:

```
router bgp 1090
 bgp confederation peers 1091 1092 1093
```

Related Commands

Command	Description
bgp confederation identifier	Specifies a BGP confederation identifier.

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

half-life	(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.
reuse	(Optional) Reuse values based on accumulated penalties. 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.
suppress	(Optional) A route is suppressed when its penalty exceeds this limit. The range is from 1 to 20000; the default is 2000.
max-suppress-time	(Optional) Maximum time (in minutes) a route can be suppressed. The range is from 1 to 20000; the default is 4 times the *half-life*. If the *half-life* value is allowed to default, the maximum suppress time defaults to 60 minutes. When the *max-suppress-time* is configured, the maximum penalty will never be exceeded, regardless of the number of times that the prefix dampens. The maximum penalty is computed with the following formula: Max penalty = reuse-limit *2^(maximum suppress time/half time)
route-map *map-name*	(Optional) Name of route map that controls where BGP route dampening is enabled.

Defaults

This command is disabled by default

half-life: 15 minutes

reuse: 750

suppress: 2000

max-suppress-time: 4 times *half-life*

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

If this command is used with no arguments, it enables BGP route dampening. The *half-life*, *reuse*, *suppress*, and *max-suppress-time* arguments are position-dependent. Therefore, if any of these arguments are issued, they must all be specified.

When BGP dampening is configured and a prefix is withdrawn, BGP considers the withdrawn prefix as a flap and increases the penalty by a 1000. If BGP receives an attribute change, BGP increases the penalty by 500. If then the prefix has been withdrawn, BGP keeps the prefix in the BGP table as a history entry. If the prefix has not been withdrawn by the neighbor and BGP is not using this prefix, the prefix is marked as dampened. Dampened prefixes are not used in the BGP decision process and not installed to the routing table.

Examples

The following router configuration mode example sets the half life to 30 minutes, the reuse value to 1500, the suppress value to 10000, and the maximum suppress time to 120 minutes:

```
router bgp 5
 bgp dampening 30 1500 10000 120
```

The following address family configuration mode example sets the half life to 30 minutes, the reuse value to 1500, the suppress value to 10000, and the maximum suppress time to 120 minutes:

```
router bgp 5
 address-family ipv4 multicast
 bgp dampening 30 1500 10000 120
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
clear ip bgp dampening	Clears BGP route dampening information and unsuppresses the suppressed routes.
clear ip bgp flap-statistics	Clears BGP flap statistics.
show ip bgp dampened-paths	Displays BGP dampened routes.
show ip bgp flap-statistics	Displays BGP flap statistics.

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.

Defaults

This command is disabled by default.

Command Modes

Address family

Router configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use the **neighbor activate** address family configuration command for each neighbor you want to run the **bgp default ipv4-unicast** command for under the IPv4 unicast address family.

Examples

The following example enables IP version 4 unicast address family on all neighbors:

```
bgp default ipv4-unicast
```

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a neighboring router.

bgp default local-preference

To change the default local preference value, use the **bgp default local-preference** command in router configuration mode. 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.

Defaults

Local preference value of 100

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Generally, the default value of 100 allows you to easily define a particular path as less preferable than paths with no local preference attribute. The preference is sent to all routers and access servers in the local autonomous system.

Examples

The following example raises the default local preference value from the default of 100 to 200:

```
router bgp 200
 bgp default local-preference 200
```

Related Commands

Command	Description
set local-preference	Specifies a preference value for the autonomous system path.

bgp deterministic-med

To have Cisco IOS software enforce the deterministic comparison of the Multi Exit Discriminator (MED) variable between all paths received from the same autonomous system, use the **bgp deterministic-med** command in router configuration mode. To disable 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.

Defaults

The software does not enforce the deterministic comparison of the MED variable between all paths received from the same autonomous system.

Command Modes

Router configuration

Address-family configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

After the **bgp always-compare-med** command is configured, all paths for the same prefix that are received from different neighbors, which are in the same autonomous system, will be grouped together and sorted by the ascending MED value (received-only paths are ignored and not grouped or sorted). The best path selection algorithm will then pick the best paths using the existing rules; the comparison is made on a per neighbor autonomous system basis and then global basis. The grouping and sorting of paths occurs immediately after this command is entered. For correct results, all routers in the local autonomous system must have this command enabled (or disabled).

Examples

The following example specifies that the BGP router compare MED variables when choosing among routes advertised by the same subautonomous system within a confederation:

```
Router(config)# router bgp 204
Router(config-router)# bgp deterministic-med
```

The following example **show ip bgp** command output illustrates how route selection is affected by the configuration of the **bgp deterministic-med** command. The order in which routes are received affects how routes are selected for best path selection when the **bgp deterministic-med** command is not enabled.

The following sample output from the **show ip bgp** command shows three paths that are received for the same prefix (10.100.0.0), and the **bgp deterministic-med** command is not enabled:

```
router# show ip bgp 10.100.0.0
BGP routing table entry for 10.100.0.0/16, version 40
Paths: (3 available, best #3, advertised over IBGP, EBGP)
  109
    192.168.43.10 from 192.168.43.10 (192.168.43.1)
      Origin IGP, metric 0, localpref 100, valid, internal
  2051
    192.168.43.22 from 192.168.43.22 (192.168.43.2)
      Origin IGP, metric 20, localpref 100, valid, internal
  2051
    192.168.43.3 from 192.168.43.3 (10.4.1.1)
      Origin IGP, metric 30, valid, external, best
```

If the **bgp deterministic-med** command is not enabled on the router, the route selection can be affected by the order in which the routes are received. Consider the following scenario in which a router received three paths for the same prefix:

The **clear ip bgp *** command is entered to clear all routes in the local routing table.

```
Router# clear ip bgp *
```

The **show ip bgp** command is issued again after the routing table has been repopulated. Note that the order of the paths changed after clearing the BGP session. The results of the selection algorithm also changed. This occurred because the order in which the paths were received was different for the second session.

```
Router# show ip bgp 10.100.0.0

BGP routing table entry for 10.100.0.0/16, version 2
Paths: (3 available, best #3, advertised over EBGP)
  109 192.168.43.10 from 192.168.43.10 (192.168.43.1)
      Origin IGP, metric 0, localpref 100, valid, internal
  2051
    192.168.43.3 from 192.168.43.3 (10.4.1.1)
      Origin IGP, metric 30, valid, external
  2051
    192.168.43.22 from 192.168.43.22 (192.168.43.2)
      Origin IGP, metric 20, localpref 100, valid, internal, best
```

If the **bgp deterministic-med** command is enabled, then the result of the selection algorithm will always be the same, regardless of the order in which the paths are received by the local router. The following output is always generated when the **bgp deterministic-med** command is entered on the local router in this scenario:

```
Router# show ip bgp 10.100.0.0
BGP routing table entry for 10.100.0.0/16, version 15
Paths: (3 available, best #1, advertised over EBGP)
  109
    192.168.43.10 from 192.168.43.10 (192.168.43.1)
      Origin IGP, metric 0, localpref 100, valid, internal, best 3
    192.168.43.22 from 192.168.43.22 (192.168.43.2)
      Origin IGP, metric 20, localpref 100, valid, internal 3
    192.168.43.3 from 192.168.43.3 (10.4.1.1)
      Origin IGP, metric 30, valid, external
```

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection or session.

show ip bgp	Displays entries in the BGP routing table.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.

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.

Defaults

The behavior of this command is enabled by default.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Examples

The following example disables the automatic resetting of BGP sessions in router configuration mode:

```
router bgp 109
 no bgp fast-external-fallover
```

The following example disables the automatic resetting of BGP sessions in address family configuration mode:

```
router bgp 109
address-family ipv4 unicast
 no bgp fast-external-fallover
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.

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.

Defaults

BGP neighbor changes are logged.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
11.1 CC	This command was introduced.
12.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.0(1)	BGP neighbor changes are logged by default.

Usage Guidelines

The **bgp log-neighbor-changes** command enables logging of BGP neighbor status changes (up or down) and resets for troubleshooting network connectivity problems and measuring network stability. Unexpected neighbor resets might indicate high error rates or high packet loss in the network and should be investigated.

Using the **bgp log-neighbor-changes** command to enable status change message logging does not cause a substantial performance impact, unlike, for example, enabling per BGP update debugging. If the UNIX syslog facility is enabled, messages are sent to the UNIX host running the syslog daemon so that the messages can be stored and archived. If the UNIX syslog facility is not enabled, the status change messages are retained in the internal buffer of the router, and are not stored to disk. You can set the size of this buffer, which is dependent upon the available RAM, using the **logging buffered** command.

The neighbor status change messages are not tracked if the **bgp log-neighbor-changes** command is not enabled, except for the reset reason, which is always available as output of the **show ip bgp neighbors** command.

The **eigrp log-neighbor-changes** command enables logging of Enhanced IGRP (EIGRP) neighbor adjacencies, but messages for BGP neighbors are logged only if they are specifically enabled with the **bgp log-neighbor-changes** command.

Use the **show logging** command to display the log for the BGP neighbor changes.

Examples

The following example logs neighbor changes for BGP in router configuration mode:

```
bgp router 100
 bgp log-neighbor-changes
```

The following example logs neighbor changes for BGP in address family configuration mode:

```
bgp router 100
address-family ipv4 unicast
 bgp log-neighbor-changes
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
eigrp log-neighbor-changes	Enables the logging of neighbor adjacency changes to monitor the stability of the routing system and to help detect problems.
logging buffered	Logs messages to an internal buffer.
show ip bgp ipv4	Displays information about the TCP and BGP connections to neighbors.
show ip bgp neighbors	Displays information about BGP neighbors.
show logging	Displays the state of logging (syslog).

bgp redistribute-internal

To allow the redistribution of iBGP routes into an interior gateway protocol such as IS-IS or OSPF, use the **bgp redistribute-internal** command in router configuration mode. To remove the **bgp redistribute-internal** command from the configuration file and restore the system to its default condition where the software does not allow the redistribution of iBGP routes into Interior Gateway Protocols (IGPs), use the **no** form of this command.

bgp redistribute-internal

no bgp redistribute-internal

Syntax Description

This command has no arguments or keywords.

Defaults

By default iBGP routes are not redistributed into IGPs.

Command Modes

Router configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

Use of the **bgp redistribute-internal** command requires the **clear ip bgp** command to be issued to reset BGP connections.

Caution Redistributing iBGP routes into IGPs may cause routing loops to form within an autonomous system. Use this command with caution.

Examples

The following example shows iBGP routes being redistributed into OSPF:

```
router ospf 300
 redistribute bgp 200
!
router bgp 200
 bgp redistribute-internal
!
clear ip bgp *
```

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection or session.

bgp router-id

To configure a fixed router ID for a BGP-speaking router, use the **bgp router-id** command in router configuration mode. 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

ip-address	IP address of the router.

Defaults

The router ID is set to the IP address of a loopback interface if one is configured. If no virtual interfaces are configured, the highest IP address is configured for a physical interface on that router. Peering sessions will be reset if the router ID is changed.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command to configure a fixed router ID as an identifier of the router running BGP. A loopback interface, if one is configured, is more effective than a fixed interface as an identifier because there is no physical link to go down.

Examples

The following example shows the local router configured with the router ID of 192.168.70.24:

```
router bgp 100
  no synchronization
  bgp router-id 192.168.70.24
```

Related Commands

Command	Description
show ip bgp	Displays entries in the BGP routing table.

bgp rr-group

To create a route-reflector group and enable automatic inbound filtering for VPN version 4 (VPNv4) updates based on the allowed route target (RT) extended communities, use the **bgp rr-group** command in address family configuration mode. To disable a route-reflector group or route reflector, use the **no** form of this command.

bgp rr-group *extcom-list-number*

no bgp rr-group

Syntax Description

extcom-list-number	Number of a specific extended community-list that will be supported by the route-reflector group. The range of extended community-list numbers that can be specified is from 1 to 199. However, only one extended community-list is specified with the *extcom-list-number* argument.

Defaults

This command has no default behavior.

Command Modes

Address family configuration

Command History

Release	Modification
12.1	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S. The maximum number of extended community-lists that can supported by a route-reflector group was changed from 199 to 500.

Usage Guidelines

The **bgp rr-group** command can be used with the **ip extcommunity-list** command. The **ip extcommunity-list** command is used to create an extended community-list and specify a list of extended community RTs. Only extended community-lists are supported.

Examples

The following example configures a route-reflector group that will accept extended community-list number 500:

```
router bgp 101
 address-family vpnv4
 bgp rr-group 500
```

Related Commands

Command	Description
ip extcommunity-list	Creates an extended community access list.

clear ip bgp

To reset a BGP connection using BGP soft reconfiguration, use the **clear ip bgp** command in privileged EXEC mode at the system prompt.

clear ip bgp {* | *neighbor-address* | *peer-group-name*} [**soft** [**in** | **out**]]

Syntax Description

*	Specifies that all current BGP sessions will be reset.
neighbor-address	Specifies that only the identified BGP neighbor will be reset.
peer-group-name	Specifies that the specified BGP peer group will be reset.
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 is triggered.

Defaults

No reset is initiated.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(6)T	The dynamic inbound soft reset capability was added.
12.0(2)S	The dynamic inbound soft reset capability was added.

Usage Guidelines

You can reset inbound routing table updates dynamically or by generating new updates using stored update information. Using stored update information required additional memory for storing the updates.

To reset inbound routing table updates dynamically, all BGP routers must support the route refresh capability. To determine whether a BGP router supports this capability, use the **show ip bgp neighbors** command. If a router supports the route refresh capability, the following message is displayed:

```
Received route refresh capability from peer.
```

If all BGP routers support the route refresh capability, use the **clear ip bgp** {* | *address* | *peer-group -name*} **in** command. You need not use the **soft** keyword, because soft reset is automatically assumed when the route refresh capability is supported.

To generate new inbound updates from stored update information (rather than dynamically) without resetting the BGP session, you must preconfigure the local BGP router using the **neighbor soft-reconfiguration inbound** command. This preconfiguration causes the software to store all received updates without modification regardless of whether an update is accepted by the inbound policy. Storing updates is memory intensive and should be avoided if possible.

Outbound BGP soft configuration has no memory overhead and does not require any preconfiguration. You can trigger an outbound reconfiguration on the other side of the BGP session to make the new inbound policy take effect.

Use this command whenever any of the following changes occur:

- Additions or changes to the BGP-related access lists
- Changes to BGP-related weights
- Changes to BGP-related distribution lists
- Changes to BGP-related route maps

Examples

The following example clears the inbound session with the neighbor 10.108.1.1 without resetting the session:

```
Router# clear ip bgp 10.108.1.1 soft in
```

The following example clears the outbound session with the peer group named corp without resetting the session:

```
Router# clear ip bgp corp soft out
```

Related Commands

Command	Description
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
show ip bgp	Displays entries in the BGP routing table.

clear ip bgp dampening

To clear BGP route dampening information and unsuppress the suppressed routes, use the **clear ip bgp dampening** command in privileged EXEC mode.

clear ip bgp dampening [*ip-address network-mask*]

Syntax Description

ip-address	(Optional) IP address of the network about which to clear dampening information.
network-mask	(Optional) Network mask applied to the *ip-address* argument.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.

Examples

The following example clears route dampening information about the route to network 192.168.0.0 and unsuppresses its suppressed routes. When the address and mask arguments are not specified, the **clear ip bgp dampening** command clears route dampening information for the entire BGP routing table.

```
Router# clear ip bgp dampening  192.168.0.0 255.255.0.0
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
show ip bgp dampened-paths	Displays BGP dampened routes.

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 VPNn4 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.

Defaults

A reset is not initiated.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(2)S	This command was introduced.

Usage Guidelines

Using the **clear ip bgp external** command without the **soft** keyword will reset the session.

Examples

The following example clears an inbound session with the eBGP peers:

```
Router# clear ip bgp external in
```

or

```
Router# clear ip bgp external soft in
```

The following examples clear an outbound address family IPv4 multicast session with the eBGP peers:

```
Router# clear ip bgp external ipv4 multicast out
```

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection or session.

neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
show ip bgp	Displays entries in the BGP routing table.

clear ip bgp flap-statistics

To clear BGP flap statistics, use the **clear ip bgp flap-statistics** command in privileged EXEC mode.

clear ip bgp *ip-address* **flap-statistics** [{**regexp** *regexp*} | {**filter-list** *list-name*} | {*ip-address* *network-mask*}]

clear ip bgp [*ip-address*] **flap-statistics**

Syntax Description

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.
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.
network-mask	(Optional) Network mask applied to the *address* argument.

Defaults

No statistics are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

If no arguments or keywords are specified, the router will clear BGP flap statistics for all routes.

The flap statistics for a route are also cleared when a BGP peer is reset. Although the reset withdraws the route, no penalty is applied in this instance even though route flap dampening is enabled.

Examples

The following example clears all of the flap statistics for paths that pass filter list 3:

```
Router# clear ip bgp flap-statistics filter-list 3
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.

clear ip bgp peer-group

To clear all the members of a BGP peer group, use the **clear ip bgp peer-group** command in privileged EXEC mode.

clear ip bgp peer-group *tag*

Syntax Description

tag	Name of the BGP peer group to clear.

Defaults

No BGP peer group members are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.

Examples

The following example clears all members from the BGP peer group named internal:

```
Router# clear ip bgp peer-group internal
```

Related Commands

Command	Description
neighbor peer-group (assigning members)	Configures a BGP neighbor to be a member of a peer group.

clear ip prefix-list

To reset the hit count of the prefix list entries, use the **clear ip prefix-list** command in privileged EXEC mode.

clear ip prefix-list [*prefix-list-name*] [*network/length*]

Syntax Description

prefix-list-name	(Optional) The name of the prefix list from which the hit count is to be cleared.
network/length	(Optional) The network number and length (in bits) of the network mask. The slash mark is required.

Defaults

Does not clear the hit count.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The hit count is a value indicating the number of matches to a specific prefix list entry.

Examples

The following example clears the hit count from the prefix list entries for the prefix list named first_list that match the network mask 10.0.0.0/8:

```
Router# clear ip prefix-list first_list 10.0.0.0/8
```

Related Commands

Command	Description
distribute-list in (IP)	Filters networks received in updates.
distribute-list out	Suppresses networks from being advertised in updates.
ip prefix-list	Creates an entry in a prefix list.
ip prefix-list description	Adds a text description of a prefix list.
ip prefix-list sequence-number	Enables the generation of sequence numbers for entries in a prefix list.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
show ip bgp regexp	Displays information about a prefix list or prefix list entries.

default-information originate (BGP)

To control the redistribution of a protocol or network 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.

Defaults

This command is disabled by default.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

The **default-information originate** command should be used if the network operator needs to control the redistribution of default routes. Using the **default-information originate** command in BGP is similar to using the **network** command. However, to achieve the same result as configuring the **network** command with the route 0.0.0.0, the **default-information originate** command requires an explicit redistribution of the route 0.0.0.0. The **network** command requires only that route 0.0.0.0 is specified in the Interior Gateway Protocol (IGP) routing table. For this reason, the **network** command is preferred for redistributing default routes and protocols into BGP.

Examples

The following address family configuration mode example configures BGP to redistribute OSPF into BGP:

```
router bgp 164
 address-family ipv4 unicast
 default-information originate
 redistribute ospf 109
```

The following router configuration mode example configures BGP to redistribute OSPF into BGP:

```
router bgp 164
 default-information originate
 redistribute ospf 109
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
neighbor ebgp-multihop	Accepts and attempts BGP connections to external peers residing on networks that are not directly connected.
network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP routing process.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

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

number	Default metric value appropriate for the specified routing protocol.

Defaults

Built-in, automatic metric translations, as appropriate for each routing protocol

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

The **default-metric** command is used in conjunction with the **redistribute** router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

In BGP, this command sets the Multi Exit Discriminator (MED) metric. (The name of this metric for BGP Versions 2 and 3 is INTER_AS.)

Examples

The following router configuration mode example shows a router in autonomous system 109 using both the BGP and the Open Shortest Path First (OSPF) routing protocols. In the example, OSPF-derived routes are advertised by BGP with a default metric of 10:

```
router bgp 109
 default-metric 10
 redistribute ospf
```

The following address family configuration mode example shows a router in autonomous system 109 using both the BGP and the OSPF routing protocols. In the example, OSPF-derived routes are advertised by BGP with a default metric of 10:

```
router bgp 109
address-family ipv4 unicast
 default-metric 10
 redistribute ospf
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

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

external-distance	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.
internal-distance	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.
local-distance	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.

Defaults

external-distance: 20

internal-distance: 200

local-distance: 200

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is a positive integer from 1 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

Use this command if another protocol is known to be able to provide a better route to a node than was actually learned via external BGP (eBGP), or if some internal routes should be preferred by BGP.

Caution Changing the administrative distance of BGP internal routes is considered dangerous and is not recommended. One problem that can arise is the accumulation of routing table inconsistencies, which can break routing.

The **distance bgp** command replaces the **distance mbgp** command.

Examples

In the following router configuration mode example, internal routes are known to be preferable to those learned through the Interior Gateway Protocol (IGP), so the administrative distance values are set accordingly:

```
router bgp 109
 network 10.108.0.0
 neighbor 192.168.6.6 remote-as 123
 neighbor 172.16.1.1 remote-as 47
 distance bgp 20 20 200
```

In the following address family configuration mode example, internal routes are known to be preferable to those learned through IGP, so the administrative distance values are set accordingly:

```
router bgp 109
neighbor 192.168.6.6 remote-as 123
neighbor 172.16.1.1 remote-as 47
address family ipv4 multicast
 network 10.108.0.0
 distance bgp 20 20 200
 neighbor 192.168.6.6 activate
 neighbor 172.16.1.1 activate
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.

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

access-list-number	Standard IP access list number. The list defines which networks are to be received and which are to be suppressed in routing updates.
prefix *prefix-list-name*	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.
interface-type	(Optional) Interface type.
interface-number	(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.

Defaults

This command is disabled by default.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-number*, *interface-type*, and *interface-number* arguments were added.
12.0	The *prefix-list-name* argument was added.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

This command is not supported in Intermediate Sytem-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF).

Using a prefix list allows filtering based upon the prefix length, making it possible to filter either on the prefix list, the gateway, or both for incoming updates.

Do not use both the access-*list-number* and *prefix-list-name* arguments with the **distribute-list in** command.

Note To suppress networks from being advertised in updates, use the **distribute-list out** command.

Examples

In the following router configuration mode example, the BGP routing process accepts only two networks—network 0.0.0.0 and network 10.108.0.0:

```
access-list 1 permit 0.0.0.0
access-list 1 permit 10.108.0.0
access-list 1 deny 0.0.0.0 255.255.255.255
router bgp
 network 10.108.0.0
 distribute-list 1 in
```

In the following address family configuration mode example, the process accepts only two networks—network 0.0.0.0 and network 10.108.0.0:

```
access-list 1 permit 0.0.0.0
access-list 1 permit 10.108.0.0
access-list 1 deny 0.0.0.0 255.255.255.255
router bgp
address-family ipv4 multicast
 network 10.108.0.0
 distribute-list 1 in
```

In the following example, the BGP routing process accepts only networks with prefixes that match those in the prefix list named firstlist on the Ethernet interface 0:

```
router bgp
distribute-list prefix firstlist in ethernet 0
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
clear ip prefix-list	Resets the hit count of the prefix list entries.
distribute-list out	Suppresses networks from being advertised in updates.
ip prefix-list	Creates an entry in a prefix list.
ip prefix-list description	Adds a text description of a prefix list.

ip prefix-list sequence-number	Enables the generation of sequence numbers for entries in a prefix list.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
show ip bgp regexp	Displays information about a prefix list or prefix list entries.

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

access-list-number	Standard IP access list number. The list defines which networks are to be received and which are to be suppressed in routing updates.
prefix *prefix-list-name*	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.
interface-name	(Optional) Name of a particular interface.
routing-process	(Optional) Name of a particular routing process, or the keyword **static** or **connected**.
as-number	(Optional) Autonomous system number.

Defaults

This command is disabled by default.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-number* argument was added.
12.0	The *prefix-list-name* argument was added.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

When redistributing networks, a routing process name can be specified as an optional trailing argument to the **distribute-list** command. Specifying an argument causes the access list to be applied to only those routes derived from the specified routing process. After the process-specific access list is applied, any access list specified by a **distribute-list** command without a process name argument will be applied. Addresses not specified in the **distribute-list** command will not be advertised in outgoing routing updates.

Do not use both the *prefix-list* and *access-list-name* arguments with the **distribute-list out** command.

Note To filter networks received in updates, use the **distribute-list in** command.

Examples

The following router configuration mode example causes only one network (network 10.108.0.0) to be advertised by a RIP routing process:

```
access-list 1 permit 10.108.0.0
access-list 1 deny 0.0.0.0 255.255.255.255
router rip
 network 10.108.0.0
 distribute-list 1 out
```

The following address family configuration mode example causes only one network (network 10.108.0.0) to be advertised by a process:

```
access-list 1 permit 10.108.0.0
access-list 1 deny 0.0.0.0 255.255.255.255
router rip
address-family ipv4 unicast
 network 10.108.0.0
 distribute-list 1 out
```

In the following example, access list 1 is applied to outgoing routing updates, and Intermediate Sytem-to-Intermediate System (IS-IS) is enabled on Ethernet interface 0. Only network 10.131.101.0 will be advertised in outgoing IS-IS routing updates.

```
router isis
 redistribute ospf 109
 distribute-list 1 out
interface Ethernet 0
 ip router isis
access-list 1 permit 10.131.101.0 0.0.0.255
```

In the following example, the BGP routing process advertises only networks with prefixes that match those in the prefix list named firstlist on the Ethernet interface 0:

```
router bgp
distribute-list prefix firstlist out ethernet 0
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
clear ip prefix-list	Resets the hit count of the prefix list entries.
distribute-list in	Filters networks received in updates.
ip prefix-list	Creates an entry in a prefix list.
ip prefix-list description	Adds a text description of a prefix list.

ip prefix-list sequence-number	Enables the generation of sequence numbers for entries in a prefix list
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
show ip bgp regexp	Displays information about a prefix list or prefix list entries.

export map

To configure an export route map for a VRF, use the **export map** command in VRF configuration mode.

export map *route-map*

Syntax Description

route-map	Specifies the route map to be used as an export route map for the VRF.

Defaults

This command has no default behavior.

Command Modes

VRF configuration mode

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use an export route map when an application requires finer control over the routes that are exported out of a VRF than the control that is provided by import and export extended communities configured for the importing and exporting VRFs.

The **export map** command associates a route map with the specified VRF. You can use a route map to filter routes that are eligible for export out of a VRF, based on the route target extended community attributes of the route.

Only one export route map per VRF is supported.

Examples

The following example shows how to configure an export route map for a VRF:

```
Router(config)# ip vrf vrf_red
Router(config-vrf)# export map blue_export_map
```

Related Commands

Command	Description
import map	Configures an import route map for a VRF.
ip extcommunity-list	Creates an extended community list for BGP and controls access to it.
ip vrf	Configures a VRF routing table.
route-target	Creates a route-target extended community for a VRF.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

ip as-path access-list

To define a BGP autonomous system path access list, use the **ip as-path access-list** command in global configuration mode. 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

access-list-number	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.
as-regexp	Autonomous system in the access list using a regular expression. Refer to the "Regular Expressions" appendix in the *Cisco IOS Terminal Services Configuration Guide* for information about forming regular expressions.

Defaults

No access lists are defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can specify an access list filter on both inbound and outbound BGP routes. Each filter is an access list based on regular expressions. If the regular expression matches the representation of the autonomous system path of the route as an ASCII string, then the **permit** or **deny** condition applies. The autonomous system path does not contain the local autonomous system number. Use the **ip as-path access-list** global configuration command to define an BGP access list, and the **neighbor** router configuration command to apply a specific access list.

Examples

The following example specifies that the BGP neighbor with IP address 172.16.1.1 is not sent advertisements about any path through or from the adjacent autonomous system 123:

```
ip as-path access-list 1 deny _123_
ip as-path access-list 1 deny ^123$

router bgp 109
 network 10.108.0.0
 neighbor 192.168.6.6 remote-as 123
 neighbor 172.16.1.1 remote-as 47
 neighbor 172.16.1.1 filter-list 1 out
```

Related Commands

Command	Description
neighbor distribute-list	Distributes BGP neighbor information as specified in an access list.
neighbor filter-list	Sets up a BGP filter.

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** command in global configuration mode. To reenable 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.

Defaults

BGP communities are displayed in the Cisco default format, one 32-bit number.

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

RFC 1997, *BGP Communities Attribute* specifies that a BGP community is made up of two parts that are 2 bytes long. The first part is the autonomous system number and the second part is a 2-byte number. In the most recent version of the RFC, a community is of the form AA:NN. The Cisco default community format is one 32-bit number. The **ip bgp-community new-format** command changes the community format to AA:NN to conform to RFC 1997.

Examples

The following example upgrades a router that uses the 32-bit number community format to the AA:NN format:

```
Router(config)# ip bgp-community new-format
```

The following example shows how BGP community numbers are displayed when the **ip bgp-community new-format** command is enabled:

```
Router# show ip bgp 10.0.0.0

BGP routing table entry for 10.0.0.0/8, version 4
Paths: (2 available, best #2, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
  10.0.33.35
  35
    10.0.33.35 from 10.0.33.35 (192.168.3.3)
      Origin incomplete, metric 10, localpref 100, valid, external
      Community: 1:1
  Local
    0.0.0.0 from 0.0.0.0 (10.0.33.34)
      Origin incomplete, metric 0, localpref 100, weight 32768, valid, sourced, best
```

Related Commands

Command	Description
show ip bgp	Displays entries in the BGP routing table.

ip community-list

To create a community list for BGP and control access to it, use the **ip community-list** command in global configuration mode. 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

community-list-number	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.
community-number	Community number configured by a **set community** command. Valid value is one of the following: • 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** —Do not advertise this route to peers outside the local autonomous system. This route will not be advertised to other autonomous systems or sub-autonomous systems when confederations are configured. • **no-advertise**—Do not advertise this route to any peer (internal or external).

Defaults

Once you permit a value for the community number, the community list defaults to an implicit deny for everything else that has not been permitted.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0	The **local-as** attribute was added.

Examples

In the following example, Cisco IOS software permits all routes except the routes with the communities 5 and 10 or 10 and 15:

```
ip community-list 1 deny 5 10
ip community-list 1 deny 10 15
ip community-list 1 permit internet
```

The following example permits all routes within the local autonomous system:

```
ip community-list 1 permit local-as
```

Related Commands

Command	Description
set community	Sets the BGP COMMUNITIES attribute.
show ip bgp community	Displays routes that belong to specified BGP communities.

ip extcommunity-list

To create an extended community access list and control access to it, use the **ip extcommunity-list** command in global configuration mode. To delete the community list, use the **no** form of this command.

ip extcommunity-list *standard-list-number expanded-list-number* [*regular-expression*]{**permit** | **deny**} [**rt** | **soo** *extended-community-value*]

no ip extcommunity-list

Syntax Description

standard-list-number	Integer from 1 to 99 that identifies one or more permit or deny groups of extended communities.
expanded-list-number	Integer from 100 to 500 that identifies one or more permit or deny groups of extended communities. Regular expressions can be configured with expanded lists but not standard lists.
regular-expression	(Optional) An input string pattern to match against.
permit	Permits access for a matching condition.
deny	Denies access for a matching condition.
rt	(Optional) Specifies the route target (RT) extended community attribute. The **rt** keyword can be configured only with standard extended community lists and not expanded community lists.
soo	(Optional) Specifies the site of origin (SOO) extended community attribute. The **soo** keyword can be configured only with standard extended community lists and not expanded community lists.
extended-community-value	Specifies the route target or site of origin. The value can be one of the following combinations: • *autonomous-system-number***:***network-number* • *ip-address***:***network-number* The colon is used to separate the autonomous system number and network number or IP address and network number.

Defaults

Once you permit a value for the community number, the community list defaults to an implicit deny for everything else that has not been permitted.

Command Modes

Global configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).

The **ip extcommunity-list** command is used to configure extended community lists. All of the standard rules of access lists apply to the configuration of extended community lists. Regular expressions are supported by the expanded range of extended community list numbers. All regular expression configuration options are supported.

The route target (RT) extended community attribute is configured with the **rt** keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.

The site of origin (SOO) extended community attribute is configured with the **soo** keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO can be applied to routes that are learned from VRFs. The SOO should not be configured for stub sites or sites that are not multihomed.

Examples

The following example configures an extended community list that will permit routes from route target 901:10 and site of origin 802:20 and deny routes from route target 703:30 and site of origin 604:40:

```
Router(config)# ip extcommunity-list 1 permit rt 901:10
Router(config)# ip extcommunity-list 1 permit soo 802:20
Router(config)# ip extcommunity-list 1 deny rt 703:30 soo 604:40
```

The following example configures an extended community list (in the expanded range) that specifies that the BGP neighbor with IP address 192.168.1.1 is not sent advertisements about any path through or from autonomous system 123:

```
Router(config)# ip extcommunity-list 500 deny _123_
Router(config)# ip extcommunity-list 500 deny ^123 .*
Router(config)# router bgp 101
Router(config-router)# network 172.16.0.0
Router(config-router)# neighbor 10.140.6.6 remote-as 123
Router(config-router)# neighbor 192.168.1.1 remote-as 47
Router(config-router)# neighbor 10.125.1.1 filter-list 1 out
```

The following example configures an extended community list (in the expanded range) that permits routes from autonomous system 123 and denies all other routes:

```
Router(config)# ip extcommunity-list 500 permit (1-3)*
Router(config)# ip extcommunity-list 500 deny (^0-9)*
```

Related Commands

Command	Description
export map	Configures an export route map for a VRF.
match community	Matches a BGP VPN extended community list.
set extcommunity	Sets BGP extended community attributes.

show ip extcommunity-list	Displays routes that are permitted by the extended community list.
show route-map	Displays configured route maps.

ip prefix-list

To create an entry in a prefix list, use the **ip prefix-list** command in global configuration mode. To delete the entry, use the **no** form of this command.

ip prefix-list *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*}[**ge** *ge-value*] [**le** *le-value*]

no ip prefix-list *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*}[**ge** *ge-value*] [**le** *le-value*]

Syntax Description

list-name	Name of a prefix list.
seq	(Optional) Applies the sequence number to the prefix list entry being created or deleted.
seq-value	(Optional) Specifies the sequence number for the prefix list entry.
deny	Denies access for a matching condition.
permit	Permits access for a matching condition.
network/length	(Mandatory) The network number and length (in bits) of the network mask. The slash mark is required.
ge	(Optional) Applies the *ge-value* to the range specified. The *ge-value* represents the minimum prefix length to be matched.
ge-value	(Optional) Specifies the lesser value of a range (the “from” portion of the range description).
le	(Optional) Applies the *le-value* to the range specified. The *le-value* represents the minimum prefix length to be matched.
le-value	(Optional) Specifies the greater value of a range (the “to” portion of the range description).

Defaults

No prefix lists are created.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

When multiple entries of a prefix list match a given prefix, the longest, most specific match is chosen.

The router begins the search at the top of the prefix list, with the sequence number 1. Once a match or deny occurs, the router need not go through the rest of the prefix list. For efficiency, you may want to put the most common matches or denials near the top of the list, using the *seq-value* argument in the **ip prefix-list** command. The **show** commands always include the sequence numbers in their output.

By default, the sequence numbers are automatically generated.They can be suppressed with the **no ip prefix-list seq** command. Sequence values are generated in increments of 5. The first sequence value generated in a prefix list would be 5, then 10, then 15, and so on. If you specify a value for an entry and then do not specify values for subsequent entries, the assigned (generated) sequence values are incremented in units of 5. For example, if you specify that the first entry in the prefix list has a sequence value of 3 and then do not specify sequence values for the other entries, the automatically generated numbers will be 8, 13, 18, and so on.

The **ge** and **le** keywords can be used to specify the range of the prefix length to be matched for prefixes that are more specific than the *network/len* argument. Exact match is assumed when neither **ge** nor **le** is specified. The range is assumed to be from *ge-value* to 32 if only the **ge** attribute is specified. The range is assumed to be from **len** to *le-value* if only the **le** attribute is specified.

A specified *ge-value* and/or *le-value* must satisfy the following condition:

len < *ge-value* < *le-value* <= 32

Notes:

- If you use the **ip prefix-list** command with the **default-information originate** command to generate default routes, specify only IP adress matching. Avoid using the **ge** and **le** keywords.

  For example, the following command works:

  ```
  ip prefix-list anyrtcondition seq 5 permit 0.0.0.0/0
  ```

  However, the following command is not supported:

  ```
  ip prefix-list anyrtcondition seq 5 permit 0.0.0.0/0 le 32
  ```

- Using the **ip prefix-list** command with the **route-map** and **match ip next-hop** commands is not supported. Only IP address match clauses are supported.

Examples

The following examples show how a prefix list can be used.

To deny the default route 0.0.0.0/0:

```
ip prefix-list abc deny 0.0.0.0/0
```

To permit the prefix10.0.0.0/8:

```
ip prefix-list abc permit10.0.0.0/8
```

The following examples show how to specify a group of prefixes.

To accept a mask length of up to 24 bits in routes with the prefix 192/8:

```
ip prefix-list abc permit 192.168.0.0/8 le 24
```

To deny mask lengths greater than 25 bits in routes with a prefix of 192/8:

```
ip prefix-list abc deny 192.168.0.0/8 ge 25
```

To permit mask lengths from 8 to 24 bits in all address space:

```
ip prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

To deny mask lengths greater than 25 bits in all address space:

```
ip prefix-list abc deny 0.0.0.0/0 ge 25
```

To deny all mask lengths within the network 10/8:

```
ip prefix-list abc deny 10.0.0.0/8 le 32
```

To deny all masks with a length greater than or equal to 25 bits within the network 192.168.1/24:

```
ip prefix-list abc deny 192.168.1.0/24 ge 25
```

To permit all routes:

```
ip prefix-list abc permit 0.0.0.0/0 le 32
```

Related Commands

Command	Description
clear ip prefix-list	Resets the hit count of the prefix list entries.
ip prefix-list description	Adds a text description of a prefix list.
ip prefix-list sequence-number	Enables the generation of sequence numbers for entries in a prefix list.
match route-type (IP)	Redistributes routes of the specified type.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
neighbor prefix-list	Distributes BGP neighbor information as specified in a prefix list.
show ip prefix-list	Displays information about a prefix list or prefix list entries.

ip prefix-list description

To add a text description of a prefix list, use the **ip prefix-list description** command in global configuration mode. To remove the text description, use the **no** form of this command.

ip prefix-list *list-name sequence-number* **description** *text*

no ip prefix-list *list-name sequence-number* **description** *text*

Syntax Description

list name	Prefix list name.
sequence-number	Sequence number of the prefix list.
text	Text description of te prefix list.

Defaults

There is no text description.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-name*, *type*, and *number* arguments were added.
12.0	The *prefix-lis*t argument was added.

Usage Guidelines

This command is not supported in the Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF) protocols.

To suppress networks from being advertised in updates, use the **distribute-list out** command.

Examples

The following example shows a prefix list description that indicates which routes are permitted by the prefix list:

```
ip prefix-list customerA description Permit routes from customer A
```

Related Commands

Command	Description
clear ip prefix-list	Resets the hit count of the prefix list entries.
distribute-list out	Suppresses networks from being advertised in updates.
ip prefix-list	Creates an entry in a prefix list.
ip prefix-list sequence-number	Enables the generation of sequence numbers for entries in a prefix list.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
neighbor prefix-list	Distributes BGP neighbor information as specified in a prefix list.
show ip prefix-list	Displays information about a prefix list or prefix list entries.

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** command in global configuration mode. 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.

Defaults

There is no text description.

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.

Examples

The following example disables the default automatic generation of sequence numbers for prefix list entries:

```
no ip prefix-list sequence-number
```

Related Commands

Command	Description
clear ip prefix-list	Resets the hit count of the prefix list entries.
distribute-list in	Filters networks received in updates.
distribute-list out	Suppresses networks from being advertised in updates.
ip prefix-list	Creates an entry in a prefix list.
ip prefix-list sequence-number	Enables the generation of sequence numbers for entries in a prefix list.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
neighbor prefix-list	Distributes BGP neighbor information as specified in a prefix list.
show ip prefix-list	Displays information about a prefix list or prefix list entries.

match as-path

To match a BGP autonomous system path access list, use the **match as-path** command in route-map configuration mode. 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

path-list-number	Autonomous system path access list. An integer from 1 to 199.

Defaults

No path lists are defined.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The values set by the **match as-path** and **set weight** commands override global values. For example, the weights assigned with the **match as-path** and **set weight** route-map configuration commands override the weight assigned using the **neighbor weight** command.

A route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route-map section with an explicit match specified.

Examples

The following example sets the autonomous system path to match BGP autonomous system path access list 20:

```
route-map igp2bgp
 match as-path 20
```

Related Commands

Command	Description
match community-list	Matches a BGP community.
match interface (IP)	Distributes routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.

match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
neighbor weight	Assigns weight to a neighbor connection.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value in a route map configuration.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set origin (BGP)	Sets the BGP origin code.
set tag (IP)	Sets the value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

match community

To match a Border Gateway Protocol (BGP) community, use the **match community** command in route-map configuration mode. To remove the **match community** command from the configuration file and restore the system to its default condition where the software removes the BGP community list entry, use the **no** form of this command.

match community {*standard-list-number* | *expanded-list-number* | *community-list-name* [**exact-match**]}

no match community {*standard-list-number* | *expanded-list-number* | *community-list-name* [**exact-match**]}

Syntax Description

standard-list-number	Specifies a standard community list number from 1 to 99 that identifies one or more permit or deny groups of communities.
expanded-list-number	Specifies an expanded community list number from 100 to 199 that identifies one or more permit or deny groups of communities.
community-list-name	The community list name.
exact-match	(Optional) Indicates that an exact match is required. All of the communities and only those communities specified must be present.

Defaults

No community list is matched by the route map.

Command Modes

Route-map configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

A route map can have several parts. Any route that does not match at least one **match** command relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route-map section with an explicit match specified.

Matching based on community list number or name is one of the types of **match** commands applicable to BGP.

Examples

The following example shows that the routes matching community list 1 will have the weight set to 100. Any route that has community 109 will have the weight set to 100.

```
Router(config)# ip community-list 1 permit 109
Router(config)# !
Router(config)# route-map set_weight
Router(config-route-map)#  match community 1
Router(config-route-map)# set weight 100
```

The following example shows that the routes matching community list 1 will have the weight set to 200. Any route that has community 109 alone will have the weight set to 200.

```
Router(config)# ip community-list 1 permit 109
Router(config)# !
Router(config)# route-map set_weight
Router(config-route-map)# match community 1 exact
Router(config-route-map)# set weight 200
```

In the following example, the routes that match community list LIST_NAME will have the weight set to 100. Any route that has community 101 alone will have the weight set to 100.

```
Router(config)# ip community-list 1 permit 101
Router(config)# !
Router(config)# route-map set_weight
Router(config-route-map)# match community LIST_NAME
Router(config-route-map)# set weight 100
```

Related Commands

Command	Description
ip community-list	Creates a community list for BGP and controls access to it.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
set weight	Specifies the BGP weight for the routing table.

match extcommunity

To match Border Gateway Protocol (BGP) extended community list attributes, use the **match extcommunity** command in route-map configuration mode. To remove the **match extcommunity** command from the configuration file and remove the BGP extended community list attribute entry, use the **no** form of this command.

match extcommunity *standard-list-number* | *expanded-list-number*

no match extcommunity *standard-list-number* | *extended-list-number*

Syntax Description

standard-list-number	A standard extended community list number from 1 to 99 that identifies one or more permit or deny groups of extended community attributes.
expanded-list-number	An expanded extended community list number from 100 to 500 that identifies one or more permit or deny groups of extended community attributes.

Defaults

This command is disabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).

The **match extcommunity** command is used to configure match clauses that use extended community attributes in route maps. The range of numbers that can be configured with the **match extcommunity** command is from 1 to 99. All of the standard rules of match and set clauses apply to the configuration of extended community attributes.

Examples

The following example shows that the routes that match extended community list 1 will have the weight set to 100. Any route that has extended community 1 will have the weight set to 100.

```
Router(config)# ip extcommunity-list 1 rt 100:2
Router(config)# !
Router(config)# route-map MAP_NAME permit 10
Router(config-route-map)# match extcommunity 1
Router(config-route-map)# set weight 100
```

Related Commands

Command	Description
ip extcommunity-list	Creates an extended community list for BGP and controls access to it.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
set extcommunity	Sets BGP extended community attributes.
set weight	Specifies the BGP weight for the routing table.
show ip bgp filter-list	Displays routes that are permitted by the extended community list.
show route-map	Displays configured route maps.

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 *maximum-number*

no maximum-paths

Syntax Description

maximum-number	Maximum number of parallel routes an IP routing protocol installs in a routing table, in the range from 1 to 6.

Defaults

The default for Border Gateway Protocol (BGP) is one path. The default for all other routing protocols is four paths.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0(5)T	Address family configuration mode was added.

Examples

The following router configuration example allows a maximum of two paths to a destination:

```
router bgp 5
maximum paths 2
```

The following address family configuration example allows a maximum of two paths to a destination:

```
router bgp 5
 address-family ipv4 multicast
 maximum-paths 2
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.

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

ip-address	IP address of the number.
peer-group-name	Name of a BGP peer group.
seconds	Time (in seconds) is specified by an integer from 0 to 600.

Defaults

30 seconds for external peers and 5 seconds for internal peers.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

Examples

The following router configuration mode example sets the minimum time between sending BGP routing updates to 10 seconds:

```
router bgp 5
 neighbor 4.4.4.4 advertisement-interval 10
```

The following address family configuration mode example sets the minimum time between sending BGP routing updates to 10 seconds:

```
router bgp 5
address-family ipv4 unicast
 neighbor 4.4.4.4 advertisement-interval 10
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
neighbor peer-group (creating)	Creates a BGP peer group.

neighbor advertise-map non-exist-map

To install a Border Gateway Protocol (BGP) route as a locally originated route into a BGP routing table for conditional advertisement, use the **neighbor advertise-map non-exist-map** command in router configuration mode. To disable conditional advertisement, use the **no** form of this command.

neighbor{*ip-address*} **advertise-map** {*map-name*} **non-exist-map** {*map-name*}

no neighbor{*ip-address*} **advertise-map** {*map-name*} **non-exist-map** {*map-name*}

Syntax Description

ip-address	Specifies the IP address of the router that should receive conditional advertisements for a given set of routes.
map-name	Specifies the name of the advertise-map and the non-exist-map.

Defaults

The BGP Conditional Advertisement feature is not enabled by default.

Command Modes

Address family

Router configuration

Command History

Release	Modification
11.1CC	This command was introduced.
11.2	This command was integrated into Cisco IOS Release 11.2.

Usage Guidelines

Use the **neighbor advertise-map non-exist-map** router configuration command to conditionally advertise selected routes. The route map associated with the non-exist-map specifies the prefix that the BGP speaker will track. The route map associated with the advertise-map specifies the prefix that will be advertised when the prefix in the non-exist-map no longer exists. Any BGP route that is matched by the advertise-map route map will be advertised to the neighbor if the non-exist-map route map does not match any route in the BGP routing table. If the non-exist-map route map matches any route in the BGP routing table, any BGP routes that are matched by the advertise-map route map will not be advertised to the neighbor. All routes that may be dynamically advertised or not advertised need to exist in the BGP routing table for conditional advertisement to take place. The prefix tracked by the BGP speaker must be present in the IP routing table for the conditional advertisement not to take place.

Examples

The following address family configuration example configures a router to conditionally advertise routes to 10.1.1.1:

```
router bgp 5
 address-family ipv4 multicast
 neighbor 10.1.1.1 advertise-map map1 non-exist-map map2
```

The following router configuration example configures a router to conditionally advertise routes to 10.2.1.1:

```
router bgp 5
 neighbor 10.2.1.1 advertise-map map1 non-exist-map map2
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.

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

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
route-map *map-name*	(Optional) Name of the route map. The route map allows route 0.0.0.0 to be injected conditionally.

Defaults

No default route is sent to the neighbor.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0	Modifications were added to permit extended access lists.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

This command does not require the presence of 0.0.0.0 in the local router. When used with a route map, the default route 0.0.0.0 is injected if the route map contains a **match ip address** clause and there is a route that matches the IP access list exactly. The route map can contain other match clauses also.

You can use standard or extended access lists with the **neighbor default-originate** command.

Examples

In the following router configuration example, the local router injects route 0.0.0.0 to the neighbor 172.16.2.3 unconditionally:

```
router bgp 109
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 200
 neighbor 172.16.2.3 default-originate
```

In the following address family configuration example, the local router injects route 0.0.0.0 to the neighbor 172.16.2.3 unconditionally:

```
router bgp 109
neighbor 172.16.2.3 remote-as 200
address-family ipv4 unicast
 network 172.16.0.0
 neighbor 172.16.2.3 default-originate
```

In the following example, the local router injects route 0.0.0.0 to the neighbor 172.16.2.3 only if there is a route to 198.92.68.0 (that is, if a route with any mask exists, such as 255.255.255.0 or 255.255.0.0):

```
router bgp 109
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 200
 neighbor 172.16.2.3 default-originate route-map default-map
!
route-map default-map 10 permit
 match ip address 1
!
access-list 1 permit 198.92.68.0
```

In the following example, the last line of the configuration has been changed to show the use of an extended access list. The local router injects route 0.0.0.0 to the neighbor 172.16.2.3 only if there is a route to 198.92.68.0 with a mask of 255.255.0.0:

```
router bgp 109
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 200
 neighbor 172.16.2.3 default-originate route-map default-map
!
route-map default-map 10 permit
 match ip address 1
!
access-list 100 permit ip host 198.92.68.0 host 255.255.255.0
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
neighbor ebgp-multihop	Accepts and attempts BGP connections to external peers residing on networks that are not directly connected.

neighbor description

To associate a description with a neighbor, use the **neighbor description** command in router configuration mode. 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

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
text	Text (up to 80 characters) that describes the neighbor.

Defaults

There is no description of the neighbor.

Command Modes

Router configuration

Command History

Release	Modification
11.3	This command was introduced.

Examples

In the following example, the description of the neighbor is "peer with xyz.com":

```
router bgp 109
 network 172.16.0.0
 neighbor 172.16.2.3 description peer with xyz.com
```

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* | *expanded-list-number* | *access-list-name*| *prefix-list-name*} {**in** | **out**}

no neighbor {*ip-address* | *peer-group-name*} **distribute-list** {*access-list-number* | *expanded-list-number* | *access-list-name*| *prefix-list-name*} {**in** | **out**}

Syntax Description

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
access-list-number	Number of a standard or extended access list. The range of a standard access list number is from 1 to 99. The range of an extended access list number is from 100 to 199.
expanded-list-number	Number of an expanded access list number. The range of an expanded access list is from 1300 to 2699.
access-list-name	Name of a standard or extended access list.
prefix-list-name	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 to that neighbor.

Defaults

No BGP neighbor is specified.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.0	The *peer-group-name* argument was added.
11.2	The *access-list-name* argument was added.
12.0	The *prefix-list-name* argument was added.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

Using a distribute list is one of several ways to filter advertisements. Advertisements can also be filtered by using the following methods:

- Autonomous system path filters can be configured with the **ip as-path access-list** and **neighbor filter-list** commands.
- The **access-list (IP standard)** and **access-list (IP extended)** commands can be used to configure standard and extended access lists for the filtering of advertisement.
- The **route map** command can be used to filter advertisements. Route maps may be configured with autonomous system filters, prefix filters, access lists and distribute lists.

Standard access lists may be used to filter routing updates. However, in the case of route filtering when using classless interdomain routing (CIDR), standard access lists do not provide the level of granularity that is necessary to configure advanced filtering of network addresses and masks. Extended access lists, configured with the **access-list (IP extended)** command, should be used to configure route filtering when using CIDR because extended access lists allow the network operator to use wild card bits to filter the relevant prefixes and masks. Wild card bits are similar to the bit masks that are used with normal access lists; prefix and mask bits that correspond to wild card bits that are set to 0 are used in the comparison of addresses or prefixes and wild card bits that are set to 1 are ignored during any comparisons. This function of extended access list configuration can also be used to filter addresses or prefixes based on the prefix length.

Note Do not apply both a **neighbor distribute-list** and a **neighbor prefix-list** command to a neighbor in any given direction (inbound or outbound). These two commands are mutually exclusive, and only one command (**neighbor prefix-list** or **neighbor distribute-list**) can be applied to each inbound or outbound direction.

Examples

The following router configuration mode example applies list 39 to incoming advertisements from neighbor 120.23.4.1. List 39 permits the advertisement of network 10.109.0.0.

```
router bgp 109
 network 10.108.0.0
 neighbor 120.23.4.1 distribute-list 39 in
```

The following three examples show different scenarios for using an extended access list with a distribute list. The three examples are labeled “Example A”, “Example B”, and “Example C.” Each of the example extended access list configurations are used with the **neighbor distribute-list** command configuration example below.

```
router bgp 109
 network 10.108.0.0
 neighbor 120.23.4.1 distribute-list 101 in
```

Example A

The following extended access list example will permit route 192.168.0.0 255.255.0.0 but deny any more specific routes of 192.168.0.0 (including 192.168.0.0 255.255.255.0):

```
access-list 101 permit ip 192.168.0.0 0.0.0.0 255.255.0.0 0.0.0.0
access-list 101 deny ip 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255
```

Example B

The following extended access list example will permit route 10.108.0/24 but deny 131.108/16 and all other subnets of 10.108.0.0:

```
access-list 101 permit ip 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0
access-list 101 deny ip 10.108.0.0 0.0.255.255 255.255.0.0 0.0.255.255
```

Example C

The following extended access list example will deny all prefixes that are longer than 24 bits and permit all of the shorter prefixes:

```
access-list 101 deny ip 0.0.0.0 255.255.255.255 255.255.255.0 0.0.0.255
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
ip as-path access-list	Defines a BGP-related access list.
neighbor filter-list	Sets up a BGP filter.
neighbor peer-group (creating)	Creates a BGP peer group.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.

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** command in router configuration mode. 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

ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
ttl	(Optional) Time-to-live in the range from 1 to 255 hops.

Defaults

Only directly connected neighbors are allowed.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.0	The *peer-group-name* argument was added.

Usage Guidelines

This feature should be used only under the guidance of Cisco technical support staff.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

To prevent the creation of loops through oscillating routes, the multihop will not be established if the only route to the multihop peer is the default route (0.0.0.0).

Examples

The following example allows connections to or from neighbor 10.108.1.1, which resides on a network that is not directly connected:

```
router bgp 109
 neighbor 10.108.1.1 ebgp-multihop
```

Related Commands

Command	Description
neighbor advertise-map non-exist-map	Allows a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route.
neighbor peer-group (creating)	Creates a BGP peer group.
network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP routing process.

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

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
access-list-number	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.

Defaults

No filter is used.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.1	The **weight** keyword was removed.

Usage Guidelines

This command establishes filters on both inbound and outbound BGP routes.

The weights assigned with the **match as-path** and **set weight** route-map configuration commands override the weights assigned using the **neighbor weight** command.

Refer to the "Regular Expressions" appendix in the *Cisco IOS Terminal Services Configuration Guide* for information on forming regular expressions.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command with an IP address will override the value inherited from the peer group.

Examples

In the following router configuration mode example, the BGP neighbor with IP address 172.16.1.1 is not sent advertisements about any path through or from the adjacent autonomous system 123:

```
ip as-path access-list 1 deny _123_
ip as-path access-list 1 deny ^123$

router bgp 109
 network 10.108.0.0
 neighbor 192.168.6.6 remote-as 123
 neighbor 172.16.1.1 remote-as 47
 neighbor 172.16.1.1 filter-list 1 out
```

In the following address family configuration mode example, the BGP neighbor with IP address 172.16.1.1 is not sent advertisements about any path through or from the adjacent autonomous system 123:

```
ip as-path access-list 1 deny _123_
ip as-path access-list 1 deny ^123$

router bgp 109
address-family ipv4 unicast
 network 10.108.0.0
 neighbor 192.168.6.6 remote-as 123
 neighbor 172.16.1.1 remote-as 47
 neighbor 172.16.1.1 filter-list 1 out
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
ip as-path access-list	Defines a BGP-related access list.
match as-path	Match BGP autonomous system path access lists.
neighbor distribute-list	Distributes BGP neighbor information as specified in an access list.
neighbor peer-group (creating)	Creates a BGP peer group.
neighbor weight	Assigns a weight to a neighbor connection.
set weight	Specifies the BGP weight for the routing table

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

ip-address	IP address of the local BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
as-number	Valid autonomous system number from 1 to 65535. Do not specify the autonomous system number to which the neighbor belongs.

Defaults

This command is disabled by default.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
12.0(4.4)S	This command was introduced.
12.0(5)T	Address family configuration mode was added.

Usage Guidelines

Each BGP peer or peer group can be made to have a local autonomous system value for the purpose of peering. In the case of peer groups, the local autonomous system value is valid for all peers in the peer group.

This feature cannot be customized for individual peers in a peer group.

If this command is configured, you cannot use the local BGP autonomous system number or the autonomous system number of the remote peer.

This command is valid only if the peer is a true eBGP peer. This feature does not work for two peers in different subautonomous systems in a confederation.

Examples

The following address family configuration example shows the customization of neighbor 172.20.1.1 configured to have an autonomous system number of 300 for the purpose of peering:

```
router bgp 109
address-family ipv4 multicast
 network 172.20.0.0
 neighbor 172.20.1.1 local-as 300
```

The following router configuration example shows the customization of neighbor 172.20.1.1 configured to have autonomous system number of 300 for the purpose of peering:

```
router bgp 109
 network 172.20.0.0
 neighbor 172.20.1.1 local-as 300
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
show ip bgp neighbors	Displays information about BGP neighbors.
show ip bgp peer-group	Displays information about BGP peer groups.

neighbor maximum-prefix

To control how many prefixes can be received from a neighbor, use the **neighbor maximum-prefix** command in router configuration mode. 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

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
maximum	Maximum number of prefixes allowed from this neighbor.
threshold	(Optional) Integer specifying at what percentage of *maximum* 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 *maximum* is exceeded, instead of terminating the peering.

Defaults

This command is disabled by default. There is no limit on the number of prefixes.

Command Modes

Router configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

This command allows you to configure a maximum number of prefixes that a BGP router is allowed to receive from a peer. It adds another mechanism (in addition to distribute lists, filter lists, and route maps) to control prefixes received from a peer.

When the number of received prefixes exceeds the maximum number configured, the router terminates the peering (by default). However, if the **warning-only** keyword is configured, the router instead only sends a log message, but continues peering with the sender. If the peer is terminated, the peer stays down until the **clear ip bgp** command is issued.

Examples

The following example sets the maximum number of prefixes allowed from the neighbor at 192.168.6.6 to 1000:

```
router bgp 109
 network 10.108.0.0
 neighbor 192.168.6.6 maximum-prefix 1000
```

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection using BGP soft reconfiguration.

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** command in router configuration mode. 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

ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.0	The *peer-group-name* argument was added.

Usage Guidelines

This command is useful in nonmeshed networks (such as Frame Relay or X.25) where BGP neighbors may not have direct access to all other neighbors on the same IP subnet.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command with an IP address will override the value inherited from the peer group.

For a finer granularity of control, see the **set ip next-hop** command.

Examples

The following example forces all updates destined for 10.108.1.1 to advertise this router as the next hop:

```
router bgp 109
 neighbor 10.108.1.1 next-hop-self
```

Related Commands

Command	Description
neighbor peer-group (creating)	Creates a BGP peer group.
set ip next-hop (BGP)	Indicates where to output packets that pass a match clause of a route map for policy routing.

neighbor password

To enable Message Digest 5 (MD5) authentication on a TCP connection between two BGP peers, use the **neighbor password** command in router configuration mode. 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

ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
string	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 *number-space-anything*. The space after the number causes problems.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

You can invoke authentication between two BGP peers, causing each segment sent on the TCP connection between them to be verified. This feature must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made. The authentication feature uses the MD5 algorithm. Specifying this command causes the generation and checking of the MD5 digest on every segment sent on the TCP connection.

Configuring a password for a neighbor will cause an existing session to be torn down and a new one established.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

If a router has a password configured for a neighbor, but the neighbor router does not, a message such as the following will appear on the console while the routers attempt to establish a BGP session between them:

```
%TCP-6-BADAUTH: No MD5 digest from [peer's IP address]:11003 to [local router's
IP address]:179
```

Similarly, if the two routers have different passwords configured, a message such as the following will appear on the screen:

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's
IP address]:179
```

Examples

The following example enables the authentication feature between this router and the BGP neighbor at 131.102.1.1. The password that must also be configured for the neighbor is bla4u00=2nkq.

```
router bgp 109
 neighbor 10.108.1.1 password bla4u00=2nkq
```

Related Commands

Command	Description
neighbor peer-group (creating)	Creates a BGP peer group.

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

ip-address	IP address of the BGP neighbor that belongs to the peer group specified by the *peer-group-name* argument.
peer-group-name	Name of the BGP peer group to which this neighbor belongs.

Defaults

There are no BGP neighbors in a peer group.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

The neighbor at the IP address indicated inherits all the configured options of the peer group.

Examples

The following router configuration mode example assigns three neighbors to the peer group named internal:

```
router bgp 100
 neighbor internal peer-group
 neighbor internal remote-as 100
 neighbor internal update-source loopback 0
 neighbor internal route-map set-med out
 neighbor internal filter-list 1 out
 neighbor internal filter-list 2 in
 neighbor 172.16.232.53 peer-group internal
 neighbor 172.16.232.54 peer-group internal
 neighbor 172.16.232.55 peer-group internal
 neighbor 172.16.232.55 filter-list 3 in
```

The following address family configuration mode example assigns three neighbors to the peer group named internal:

```
router bgp 100
address-family ipv4 unicast
 neighbor internal peer-group
 neighbor internal remote-as 100
 neighbor internal update-source loopback 0
 neighbor internal route-map set-med out
 neighbor internal filter-list 1 out
 neighbor internal filter-list 2 in
 neighbor 172.16.232.53 peer-group internal
 neighbor 172.16.232.54 peer-group internal
 neighbor 172.16.232.55 peer-group internal
 neighbor 172.16.232.55 filter-list 3 in
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
neighbor peer-group (creating)	Creates a BGP peer group.
neighbor shutdown	Disables a neighbor or peer group.

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

peer-group-name	Name of the BGP peer group.

Defaults

There is no BGP peer group.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
11.0	This command was introduced.
11.1(20)CC	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were added.
12.0(2)S	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were added.
12.0(7)T	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were removed. Address family configuration mode was added.

Usage Guidelines

Often in a BGP or multiprotocol BGP speaker, many neighbors are configured with the same update policies (that is, same outbound route maps, distribute lists, filter lists, update source, and so on). Neighbors with the same update policies can be grouped into peer groups to simplify configuration and make update calculation more efficient.

Note Peer group members can span multiple logical IP subnets, and can transmit, or pass along, routes from one peer group member to another.

Once a peer group is created with the **neighbor peer-group** command, it can be configured with the **neighbor** commands. By default, members of the peer group inherit all the configuration options of the peer group. Members also can be configured to override the options that do not affect outbound updates.

Peer group members will always inherit the following configuration options: remote-as (if configured), version, update-source, out-route-map, out-filter-list, out-dist-list, minimum-advertisement-interval, and next-hop-self. All the peer group members will inherit changes made to the peer group.

If a peer group is not configured with a remote-as option, the members can be configured with the **neighbor** {*ip-address* | *peer-group-name*} **remote-as** command. This command allows you to create peer groups containing external BGP (eBGP) neighbors.

Examples

The following example configurations show how to create these types of neighbor peer group:

- internal Border Gateway Protocol (iBGP) peer group
- eBGP peer group
- Multiprotocol BGP peer group

iBGP Peer Group

In the following example, the peer group named internal configures the members of the peer group to be iBGP neighbors. By definition, this is an iBGP peer group because the **router bgp** command and the **neighbor remote-as** command indicate the same autonomous system (in this case, autonomous system 100). All the peer group members use loopback 0 as the update source and use set-med as the outbound route map. The **neighbor internal filter-list 2 in** command shows that, except for 171.69.232.55, all the neighbors have filter list 2 as the inbound filter list.

```
router bgp 100
 neighbor internal peer-group
 neighbor internal remote-as 100
 neighbor internal update-source loopback 0
 neighbor internal route-map set-med out
 neighbor internal filter-list 1 out
 neighbor internal filter-list 2 in
 neighbor 171.69.232.53 peer-group internal
 neighbor 171.69.232.54 peer-group internal
 neighbor 171.69.232.55 peer-group internal
 neighbor 171.69.232.55 filter-list 3 in
```

eBGP Peer Group

The following example defines the peer group named external-peers without the **neighbor remote-as** command. By definition, this is an eBGP peer group because each individual member of the peer group is configured with its respective autonomous system number separately. Thus the peer group consists of members from autonomous systems 200, 300, and 400. All the peer group members have the set-metric route map as an outbound route map and filter list 99 as an outbound filter list. Except for neighbor 171.69.232.110, all of them have 101 as the inbound filter list.

```
router bgp 100
 neighbor external-peers peer-group
 neighbor external-peers route-map set-metric out
 neighbor external-peers filter-list 99 out
 neighbor external-peers filter-list 101 in
 neighbor 171.69.232.90 remote-as 200
 neighbor 171.69.232.90 peer-group external-peers
 neighbor 171.69.232.100 remote-as 300
 neighbor 171.69.232.100 peer-group external-peers
 neighbor 171.69.232.110 remote-as 400
 neighbor 171.69.232.110 peer-group external-peers
 neighbor 171.69.232.110 filter-list 400 in
```

Multiprotocol BGP Peer Group

In the following example, all members of the peer group are multicast-capable:

```
router bgp 100
neighbor 10.1.1.1 remote-as 1
neighbor 172.16.2.2 remote-as 2
address-family ipv4 multicast
 neighbor mygroup peer-group
 neighbor 10.1.1.1 peer-group mygroup
 neighbor 172.16.2.2 peer-group mygroup
 neighbor 10.1.1.1 activate
 neighbor 172.16.2.2 activate
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
clear ip bgp peer-group	Removes all the members of a BGP peer group.
show ip bgp peer-group	Displays information about BGP peer groups.

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

ip-address	IP address of neighbor.
peer-group-name	Name of a BGP peer group.
prefix-list-name	Name of a prefix list.
in	Access list is applied to incoming advertisements to that neighbor.
out	Access list is applied to outgoing advertisements to that neighbor.

Defaults

No BGP neighbor is specified.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
12.0	This command was introduced.
11.0	The *peer-group-name* argument was added.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

Using prefix lists is one of two ways to filter BGP advertisements. The other way is to use AS-path filters, as with the **ip as-path access-list** global configuration command and the **neighbor filter-list** command, and access or prefix lists, as with the **neighbor distribute-list** command.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command with an IP address will override the value inherited from the peer group.

Note Do not apply both a **neighbor distribute-list** and a **neighbor prefix-list** command to a neighbor in any given direction (inbound or outbound). These two commands are mutually exclusive, and only one command (**neighbor prefix-list** or **neighbor distribute-list**) can be applied to each inbound or outbound direction.

Examples

The following router configuration mode example applies the prefix list named abc to incoming advertisements to neighbor 120.23.4.1:

```
router bgp 109
 network 10.108.0.0
 neighbor 120.23.4.1 prefix-list abc in
```

The following address family configuration mode example applies the prefix list named abc to incoming advertisements to neighbor 120.23.4.1:

```
router bgp 109
address-family ipv4 unicast
 network 10.108.0.0
 neighbor 120.23.4.1 prefix-list abc in
```

The following example applies the prefix list named CustomerA to outgoing advertisements to neighbor 120.23.4.1:

```
router bgp 109
 network 10.108.0.0
 neighbor 120.23.4.1 prefix-list CustomerA out
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
clear ip prefix-list	Resets the hit count of the prefix list entries.
ip as-path access-list	Defines a BGP-related access list.
ip prefix-list	Creates an entry in a prefix list.
ip prefix-list description	Adds a text description of a prefix list.
ip prefix-list sequence-number	Enables the generation of sequence numbers for entries in a prefix list.
neighbor filter-list	Sets up a BGP filter.
neighbor remote-as	Creates a BGP peer group.
show ip bgp peer-group	Displays information about BGP peer groups.
show ip prefix-list	Displays information about a prefix list or prefix list entries.

neighbor remote-as

To add an entry to the BGP or multiprotocol BGP neighbor table, use the **neighbor remote-as** command in router configuration mode. 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

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
as-number	Autonomous system to which the neighbor belongs.

Defaults

There are no BGP or multiprotocol BGP neighbor peers.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.0	The *peer-group-name* argument was added.
11.1(20)CC	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were added.
12.0(7)T	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were removed.

Usage Guidelines

Specifying a neighbor with an autonomous system number that matches the autonomous system number specified in the **router bgp** global configuration command identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered external.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

By default, neighbors that are defined using the **neighbor remote-as** command in router configuration mode exchange only unicast address prefixes. To exchange other address prefix types, such as multicast and Virtual Private Network (VPN) Version 4, neighbors must also be activated using the **neighbor activate** command in address family configuration mode.

Examples

The following example specifies that a router at the address 10.108.1.2 is a neighbor in autonomous system number 109:

```
router bgp 110
 network 10.108.0.0
 neighbor 10.108.1.2 remote-as 109
```

The following example assigns a BGP router to autonomous system 109, and two networks are listed as originating in the autonomous system. Then the addresses of three remote routers (and their autonomous systems) are listed. The router being configured will share information about networks 10.108.0.0 and 192.31.7.0 with the neighbor routers. The first router listed is in the same Class B network address space, but in a different autonomous system; the second **neighbor remote-as** command illustrates specification of an internal neighbor (with the same autonomous system number) at address 10.108.234.2; and the last **neighbor remote-as** command specifies a neighbor on a different network.

```
router bgp 109
 network 10.108.0.0
 network 192.31.7.0
 neighbor 10.108.200.1 remote-as 167
 neighbor 10.108.234.2 remote-as 109
 neighbor 150.136.64.19 remote-as 99
```

The following example configures neighbor 10.108.1.1 in autonomous system 1 to exchange only multicast routes:

```
router bgp 109
neighbor 10.108.1.1 remote-as 1
neighbor 131.108 1.2 remote-as 1
neighbor 172.16.2.2 remote-as 2
address-family ipv4 multicast
  neighbor 10.108.1.1 activate
  neighbor 131.108 1.2 activate
  neighbor 172.16.2.2 activate
```

The following example configures neighbor 10.108.1.1 in autonomous system 1 to exchange only unicast routes:

```
router bgp 109
neighbor 10.108.1.1 remote-as 1
neighbor 131.108 1.2 remote-as 1
neighbor 172.16.2.2 remote-as 2
```

Related Commands

Command	Description
neighbor remote-as	Creates a BGP peer group.
router bgp	Configures the BGP routing process.

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** command in router configuration mode. 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

ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
10.3	This command was introduced.
11.0	The *peer-group-name* argument was added.

Usage Guidelines

This command is available for external BGP (eBGP) neighbors only.

When an update is passed to the external neighbor, if the autonomous system path includes private autonomous system numbers, the software will drop the private autonomous system numbers.

If the autonomous system path includes both private and public autonomous system numbers, the software considers this to be a configuration error and does not remove the private autonomous system numbers.

If the autonomous system path contains the autonomous system number of the eBGP neighbor, the private autonomous system numbers will not be removed.

If this command is used with confederation, it will work as long as the private autonomous system numbers follow the confederation portion of the autonomous path.

The private autonomous system values are from 64512 to 65535.

Examples

The following example shows a configuration that will remove the private autonomous system number from the updates sent to 172.16.2.33. The result is that the autonomous system path for the paths advertised by 10.108.1.1 through autonomous system 100 will just contain "100" (as seen by autonomous system 2051).

```
router bgp 100
 neighbor 10.108.1.1 description peer with private-as
 neighbor 10.108.1.1 remote-as 65001
 neighbor 172.16.2.33 description eBGP peer
 neighbor 172.16.2.33 remote-as 2051
 neighbor 172.16.2.33 remove-private-as

router-in-AS100# show ip bgp 10.0.0.0

BGP routing table entry for 10.0.0.0/8, version 15
Paths: (1 available, best #1)
  Advertised to non peer-group peers:
    172.16.2.33
  65001
    10.108.1.1 from 10.108.1.1
      Origin IGP, metric 0, localpref 100, valid, external, best

router-in-AS2501# show ip bgp 10.0.0.0

BGP routing table entry for 10.0.0.0/8, version 3
Paths: (1 available, best #1)
  Not advertised to any peer
  2
    172.16.2.32 from 172.16.2.32
      Origin IGP, metric 0, localpref 100, valid, external, best
```

Related Commands

Command	Description
neighbor remote-as	Allows entries to the BGP neighbor table.
show ip bgp	Displays entries in the BGP routing table.

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

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP or multiprotocol BGP peer group.
map-name	Name of a route map.
in	Applies route map to incoming routes.
out	Applies route map to outgoing routes.

Defaults

No route maps are applied to a peer.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

When specified in address family configuration mode, this command applies a route map to that particular address family only. When specified in router configuration mode, this command applies a route map to IP Version 4 unicast routes only.

If an outbound route map is specified, it is proper behavior to only advertise routes that match at least one section of the route map.

If you specify a BGP or multiprotocol BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

Examples

The following router configuration mode example applies a route map named internal-map to a BGP incoming route from 172.16.70.24:

```
router bgp 5
 neighbor 172.16.70.24 route-map internal-map in

route-map internal-map
 match as-path 1
 set local-preference 100
```

The following address family configuration mode example applies a route map named internal-map to a multiprotocol BGP incoming route from 172.16.70.24:

```
router bgp 5
address-family ipv4 multicast
 neighbor 172.16.70.24 route-map internal-map in

route-map internal-map
 match as-path 1
 set local-preference 100
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
neighbor remote-as	Creates a BGP peer group.

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

ip-address	IP address of the BGP neighbor being identified as a client.

Defaults

There is no route reflector in the autonomous system.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
11.1	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

By default, all internal BGP (iBGP) speakers in an autonomous system must be fully meshed, and neighbors do not readvertise iBGP learned routes to neighbors, thus preventing a routing information loop. When all the clients are disabled, the local router is no longer a route reflector.

If you use route reflectors, all iBGP speakers need not be fully meshed. In the route reflector model, an Interior BGP peer is configured to be a *route reflector* responsible for passing iBGP learned routes to iBGP neighbors. This scheme eliminates the need for each router to talk to every other router.

Use the **neighbor route-reflector-client** command to configure the local router as the route reflector and the specified neighbor as one of its clients. All the neighbors configured with this command will be members of the client group and the remaining iBGP peers will be members of the nonclient group for the local route reflector.

The **bgp client-to-client reflection** command controls client-to-client reflection.

Examples

In the following router configuration mode example, the local router is a route reflector. It passes learned iBGP routes to the neighbor at 172.16.70.24.

```
router bgp 5
 neighbor 172.16.70.24 route-reflector-client
```

In the following address family configuration mode example, the local router is a route reflector. It passes learned iBGP routes to the neighbor at 172.16.70.24.

```
router bgp 5
address-family ipv4 unicast
 neighbor 172.16.70.24 route-reflector-client
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
bgp client-to-client reflection	Restores route reflection from a BGP route reflector to clients.
bgp cluster-id	Configures the cluster ID if the BGP cluster has more than one route reflector.
neighbor route-reflector-client	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
show ip bgp	Displays entries in the BGP routing table.

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** [**both** | **standard** | **extended**]

no neighbor {*ip-address* | *peer-group-name*} **send-community**

Syntax Description

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
both	(Optional) Specifies that both standard and extended communities will be sent.
standard	(Optional) Specifies that only standard communities will be sent.
extended	(Optional) Specifies that only extended communities will be sent.

Defaults

No communities attribute is sent to any neighbor.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.3	This command was introduced.
11.0	The *peer-group-name* argument was added.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

Examples

In the following router configuration mode example, the router belongs to autonomous system 109 and is configured to send the communities attribute to its neighbor at IP address 172.16.70.23:

```
router bgp 109
 neighbor 172.16.70.23 send-community
```

In the following address family configuration mode example, the router belongs to autonomous system 109 and is configured to send the communities attribute to its neighbor at IP address 172.16.70.23:

```
router bgp 109
address-family ipv4 multicast
 neighbor 172.16.70.23 send-community
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
match community	Matches a BGP community.
neighbor remote-as	Creates a BGP peer group.
set community	Sets the BGP communities attribute.

neighbor shutdown

To disable a neighbor or peer group, use the **neighbor shutdown** command in router configuration mode. To reenable 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

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.

Defaults

No change is made to the status of any BGP neighbor or peer group.

Command Modes

Router configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The **neighbor shutdown** command terminates any active session for the specified neighbor or peer group and removes all associated routing information. In the case of a peer group, a large number of peering sessions could be terminated suddenly.

To display a summary of BGP neighbors and peer group connections, use the **show ip bgp summary** command. Those neighbors with an Idle status and the Admin entry have been disabled by the **neighbor shutdown** command.

"State/PfxRcd" shows the current state of the BGP session or the number of prefixes the router has received from a neighbor or peer group. When the maximum number (as set by the **neighbor maximum-prefix** command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is idle.

Examples

The following example disables any active session for the neighbor 172.16.70.23:

```
neighbor 172.16.70.23 shutdown
```

The following example disables all peering sessions for the peer group named internal:

```
neighbor internal shutdown
```

Related Commands

Command	Description
neighbor maximum-prefix	Controls how many prefixes can be received from a neighbor.
show ip bgp summary	Displays the status of all BGP connections.

neighbor soft-reconfiguration

To configure the Cisco IOS software to start storing updates, use the **neighbor soft-reconfiguration** command in router configuration mode. 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

ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
inbound	(Optional) Indicates that the update to be stored is an incoming update.

Defaults

Soft reconfiguration is not enabled.

Command Modes

Router configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Entering this command starts the storage of updates, which is required to do inbound soft reconfiguration. Outbound BGP soft reconfiguration does not require inbound soft reconfiguration to be enabled.

To use soft reconfiguration, or soft reset, without preconfiguration, both BGP peers must support the soft route refresh capability, which is advertised in the open message sent when the peers establish a TCP session. Routers running Cisco IOS software releases prior to Release 12.1 do not support the route refresh capability and must clear the BGP session using the **neighbor soft-reconfiguration** command. Clearing the BGP session using the **neighbor soft-reconfiguration** command has a negative effect on network operations and should be used only as a last resort. Routers running Cisco IOS software Release 12.1 or later releases support the route refresh capability and dynamic soft resets, and can use the **clear ip bgp** {* | *ip-address* | *peer-group name*} **in** command to clear the BGP session.

To determine whether a BGP router supports this capability, use the **show ip bgp neighbors** command. If a router supports the route refresh capability, the following message is displayed:

```
Received route refresh capability from peer.
```

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

Examples

The following example enables inbound soft reconfiguration for the neighbor 10.108.1.1. All the updates received from this neighbor will be stored unmodified, regardless of the inbound policy. When inbound soft reconfiguration is done later, the stored information will be used to generate a new set of inbound updates.

```
router bgp 100
 neighbor 10.108.1.1 remote-as 200
 neighbor 10.108.1.1 soft-reconfiguration inbound
```

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection using BGP soft reconfiguration.
neighbor remote-as	Creates a BGP peer group.
show ip bgp neighbors	Display information about the TCP and BGP connections to neighbors.

neighbor timers

To set the timers for a specific BGP peer or peer group, use the **neighbor timers** command in router configuration mode. 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

ip-address	(Optional) A BGP peer or peer group IP address.
peer-group-name	(Optional) Name of the BGP peer group.
keepalive	Frequency (in seconds) with which the Cisco IOS software sends *keepalive* messages to its peer. The default is 60 seconds.
holdtime	Interval (in seconds) after not receiving a *keepalive* message that the software declares a peer dead. The default is 180 seconds.

Defaults

keepalive: 60 seconds

holdtime: 180 seconds

Command Modes

Router configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The timers configured for a specific neighbor or peer group override the timers configured for all BGP neighbors using the **timers bgp** command.

Examples

The following example changes the keepalive timer to 70 seconds and the hold-time timer to 210 seconds for the BGP peer 192.98.47.0:

```
router bgp 109
 neighbor 192.98.47.0 timers 70 210
```

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

ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
route-map-name	Name of a route map.

Defaults

No routes are unsuppressed.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)T	Address family configuration mode was added.

Usage Guidelines

Use of the **neighbor unsuppress-map** command allows specified suppressed routes to be advertised.

Examples

The following address family configuration example shows the routes specified by a route map named internal-map being unsuppressed for neighbor 172.20.16.6:

```
router bgp 100
address-family ipv4 multicast
 network 172.20.0.0
 neighbor 172.20.16.6 unsuppress-map internal-map
```

The following router configuration example shows the routes specified by a route map named internal-map being unsuppressed for neighbor 172.20.16.6:

```
router bgp 100
 network 172.20.0.0
 neighbor 172.20.16.6 unsuppress-map internal-map
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the routing in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
aggregate-address	Creates an aggregate entry in a BGP routing table.
neighbor route-map	Applies a route map to inbound or outbound routes.

neighbor update-source

To have the Cisco IOS software allow Border Gateway Protocol (BGP) sessions to use a specific operational interface for TCP connections, use the **neighbor update-source** command in router configuration mode. 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

ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
interface-type	Interface to be used as the source.

Defaults

Best local address

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command works in conjunction with any specified interface on the router. The loopback interface is the interface that is most commonly used with this feature. For more information, refer to the loopback interface feature described in the "Interface Configuration Overview" chapter of the *Cisco IOS Interface Configuration Guide*.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

Examples

The following example sources BGP TCP connections for the specified neighbor with the IP address of the loopback interface rather than the best local address:

```
router bgp 110
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 110
 neighbor 172.16.2.3 update-source Loopback0
```

Related Commands

Command	Description
neighbor remote-as	Creates a BGP peer group.

neighbor version

To configure the Cisco IOS software to accept only a particular BGP version, use the **neighbor version** command in router configuration mode. 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

ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
number	BGP version number. The version can be set to 2 to force the software to use only Version 2 with the specified neighbor. The default is to use Version 4 and dynamically negotiate down to Version 2 if requested.

Defaults

BGP Version 4

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Entering this command disables dynamic version negotiation.

Note The Cisco implementation of BGP in Cisco IOS Release 12.0(5)T or earlier releases supports BGP Versions 2, 3, and 4, with dynamic negotiation down to Version 2 if a neighbor does not accept BGP Version 4 (the default version).

The Cisco implementation of BGP in Cisco IOS Release 12.0(6)T or later releases supports BGP Version 4 only and does not support dynamic negotiation down to Version 2.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

Examples

The following example locks down to Version 4 of the BGP protocol:

```
router bgp 109
 neighbor 131.104.27.2 version 4
```

Related Commands

Command	Description
neighbor remote-as	Creates a BGP peer group.

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

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
number	Weight to assign. Acceptable values are from 0 to 65535.

Defaults

Routes learned through another BGP peer have a default weight of 0 and routes sourced by the local router have a default weight of 32768.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

All routes learned from this neighbor will have the assigned weight initially. The route with the highest weight will be chosen as the preferred route when multiple routes are available to a particular network.

The weights assigned with the **set weight** route-map command override the weights assigned using the **neighbor weight** command.

Note For weight changes to take effect, use of the **clear ip bgp peer-group *** command may be necessary.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

Examples

The following router configuration mode example sets the weight of all routes learned via 172.16.12.1 to 50:

```
router bgp 109
 neighbor 172.16.12.1 weight 50
```

The following address family configuration mode example sets the weight of all routes learned via 172.16.12.1 to 50:

```
router bgp 109
address-family ipv4 multicast
 neighbor 172.16.12.1 weight 50
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard Virtual Private Network (VPN) Version 4 address prefixes.
neighbor distribute-list	Distributes BGP neighbor information as specified in an access list.
neighbor filter-list	Sets up a BGP filter.
neighbor remote-as	Creates a BGP peer group.

network (BGP and multiprotocol BGP)

To specify the networks to be advertised by the Border Gateway Protocol (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*] [**route-map** *map-name*]

no network *network-number* [**mask** *network-mask*] [**route-map** *map-name*]

Syntax Description

network-number	Network that BGP or multiprotocol BGP will advertise.
mask	(Optional) Network or subnetwork mask. If the **mask** keyword is configured, then an exact match must exist in the routing table.
network-mask	(Optional) Network mask address.
route-map *map-name*	(Optional) Name of a route map.

Defaults

No networks are specified.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0	The limit of 200 network commands per BGP router was removed.
11.1(20)CC	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were added.
12.0(7)T	The **nlri unicast**, **nlri multicast**, and **nlri unicast multicast** keywords were removed. Address family configuration mode was added.

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0. The limit of 200 network commands per BGP router was removed in Cisco IOS Release 12.0. The maximum number of network commands you can use is now determined by the resources of the router, such as the amount of configured NVRAM or RAM.

For the information to be advertised by BGP or multiprotocol BGP, a route to the network specified must be present in the routing table. The routing information may be learned from connected routes, dynamic routing, and from static route sources.

Use the **route-map** keyword to apply a route map to a network to be advertised by the BGP and multiprotocol BGP routing processes. The specified route map can be used in filtering the network, or in setting attributes on the routes advertised by the **network** command.

Examples

The following example sets up network 10.108.0.0 to be included in the BGP updates:

```
router bgp 65000
 network 10.108.0.0
```

The following example sets up network 10.108.0.0 to be included in the multiprotocol BGP updates:

```
router bgp 65000
address family ipv4 multicast
 network 10.108.0.0
```

The following example shows the use of the **mask** keyword:

```
router bgp 65001
 network 10.0.0.0
 mask 255.0.0.0
  !
ip route 10.0.0.0 255.0.0.0 null0
```

Note This configuration will advertise a supernet 10.0.0.0/8. It is necessary to use a static route to provide the information because this summary route may not be learned through dynamic routing or from a connected interface. Specifying the null 0 interface with the **ip route** command guarantees that the routing information will always be present in the routing table.

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard Virtual Private Network (VPN) Version 4 address prefixes.
default-information originate (BGP)	Allows the redistribution of network 0.0.0.0 into BGP.
network backdoor	Specifies a backdoor route to a BGP-learned prefix that provides better information about the network.
router bgp	Configures the BGP routing process.

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

ip-address	IP address of the network to which you want a backdoor route.

Defaults

No network is marked as having a back door.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

A backdoor network is assigned an administrative distance of 200. The objective is to make Interior Gateway Protocol (IGP) learned routes preferred. A back door network is treated as a local network, except that it is not advertised. A network that is marked as a backdoor is not sourced by the local router, but should be learned from external neighbors. The BGP best path selection algorithm does not change when a network is configured as a back door.

Examples

The following address family configuration example configures network 10.108.0.0 as a local network and network 192.168.7.0 as a backdoor network:

```
router bgp 109
address-family ipv4 multicast
 network 10.108.0.0
 network 192.168.7.0 backdoor
```

The following router configuration example configures network 10.108.0.0 as a local network and network 192.168.7.0 as a backdoor network:

```
router bgp 109
 network 10.108.0.0
 network 192.168.7.0 backdoor
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
distance bgp	Allows the use of external, internal, and local administrative distances that could be a better route to a node.
network (BGP and multiprotocol BGP)	Specifies networks to be advertised by the BGP and multiprotocol BGP routing processes.
router bgp	Assigns an absolute weight to a BGP network.

router bgp

To configure the BGP routing process, use the **router bgp** command in global configuration mode. To remove a routing process, use the **no** form of this command.

router bgp *as-number*

no router bgp *as-number*

Syntax Description

as-number	Number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along.

Defaults

No BGP routing process is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command allows you to set up a distributed routing core that automatically guarantees the loop-free exchange of routing information between autonomous systems.

Examples

The following example configures a BGP process for autonomous system 120:

```
router bgp 120
```

Related Commands

Command	Description
network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP routing process.
timers bgp	Adjusts BGP network timers.

set as-path

To modify an autonomous system path for BGP routes, use the **set as-path** command in route-map configuration mode. 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.

Defaults

Autonomous system path is not modified.

Command Modes

Route-map configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

The only global BGP metric available to influence the best path selection is the autonomous system path length. By varying the length of the autonomous system path, a BGP speaker can influence the best path selection by a peer further away.

By allowing you to convert the tag into an autonomous system path, the **set as-path tag** variation of this command modifies the autonomous system length. The **set as-path prepend** variation allows you to "prepend" an arbitrary autonomous system path string to BGP routes. Usually the local autonomous system number is prepended multiple times, increasing the autonomous system path length.

Examples

The following example converts the tag of a redistributed route into an autonomous system path:

```
route-map set-as-path-from-tag
 set as-path tag
!
router bgp 100
 redistribute ospf 109 route-map set-as-path-from-tag
```

The following example prepends 100 100 100 to all the routes advertised to 10.108.1.1:

```
route-map set-as-path
 match as-path 1
 set as-path prepend 100 100 100
!
router bgp 100
 neighbor 10.108.1.1 route-map set-as-path out
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface (IP)	Distributes routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set origin (BGP)	Sets the BGP origin code.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

set comm-list delete

To remove communities from the community attribute of an inbound or outbound update, use the **set comm-list delete** command in route-map configuration mode. 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.

Defaults

No communities are removed.

Command Modes

Route-map configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

This **route-map** set command removes communities from the community attribute of an inbound or outbound update using a route map to filter and determine the communities to be deleted. Depending upon whether the route map is applied to the inbound or outbound update for a neighbor, each community that passes the route map **permit** clause and matches the given community list will be removed from the community attribute being received from or sent to the BGP neighbor.

Each entry of a standard community list should list only one community when used with the **set comm-list delete** command. For example, in order to be able to delete communities 10:10 and 10:20, you must use the following format to create the entries:

```
ip community-list 5 permit 10:10
ip community-list 5 permit 10:20
```

The following format for a community list entry, while acceptable otherwise, does not work with the **set comm-list delete** command:

```
config ip community-list 5 permit 10:10 10:20
```

When both the **set community** *community-list-number* and **set comm-list delete** commands are configured in the same sequence of a route map attribute, the deletion operation (**set comm-list delete**) is performed before the set operation (**set community** *community-list-number*).

Examples

In the following example, the communities 100:10 and 100:20 (if present) will be deleted from updates received from 171.69.233.33. Also, except for 100:50, all communities beginning with 100: will be deleted from updates sent to 171.69.233.33.

```
router bgp 100
 neighbor 171.69.233.33 remote-as 120
 neighbor 171.69.233.33 route-map ROUTEMAPIN in
 neighbor 171.69.233.33 route-map ROUTEMAPOUT out
!
ip community-list 1 permit 100:10
ip community-list 1 permit 100:20
!
ip community-list 120 deny   100:50
ip community-list 120 permit 100:.*
!
route-map ROUTEMAPIN permit 10
 set comm-list 1 delete
!
route-map ROUTEMAPOUT permit 10
 set comm-list 120 delete
```

Related Commands

Command	Description
set community	Sets the BGP communities attribute.

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	Specifies that 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	(Optional) Removes the community attribute from the prefixes that pass the route map.

Defaults

No BGP communities attributes exist.

Command Modes

Route-map configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

You must have a match clause (even if it points to a "permit everything" list) if you want to set tags.

Use the **route-map** global configuration command, and the **match** and **set** route map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route map configuration commands specify the redistribution *set actions* to be performed when all of the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

In the following example, routes that pass the autonomous system path access list 1 have the community set to 109. Routes that pass the autonomous system path access list 2 have the community set to no-export (these routes will not be advertised to any external BGP [eBGP] peers).

```
route-map set_community 10 permit
 match as-path 1
 set community 109

route-map set_community 20 permit
 match as-path 2
 set community no-export
```

In the following similar example, routes that pass the autonomous system path access list 1 have the community set to 109. Routes that pass the autonomous system path access list 2 have the community set to local-as (the router will not advertise this route to peers outside the local autonomous system.

```
route-map set_community 10 permit
 match as-path 1
 set community 109

route-map set_community 20 permit
 match as-path 2
 set community local-as
```

Related Commands

Command	Description
ip community-list	Creates a community list for BGP and control access to it.
match community	Matches a BGP community.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set comm-list delete	Removes communities from the community attribute of an inbound or outbound update.
show ip bgp community	Displays routes that belong to specified BGP communities.

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

half-life	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.
reuse	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.
suppress	Suppresses a route when its penalty exceeds this limit. The range is from 1 to 20000; the default is 2000.
max-suppress-time	Maximum time (in minutes) a route can be suppressed. The range is from 1 to 20000; the default is four times the *half-life* value. If the *half-life* value is allowed to default, the maximum suppress time defaults to 60 minutes.

Defaults

This command is disabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

When a BGP peer is reset, the route is withdrawn and the flap statistics cleared. In this instance, the withdrawal does not incur a penalty even though route flap dampening is enabled.

Examples

The following example sets the half life to 30 minutes, the reuse value to 1500, the suppress value to 10000; and the maximum suppress time to 120 minutes:

```
route-map tag
 match as path 10
 set dampening 30 1500 10000 120
!
router bgp 100
 neighbor 171.69.233.52 route-map tag in
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface (IP)	Distributes routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set origin (BGP)	Sets the BGP origin code.
set tag (IP)	Sets the value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.
show route-map	Displays all route maps configured or only the one specified.

set extcommunity

To set Border Gateway Protocol (BGP) extended community attributes, use the **set extcommunity** command in route-map configuration mode. To delete the entry, use the **no** form of this command.

set extcommunity {**rt** *extended-community-value* [**additive**] | **soo** *extended-community-value*}

no set extcommunity {**rt** *extended-community-value* [**additive**] | **soo** *extended-community-value*}

Syntax Description

rt	Specifies the route target (RT) extended community attribute.
soo	Specifies the site of origin (SOO) extended community attribute.
extended-community-value	Specifies the value to be set. The value can be one of the following combinations: • *autonomous-system-number*:*network-number* • *ip-address*:*network-number* The colon is used to separate the autonomous system number and network number or IP address and network number.
additive	(Optional) Adds a route target to the existing route target list without replacing any existing route targets.

Defaults

Specifying new route targets with the **rt** keyword replaces existing route targets by default, unless the **additive** keyword is used. The use of the **additive** keyword adds the new route target to the existing route target list but does not replace any existing route targets.

Command Modes

Route-map configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).

The **set extcommunity** command is used to configure set clauses that use extended community attributes in route maps. All of the standard rules of match and set clauses apply to the configuration of extended community attributes.

The route target (RT) extended community attribute is configured with the **rt** keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.

The site of origin (SOO) extended community attribute is configured with the **soo** keyword. This attribute uniquely identifies the site from which the Provider Edge (PE) router learned the route. All routes learned from a particular site must be assigned the same SOO extended community attribute, whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO can be applied to routes that are learned from VRFs. The SOO should not be configured for stub sites or sites that are not multihomed.

Examples

The following example sets the route target to extended community attribute 100:2 for routes that are permitted by the route map:

```
Router(config)# access-list 2 permit 192.168.78.0 255.255.255.0
Router(config)# route-map MAP_NAME permit 10
Router(config-route-map)# match ip-address 2
Router(config-route-map)# set extcommunity rt 100:2
```

The following example sets the route target to extended community attribute 100:3 for routes that are permitted by the route map. The use of the **additive** keyword adds route target 100:3 to the existing route target list but does not replace any existing route targets.

```
Router(config)# access-list 3 permit 192.168.79.0 255.255.255.0
Router(config)# route-map MAP_NAME permit 10
Router(config-route-map)# match ip-address 3
Router(config-route-map)# set extcommunity rt 100:3 additive
```

Note Configuring route targets with the **set extcommunity** command will replace existing route targets, unless the **additive** keyword is used.

The following example sets the site of origin to extended community attribute 100:4 for routes that are permitted by the route map:

```
Router(config)# access-list 4 permit 192.168.80.0 255.255.255.0
Router(config)# route-map MAP_NAME permit 10
Router(config-route-map)# match ip-address 4
Router(config-route-map)# set extcommunity soo 100:4
```

Related Commands

Command	Description
ip extcommunity-list	Creates an extended community list and controls access to it.
match extcommunity	Matches a BGP VPN extended community list.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
route-target	Creates a route target extended community for a VRF.
show ip extcommunity-list	Displays routes that are permitted by the extended community list.
show route-map	Displays all route maps configured or only the one specified.

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** command in route-map configuration mode. 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

ip-address	IP address of the next hop to which packets are output. The next hop must be an adjacent router.
peer-address	(Optional) Sets the next hop to be the BGP peering address.

Defaults

This command is disabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0	The **peer-address** keyword was added.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *ip-address* argument.

Use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for policy routing packets. The **ip policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which policy routing occurs. The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

If the interface associated with the first next hop specified with the **set ip next-hop** command is down, the optionally specified IP addresses are tried in turn.

When the **set ip next-hop** command is used with the **peer-address** keyword in an inbound route map of a BGP peer, the next hop of the received matching routes will be set to be the neighbor peering address, overriding any third-party next hops. So the same route map can be applied to multiple BGP peers to override third-party next hops.

When the **set ip next-hop** command is used with the **peer-address** keyword in an outbound route map of a BGP peer, the next hop of the advertised matching routes will be set to be the peering address of the local router, thus disabling the next hop calculation. The **set ip next-hop** command has finer granularity than the per-neighbor **neighbor next-hop-self** command, because you can set the next hop for some routes, but not others. The **neighbor next-hop-self** command sets the next hop for all routes sent to that neighbor.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ip next-hop**
2. **set interface**
3. **set ip default next-hop**
4. **set default interface**

Examples

In the following example, three routers are on the same FDDI LAN (with IP addresses 10.1.1.1, 10.1.1.2, and 10.1.1.3). Each is in a different autonomous system. The **set ip next-hop peer-address** command specifies that traffic from the router (10.1.1.3) in remote autonomous system 300 for the router (10.1.1.1) in remote autonomous system 100 that matches the route map is passed through the router bgp 200, rather than sent directly to the router (10.1.1.1) in autonomous system 100 over their mutual connection to the LAN.

```
router bgp 200
neighbor 10.1.1.3 remote-as 300
neighbor 10.1.1.3 route-map set-peer-address out
neighbor 10.1.1.1 remote-as 100
route-map set-peer-address permit 10
set ip next-hop peer-address
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
neighbor next-hop-self	Disables next hop processing of BGP updates on the router.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol to another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and that have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ip default next-hop verify-availability	Indicates 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.

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** command in route-map configuration mode. 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.

Defaults

This command is disabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

This command will cause BGP to advertise a MED value that corresponds to the IGP metric associated with the next hop of the route. This command applies to generated, internal BGP (iBGP)-, and eBGP-derived routes.

If this command is used, multiple BGP speakers in a common autonomous system can advertise different MED values for a particular prefix. Also, note that if the IGP metric changes, BGP will readvertise the route every 10 minutes.

Use the **route-map** global configuration command and the **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution *set actions* to be performed when all of the match criteria of the route map are met. When all match criteria are met, all set actions are performed.

Examples

In the following example, the MED value for all the advertised routes to neighbor 172.16.2.3 is set to the corresponding IGP metric of the next hop:

```
router bgp 109
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 200
 neighbor 172.16.2.3 route-map setMED out
!
route-map setMED permit 10
 match as-path 1
 set metric-type internal
!
 ip as-path access-list 1 permit .*
```

Related Commands

Command	Description
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

set origin (BGP)

To set the BGP origin code, use the **set origin** command in route-map configuration mode. 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.
as-number	Remote autonomous system number. This is an integer from 0 to 65535.
incomplete	Unknown heritage.

Defaults

Default origin, based on route in main IP routing table

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You must have a match clause (even if it points to a "permit everything" list) if you want to set tags.

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution *set actions* to be performed when all of the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

The following example sets the origin of routes that pass the route map to IGP:

```
route-map set_origin
 match as-path 10
 set origin igp
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community-list	Matches a BGP community.
match interface (IP)	Distributes routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value in a route map configuration.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets the value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

set weight

To specify the BGP weight for the routing table, use the **set weight** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set weight *number*

no set weight *number*

Syntax Description

number	Weight value. It can be an integer from 0 to 65535.

Defaults

The weight is not changed by the specified route map.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The implemented weight is based on the first matched autonomous system path. Weights indicated when an autonomous system path is matched override the weights assigned by global **neighbor** commands. In other words, the weights assigned with the **set weight** route-map configuration command override the weights assigned using the **neighbor weight** command.

Examples

The following example sets the BGP weight for the routes matching the autonomous system path access list to 200:

```
route-map set-weight
 match as-path 10
 set weight 200
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community-list	Matches a BGP community.
match interface (IP)	Distributes routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.

match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value in a route map configuration.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set origin (BGP)	Sets the BGP origin code.
set tag (IP)	Sets the value of the destination routing protocol.

show ip bgp

To display entries in the BGP routing table, use the **show ip bgp** command in EXEC mode.

show ip bgp [*network*] [*network-mask*] [**longer-prefixes**]

Syntax Description

network	(Optional) Network number, entered to display a particular network in the BGP routing table.
network-mask	(Optional) Displays all BGP routes matching the address and mask pair.
longer-prefixes	(Optional) Displays the route and more specific routes.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0	The display of prefix advertisement statistics was added.
12.0(6)T	The display of a message indicating support for route refresh capability was added.

Examples

The following is sample output from the **show ip bgp** command in privileged EXEC mode:

```
Router# show ip bgp

BGP table version is 5, local router ID is 10.0.33.34
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 1.0.0.0          0.0.0.0                  0         32768 ?
*  2.0.0.0          10.0.33.35              10             0 35 ?
*>                  0.0.0.0                  0         32768 ?
*  10.0.0.0         10.0.33.35              10             0 35 ?
*>                  0.0.0.0                  0         32768 ?
*> 192.168.0.0/16   10.0.33.35              10             0 35 ?
```

Table 32 describes the significant fields shown in the display.

Table 32 show ip bgp Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Table 32 show ip bgp Field Descriptions (continued)

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

The following is sample output from the **show ip bgp** command in privileged EXEC mode when you specify the **longer-prefixes** keyword:

```
Router# show ip bgp 172.16.0.0 255.255.0.0 longer-prefixes

BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 172.16.0.0       172.16.72.30        8896         32768 ?
*                   172.16.72.30                         0 109 108 ?
*> 172.16.1.0       172.16.72.30        8796         32768 ?
*                   172.16.72.30                         0 109 108 ?
*> 172.16.11.0      172.16.72.30       42482         32768 ?
*                   172.16.72.30                         0 109 108 ?
*> 172.16.14.0      172.16.72.30        8796         32768 ?
*                   172.16.72.30                         0 109 108 ?
*> 172.16.15.0      172.16.72.30        8696         32768 ?
*                   172.16.72.30                         0 109 108 ?
*> 172.16.16.0      172.16.72.30        1400         32768 ?
*                   172.16.72.30                         0 109 108 ?
*> 172.16.17.0      172.16.72.30        1400         32768 ?
*                   172.16.72.30                         0 109 108 ?
*> 172.16.18.0      172.16.72.30        8876         32768 ?
*                   172.16.72.30                         0 109 108 ?
*> 172.16.19.0      172.16.72.30        8876         32768 ?
*                   172.16.72.30                         0 109 108 ?
```

The following is sample output from the **show ip bgp** command in privileged EXEC mode, showing information for prefix 3.0.0.0:

```
Router# show ip bgp 3.0.0.0
BGP routing table entry for 3.0.0.0/8, version 628
Paths: (1 available, best #1)
Advertised to peer-groups:
 ebgp
Advertised to non peer-group peers:
 171.69.232.162
109 65000 297 701 80
 171.69.233.56 from 171.69.233.56 (172.19.185.32)
  Origin incomplete, localpref 100, valid, external, best, ref 2
```

Note If a prefix has not been advertised to any peer, the display shows “Not advertised to any peer.”

Related Commands

Command	Description
neighbor maximum-prefix	Resets a BGP connection or session.
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.

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** command in EXEC mode.

show ip bgp cidr-only

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show ip bgp cidr-only** command in privileged EXEC mode:

```
Router# show ip bgp cidr-only

BGP table version is 220, local router ID is 172.16.73.131
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 192.168.0.0/8    172.16.72.24                         0 1878 ?
*> 172.16.0.0/16    172.16.72.30                         0 108 ?
```

Table 33 describes the significant fields shown in the display.

Table 33 show ip bgp cidr-only Field Descriptions

Field	Description
BGP table version is 220	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.

Table 33 show ip bgp cidr-only Field Descriptions (continued)

Field	Description
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the access server has some non-BGP route to this network.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a **network** router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

show ip bgp community

To display routes that belong to specified BGP communities, use the **show ip bgp community** command in EXEC mode.

show ip bgp community *community-number* [**exact**]

Syntax Description

community-number	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.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.0	The **local-as** community was added.

Examples

The following is sample output from the **show ip bgp community** command in privileged EXEC mode:

```
router# show ip bgp community 111:12345 local-as

 BGP table version is 10, local router ID is 224.0.0.10
 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
 Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop          Metric LocPrf Weight Path
 *> 172.16.2.2/32    172.43.222.2           0             0 222 ?
 *> 10.0.0.0         172.43.222.2           0             0 222 ?
 *> 172.43.0.0       172.43.222.2           0             0 222 ?
 *> 172.43.44.44/32  172.43.222.2           0             0 222 ?
 *  172.43.222.0/24  172.43.222.2           0             0 222 i
 *> 172.17.240.0/21  172.43.222.2           0             0 222 ?
 *> 192.168.212.0    172.43.222.2           0             0 222 i
 *> 172.39.1.0       172.43.222.2           0             0 222 ?
```

Table 34 describes the significant fields shown in the display.

Table 34 show ip bgp community Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Table 34 show ip bgp community Field Descriptions (continued)

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show ip bgp community-list

To display routes that are permitted by the BGP community list, use the **show ip bgp community-list** command in EXEC mode.

show ip bgp community-list *community-list-number* [**exact**]

Syntax Description

community-list-number	Community list number in the range from 1 to 99.
exact	(Optional) Displays only routes that have an exact match.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.

Examples

The following is sample output of the **show ip bgp community-list** command in privileged EXEC mode:

```
Router# show ip bgp community-list 20

BGP table version is 716977, local router ID is 193.0.32.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop         Metric LocPrf Weight Path
* i3.0.0.0          193.0.22.1            0    100      0 1800 1239 ?
*>i                 193.0.16.1            0    100      0 1800 1239 ?
* i6.0.0.0          193.0.22.1            0    100      0 1800 690 568 ?
*>i                 193.0.16.1            0    100      0 1800 690 568 ?
* i7.0.0.0          193.0.22.1            0    100      0 1800 701 35 ?
*>i                 193.0.16.1            0    100      0 1800 701 35 ?
*                   172.16.72.24                        0 1878 704 701 35 ?
* i8.0.0.0          193.0.22.1            0    100      0 1800 690 560 ?
*>i                 193.0.16.1            0    100      0 1800 690 560 ?
*                   172.16.72.24                        0 1878 704 701 560 ?
* i13.0.0.0         193.0.22.1            0    100      0 1800 690 200 ?
*>i                 193.0.16.1            0    100      0 1800 690 200 ?
*                   172.16.72.24                        0 1878 704 701 200 ?
* i15.0.0.0         193.0.22.1            0    100      0 1800 174 ?
*>i                 193.0.16.1            0    100      0 1800 174 ?
* i16.0.0.0         193.0.22.1            0    100      0 1800 701 i
*>i                 193.0.16.1            0    100      0 1800 701 i
*                   172.16.72.24                        0 1878 704 701 i
```

Table 35 describes the significant fields shown in the display.

Table 35 show ip bgp community list Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show ip bgp dampened-paths

To display BGP dampened routes, use the **show ip bgp dampened-paths** command in EXEC mode.

show ip bgp dampened-paths

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Examples

The following is sample output from the **show ip bgp dampened-paths** command in privileged EXEC mode:

```
Router# show ip bgp dampened-paths

BGP table version is 10, local router ID is 171.69.232.182
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From             Reuse   Path
*d 10.0.0.0         171.69.232.177   00:18:4 100 ?
*d 12.0.0.0         171.69.232.177   00:28:5 100 ?
```

Table 36 describes the significant fields shown in the display.

Table 36 show ip bgp dampened-paths Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router	IP address of the router where route dampening is enabled.
*d	Route to the network indicated is dampened.
From	IP address of the peer that advertised this path.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear ip bgp dampening	Clears BGP route dampening information and unsuppresses the suppressed routes.

show ip bgp filter-list

To display routes that conform to a specified filter list, use the **show ip bgp filter-list** command in EXEC mode.

show ip bgp filter-list *access-list-number*

Syntax Description

access-list-number	Number of an autonomous system path access list. It can be a number from 1 to 199.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show ip bgp filter-list** command in privileged EXEC mode:

```
Router# show ip bgp filter-list 2

BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*  172.16.0.0       172.16.72.30                         0 109 108 ?
*  172.16.1.0       172.16.72.30                         0 109 108 ?
*  172.16.11.0      172.16.72.30                         0 109 108 ?
*  172.16.14.0      172.16.72.30                         0 109 108 ?
*  172.16.15.0      172.16.72.30                         0 109 108 ?
*  172.16.16.0      172.16.72.30                         0 109 108 ?
*  172.16.17.0      172.16.72.30                         0 109 108 ?
*  172.16.18.0      172.16.72.30                         0 109 108 ?
*  172.16.19.0      172.16.72.30                         0 109 108 ?
*  172.16.24.0      172.16.72.30                         0 109 108 ?
*  172.16.29.0      172.16.72.30                         0 109 108 ?
*  172.16.30.0      172.16.72.30                         0 109 108 ?
*  172.16.33.0      172.16.72.30                         0 109 108 ?
*  172.16.35.0      172.16.72.30                         0 109 108 ?
*  172.16.36.0      172.16.72.30                         0 109 108 ?
*  172.16.37.0      172.16.72.30                         0 109 108 ?
*  172.16.38.0      172.16.72.30                         0 109 108 ?
*  172.16.39.0      172.16.72.30                         0 109 108 ?
```

Table 37 describes the significant fields shown in the display.

Table 37 show ip bgp filter-list Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP route to this network.
Metric	If shown, this is the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a **network** router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

show ip bgp flap-statistics

To display BGP flap statistics, use the **show ip bgp flap-statistics** command in EXEC mode.

show ip bgp flap-statistics [{**regexp** *regexp*} | {**filter-list** *access-list*} | {*ip-address mask* [**longer-prefix**]}]

Syntax Description

regexp *regexp*	(Optional) Clears flap statistics for all the paths that match the regular expression.
filter-list *access-list*	(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.
mask	(Optional) Network mask applied to the value.
longer-prefix	(Optional) Displays flap statistics for more specific entries.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

If no arguments or keywords are specified, the router displays flap statistics for all routes.

Examples

The following is sample output from the **show ip bgp flap-statistics** command in privileged EXEC mode:

```
Router# show ip bgp flap-statistics

BGP table version is 10, local router ID is 171.69.232.182
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From            Flaps Duration Reuse    Path
*d 10.0.0.0         171.69.232.177  4     00:13:31 00:18:10 100
*d 12.0.0.0         171.69.232.177  4     00:02:45 00:28:20 100
```

Table 38 describes the significant fields shown in the display.

Table 38 show ip bgp flap-statistics Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router where route dampening is enabled.
Network	Route to the network indicated is dampened.

Table 38 show ip bgp flap-statistics Field Descriptions (continued)

Field	Description
From	IP address of the peer that advertised this path.
Flaps	Number of times the route has flapped.
Duration	Time (in hours:minutes:seconds) since the router noticed the first flap.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear ip bgp flap-statistics	Clears BGP flap statistics.

show ip bgp inconsistent-as

To display routes with inconsistent originating autonomous systems, use the **show ip bgp inconsistent-as** command in EXEC mode.

show ip bgp inconsistent-as

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Examples

The following is sample output from the **show ip bgp inconsistent-as** command in privileged EXEC mode:

```
Router# show ip bgp inconsistent-as

BGP table version is 87, local router ID is 172.19.82.53
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*  11.0.0.0         171.69.232.55          0             0 300 88 90 99 ?
*>                  171.69.232.52       2222             0 400 ?
*  171.69.0.0       171.69.232.55          0             0 300 90 99 88 200 ?
*>                  171.69.232.52       2222             0 400 ?
*  200.200.199.0    171.69.232.55          0             0 300 88 90 99 ?
*>                  171.69.232.52       2222             0 400 ?
```

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.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

The following is sample output from the **show ip bgp ipv4 unicast** command:

```
Router# show ip bgp ipv4 unicast

 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24   172.16.10.1             0             0  300 i
*> 10.10.20.0/24   172.16.10.1             0             0  300 i
*  10.20.10.0/24   172.16.10.1             0             0  300 i
```

The following is sample output from the **show ip bgp ipv4 multicast** command:

```
Router# show ip bgp ipv4 multicast

 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24   172.16.10.1             0             0  300 i
*> 10.10.20.0/24   172.16.10.1             0             0  300 i
*  10.20.10.0/24   172.16.10.1             0             0  300 i
```

Table 39 describes the significant fields shown in the display.

Table 39 show ip bgp ipv4 unicast Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Table 39 show ip bgp ipv4 unicast Field Descriptions (continued)

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is damped. h—The table entry history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is displayed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

Related Commands

Command	Description
show ip bgp	Displays entries in the BGP routing table.

show ip bgp neighbors

To display information about the TCP and BGP connections to neighbors, use the **show ip bgp neighbors** command in EXEC mode.

show ip bgp neighbors [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | {**paths** *regexp*} | **dampened-routes**]

Syntax Description

neighbor-address	(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 *regexp*	(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.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.2	The **received-routes** keyword was added.

Examples

The following is sample output from the **show ip bgp neighbors** command in privileged EXEC mode:

```
Router# show ip bgp neighbors 172.16.232.178

BGP neighbor is 172.16.232.178,  remote AS 35, external link
  BGP version 4, remote router ID 192.168.3.3
  BGP state = Established, up for 1w1d
  Last read 00:00:53, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 Multicast: advertised and received
  Received 12519 messages, 0 notifications, 0 in queue
  Sent 12523 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor
  Inbound path policy configured
  Outbound path policy configured
```

```
  Route map for incoming advertisements is uni-in
  Route map for outgoing advertisements is uni-out
  3 accepted prefixes consume 108 bytes
  Prefix advertised 6, suppressed 0, withdrawn 0

 For address family: IPv4 Multicast
  BGP table version 5, neighbor version 5
  Index 1, Offset 0, Mask 0x2
  Inbound path policy configured
  Outbound path policy configured
  Route map for incoming advertisements is mul-in
  Route map for outgoing advertisements is mul-out
  3 accepted prefixes consume 108 bytes
  Prefix advertised 6, suppressed 0, withdrawn 0

  Connections established 2; dropped 1
  Last reset 1w1d, due to Peer closed the session
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 172.16.232.178, Local port: 179
Foreign host: 172.16.232.179, Foreign port: 11002

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x2CF49CF8):
Timer          Starts    Wakeups            Next
Retrans         12518          0             0x0
TimeWait            0          0             0x0
AckHold         12514      12281             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss:  273358651  snduna:  273596614  sndnxt:  273596614     sndwnd:  15434
irs:  190480283  rcvnxt:  190718186  rcvwnd:      15491  delrcvwnd:    893

SRTT: 300 ms, RTTO: 607 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs

Datagrams (max data segment is 1460 bytes):
Rcvd: 24889 (out of order: 0), with data: 12515, total data bytes: 237921
Sent: 24963 (retransmit: 0), with data: 12518, total data bytes: 237981
```

Table 40 describes the significant fields shown in the display.

Table 40 show ip bgp neighbors Field Descriptions

Field	Description
BGP neighbor	IP address of the BGP neighbor and its autonomous system number. If the neighbor is in the same autonomous system as the router, then the link between them is internal; otherwise, it is considered external.
remote AS	Autonomous system of the neighbor.
external link	Indicates that this peer is an external BGP (eBGP) peer.
BGP version	BGP version being used to communicate with the remote router; the router ID (an IP address) of the neighbor is also specified.
remote router ID	IP address of the neighbor.
BGP state	Internal state of this BGP connection.
up for	Amount of time that the underlying TCP connection has been in existence.
Last read	Time that BGP last read a message from this neighbor.
hold time	Maximum amount of time that can elapse between messages from the peer.
keepalive interval	Time period between sending keepalive packets, which help ensure that the TCP connection is up.
Neighbor capabilities	BGP capabilities advertised and received from this neighbor.
Route refresh	Indicates that the neighbor supports dynamic soft reset using the route refresh capability.
Address family IP Version 4 Unicast:	IP Version 4 unicast-specific properties of this neighbor.
Address family IP Version 4 Multicast:	IP Version 4 multicast-specific properties of this neighbor.
Received	Number of total BGP messages received from this peer, including keepalives.
notifications	Number of error messages received from the peer.
Sent	Total number of BGP messages that have been sent to this peer, including keepalives.
notifications	Number of error messages the router has sent to this peer.
Route refresh request:	Number of route refresh requests sent and received from this neighbor.
advertisement runs	Value of minimum advertisement interval.
For address family:	Address family to which the following fields refer.
BGP table version	Indicates that the neighbor has been updated with this version of the primary BGP routing table.
neighbor version	Number used by the software to track the prefixes that have been sent and those that must be sent to this neighbor.
Community attribute	Appears if the **neighbor send-community** command is configured for this neighbor.
Inbound path policy	Indicates if an inbound policy is configured.
Outbound path policy	Indicates if an outbound policy is configured.
mul-in	Name of inbound route map for the multicast address family.

Table 40 show ip bgp neighbors Field Descriptions (continued)

Field	Description
mul-out	Name of outbound route map for the multicast address family.
accepted prefixes	Number of prefixes accepted.
Prefix advertised	Number of prefixes advertised.
suppressed	Number of prefixes suppressed.
withdrawn	Number of prefixes withdrawn.
Connections established	Number of times the router has established a TCP connection and the two peers have agreed to speak BGP with each other.
dropped	Number of times that a good connection has failed or been taken down.
Last reset	Elapsed time since this peering session was last reset.
Connection state	State of BGP peer.
unread input bytes	Number of bytes of packets still to be processed.
Local host, Local port	Peering address of local router, plus port.
Foreign host, Foreign port	Peering address of the neighbor.
Event Timers	Table displays the number of starts and wakeups for each timer.
iss	Initial send sequence number.
snduna	Last send sequence number the local host sent but has not received an acknowledgment for.
sndnxt	Sequence number the local host will send next.
sndwnd	TCP window size of the remote host.
irs	Initial receive sequence number.
rcvnxt	Last receive sequence number the local host has acknowledged.
rcvwnd	TCP window size of the local host.
delrecvwnd	Delayed receive window—data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is larger than a full-sized packet, at which point it is applied to the rcvwnd field.
SRTT	A calculated smoothed round-trip timeout.
RTTO	Round-trip timeout.
RTV	Variance of the round-trip time.
KRTT	New round-trip timeout (using the Karn algorithm). This field separately tracks the round-trip time of packets that have been resent.
minRTT	Smallest recorded round-trip timeout (hard wire value used for calculation).
maxRTT	Largest recorded round-trip timeout.
ACK hold	Time the local host will delay an acknowledgment in order to piggyback data on it.
Flags	IP precedence of the BGP packets.
Datagrams: Rcvd	Number of update packets received from a neighbor.

Table 40 show ip bgp neighbors Field Descriptions (continued)

Field	Description
with data	Number of update packets received with data.
total data bytes	Total bytes of data.
Sent	Number of update packets sent.
with data	Number of update packets with data sent.
total data bytes	Total number of data bytes.

The following is sample output from the **show ip bgp neighbors** command with the **advertised-routes** keyword in privileged EXEC mode:

```
Router# show ip bgp neighbors 172.16.232.178 advertised-routes

BGP table version is 27, local router ID is 172.16.232.181
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*>i110.0.0.0        172.16.232.179         0    100      0 ?
*> 200.2.2.0        0.0.0.0                0         32768 i
```

The following is sample output from the **show ip bgp neighbors** command with the **routes** keyword in privileged EXEC mode:

```
Router# show ip bgp neighbors 172.16.232.178 routes

BGP table version is 27, local router ID is 172.16.232.181
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 10.0.0.0         172.16.232.178        40             0 10 ?
*> 10.2.0.0         172.16.232.178        40             0 10 ?
```

Table 41 describes the significant fields shown in the displays.

Table 41 show ip bgp neighbors advertised-routes and routes Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

The following is sample output from the **show ip bgp neighbors** command with the **paths** keyword in privileged EXEC mode:

```
Router# show ip bgp neighbors 171.69.232.178 paths ^10

Address    Refcount Metric Path
0x60E577B0        2     40 10 ?
```

Table 42 describes the significant fields shown in the display.

Table 42 show ip bgp neighbors paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Refcount	Number of routes using that path.
Metric	The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	The autonomous system path for that route, followed by the origin code for that route.

show ip bgp paths

To display all the BGP paths in the database, use the **show ip bgp paths** command in EXEC mode.

show ip bgp paths

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show ip bgp paths** command in privileged EXEC mode:

```
Router# show ip bgp paths

Address    Hash Refcount Metric Path
0x60E5742C    0        1      0 i
0x60E3D7AC    2        1      0 ?
0x60E5C6C0   11        3      0 10 ?
0x60E577B0   35        2     40 10 ?
```

Table 43 describes the significant fields shown in the display.

Table 43 show ip bgp paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Hash	Hash bucket where path is stored.
Refcount	Number of routes using that path.
Metric	The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	The autonomous system path for that route, followed by the origin code for that route.

show ip bgp peer-group

To display information about BGP peer groups, use the **show ip bgp peer-group** command in EXEC mode.

show ip bgp peer-group [*peer-group-name*] [**summary**]

Syntax Description

peer-group-name	(Optional) Displays information about that specific peer group.
summary	(Optional) Displays a summary of the status of all the members of a peer group.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Examples

The following is sample output from **show ip bgp peer-group** command for a peer group named internal in privileged EXEC mode:

```
Router# show ip bgp peer-group internal

BGP peer-group is internal, remote AS 100
  BGP version 4
  Minimum time between advertisement runs is 5 seconds

 For address family:IPv4 Unicast
  BGP neighbor is internal, peer-group internal, members:
           10.1.1.1         10.1.1.2
  Index 3, Offset 0, Mask 0x8
  Incoming update AS path filter list is 53
  Outgoing update AS path filter list is 54
  Route map for incoming advertisements is MAP193
  Route map for outgoing advertisements is MAP194
  Update messages formatted 0, replicated 0
```

show ip bgp regexp

To display routes matching the autonomous system path regular expression, use the **show ip bgp regexp** command in EXEC mode.

show ip bgp regexp *regexp*

Syntax Description

regexp	Regular expression to match the BGP autonomous system paths.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show ip bgp regexp** command in privileged EXEC mode:

```
Router# show ip bgp regexp 108$

BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*  172.16.0.0       172.16.72.30                         0 109 108 ?
*  172.16.1.0       172.16.72.30                         0 109 108 ?
*  172.16.11.0      172.16.72.30                         0 109 108 ?
*  172.16.14.0      172.16.72.30                         0 109 108 ?
*  172.16.15.0      172.16.72.30                         0 109 108 ?
*  172.16.16.0      172.16.72.30                         0 109 108 ?
*  172.16.17.0      172.16.72.30                         0 109 108 ?
*  172.16.18.0      172.16.72.30                         0 109 108 ?
*  172.16.19.0      172.16.72.30                         0 109 108 ?
*  172.16.24.0      172.16.72.30                         0 109 108 ?
*  172.16.29.0      172.16.72.30                         0 109 108 ?
*  172.16.30.0      172.16.72.30                         0 109 108 ?
*  172.16.33.0      172.16.72.30                         0 109 108 ?
*  172.16.35.0      172.16.72.30                         0 109 108 ?
*  172.16.36.0      172.16.72.30                         0 109 108 ?
*  172.16.37.0      172.16.72.30                         0 109 108 ?
*  172.16.38.0      172.16.72.30                         0 109 108 ?
*  172.16.39.0      172.16.72.30                         0 109 108 ?
```

show ip bgp summary

To display the status of all BGP connections, use the **show ip bgp summary** command in EXEC mode.

show ip bgp summary

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0	The PfxRcd and Admin fields were added to the output.

Examples

The following is sample output from the **show ip bgp summary** command in privileged EXEC mode:

```
Router# show ip bgp summary

BGP router identifier 172.16.1.1, local AS number 100
BGP table version is 199, main routing table version 199
37 network entries and 59 paths using 5713 bytes of memory
18 BGP path attribute entries using 936 bytes of memory
10 BGP AS-PATH entries using 240 bytes of memory
7 BGP community entries using 168 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
36 received paths for inbound soft reconfiguration
BGP activity 37/2849 prefixes, 60/1 paths, scan interval 15 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down State/PfxRcd
10.100.1.1      4   200      26      22      199    0    0 00:14:23 23
10.200.1.1      4   300      21      51      199    0    0 00:13:40 0
```

Table 44 describes the significant fields shown in the display.

Table 44 show ip bgp summary Field Descriptions

Field	Description
BGP router identifier	In order of precedence and availability, router identifier specified by the **bgp router-id** command, loopback address, or lowest IP address.
BGP table version	Internal version number of BGP database.
main routing table version	Last version of BGP database that was injected into the main routing table.
Neighbor	IP address of a neighbor.
V	BGP version number spoken to that neighbor.
AS	Autonomous system.

Table 44 show ip bgp summary Field Descriptions (continued)

Field	Description
MsgRcvd	BGP messages received from that neighbor.
MsgSent	BGP messages sent to that neighbor.
TblVer	Last version of the BGP database that was sent to that neighbor.
InQ	Number of messages from that neighbor waiting to be processed.
OutQ	Number of messages waiting to be sent to that neighbor.
Up/Down	The length of time that the BGP session has been in the Established state, or the current state if it is not Established.
State/PfxRcd	Current state of the BGP session/the number of prefixes the router has received from a neighbor or peer group. When the maximum number (as set by the **neighbor maximum-prefix** command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is Idle. An (Admin) entry with Idle status indicates that the connection has been shut down using the **neighbor shutdown** command.

Related Commands

Command	Description
neighbor maximum-prefix	Controls how many prefixes can be received from a neighbor.
neighbor shutdown	Disables a neighbor or peer group.
show ip bgp summary	Displays the status of all BGP connections.

show ip extcommunity-list

To display routes that are permitted by an extended community list, use the **show ip extcommunity-list** command in EXEC mode.

show ip extcommunity-list [*community-list-number*]

Syntax Description

community-list-number	(Optional) Community list number in the range from 1 to 199. A standard extended list is from 1 to 99. An expanded extended list is from 100 to 199.

Defaults

If a specific extended community list number is not specified when the **show ip extcommunity-list** command is entered, all locally configured extended community lists will be displayed by default.

Command Modes

EXEC

Command History

Release	Modification
12.1	This command was introduced.

Examples

The following is sample output from the **show ip extcommunity-list** command in EXEC mode:

```
Router# show ip extcommunity-list

Extended community standard list 1
     permit RT:901:10
     permit SoO:802:20
     deny RT:703:30 SoO:604:40
Extended community standard list 99
     permit RT:604:40 SoO:505:50
     deny RT:406:60 SoO:307:70
```

Related Commands

Command	Description
show route-map	Displays configured route maps.

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.
prefix-list-name	(Optional) The name of a specific prefix list.
network/length	(Optional) The network number and length (in bits) of the network mask.
seq	(Optional) Applies the sequence number to the prefix list entry.
sequence-number	(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 *network/length.*
first-match	(Optional) Displays the entry of a prefix list that matches the given *network/length*.

Command Modes

EXEC

Command History

Release	Modification
12.0	This command was introduced.

Examples

The following example shows the output of the **show ip prefix-list** command with details about the prefix list named test in privileged EXEC mode:

```
Router# show ip prefix-list detail test

ip prefix-list test:
Description: test-list
 count: 1, range entries: 0, sequences: 10 - 10, refcount: 3
 seq 10 permit 35.0.0.0/8 (hit count: 0, refcount: 1)
```

Related Commands

Command	Description
clear ip prefix-list	Resets the hit count of the prefix list entries.
distribute-list in	Filters networks received in updates.
distribute-list out	Suppresses networks from being advertised in updates.
ip prefix-list	Creates an entry in a prefix list.
ip prefix-list description	Adds a text description of a prefix list.

match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
neighbor prefix-list	Distributes BGP neighbor information as specified in a prefix list.

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.

Defaults

The behavior of this command is enabled by default.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

Usually, a BGP speaker does not advertise a route to an external neighbor unless that route is local or exists in the IGP. The **no synchronization** command allows the Cisco IOS software to advertise a network route without waiting for the IGP. This feature allows routers and access servers within an autonomous system to have the route before BGP makes it available to other autonomous systems.

Use the **synchronization** command if routers in the autonomous system do not speak BGP.

Examples

The following router configuration mode example enables a router to advertise a network route without waiting for IGP:

```
router bgp 120
 no synchronization
```

The following address family configuration mode example enables a router to advertise a network route without waiting for IGP:

```
router bgp 120
address-family ipv4 unicast
 no synchronization
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.

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

map-name	Route map name, from the **route-map** command.

Defaults

This command is disabled by default.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

This command adds the route map name defined by the **route-map** command to the IP routing table. This command is used to set the tag name and the route metric to implement redistribution.

You can use **match** clauses of route maps in the **table-map** command. IP access list, autonomous system paths, and next hop match clauses are supported.

Examples

In the following router configuration mode example, the Cisco IOS software is configured to automatically compute the tag value for the BGP learned routes and to update the IP routing table:

```
route-map tag
 match as path 10
 set automatic-tag
!
router bgp 100
 table-map tag
```

In the following address family configuration mode example, the Cisco IOS software is configured to automatically compute the tag value for the BGP learned routes and to update the IP routing table:

```
route-map tag
 match as path 10
 set automatic-tag
!
router bgp 100
address-family ipv4 unicast
 table-map tag
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
match as-path	Matches a BGP autonomous system path access list.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

timers bgp

To adjust BGP network timers, use the **timers bgp** command in router configuration mode. To reset the BGP timing defaults, use the **no** form of this command.

timers bgp *keepalive holdtime*

no timers bgp

Syntax Description

keepalive	Frequency (in seconds) with which the Cisco IOS software sends *keepalive* messages to its peer. The default is 60 seconds.
holdtime	Interval (in seconds) after not receiving a *keepalive* message that the software declares a peer dead. The default is 180 seconds.

Defaults

keepalive: 60 seconds

holdtime: 180 seconds

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.

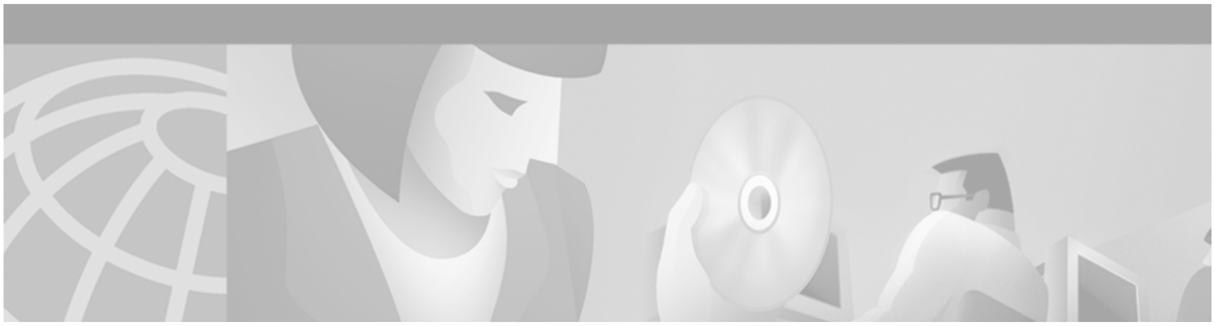
Examples

The following example changes the keepalive timer to 70 seconds and the hold-time timer to 210 seconds:

```
timers bgp 70 210
```

Related Commands

Command	Description
clear ip bgp peer-group	Removes all the members of a BGP peer group.
router bgp	Configures the BGP routing process.
show ip bgp	Displays entries in the BGP routing table.



Multiprotocol BGP Extensions for IP Multicast Commands

Use the commands in this chapter to configure and monitor multiprotocol BGP. Multiprotocol BGP is based on RFC 2283, *Multiprotocol Extensions for BGP-4*. For multiprotocol BGP configuration information and examples, refer to the "Configuring Multiprotocol BGP Extensions for IP Multicast" chapter of the *Cisco IOS IP Configuration Guide*. For BGP configuration information and examples, refer to the "Configuring BGP" chapter of the *Cisco IOS IP Configuration Guide*. For BGP command descriptions, refer to the "BGP Commands" chapter of this document.

Commands in this chapter that have been replaced by new or existing commands are no longer documented. Table 45 maps the previous commands to their replacements.

Table 45 Mapping Previous Commands to Replacement Commands

Old Command	Replacement Command
distance mbgp	**distance bgp**
match nlri	**address-family ipv4** **address-family vpnv4**
set nlri	**address-family ipv4** or **address-family vpnv4**
show ip mbgp	**show ip bgp ipv4 multicast**
show ip mbgp summary	**show ip bgp ipv4 multicast summary**

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** command in router configuration mode. 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

multicast	(Optional) Specifies IP Version 4 multicast address prefixes.
unicast	(Optional) Specifies IP Version 4 unicast address prefixes.
vrf *vrf-name*	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance to associate with subsequent IP Version 4 address family configuration mode commands.

Defaults

IP Version 4 address prefixes are not enabled. Unicast address prefixes are the default when IP Version 4 address prefixes are configured.

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

The **address-family ipv4** command places the router in address family configuration mode (prompt: `config-router-af`), from which you can configure routing sessions that use standard IP Version 4 address prefixes. To leave address family configuration mode and return to router configuration mode, type **exit**.

Routing information for address family IP Version 4 is advertised by default when you configure a BGP routing session using the **neighbor remote-as** command unless you enter the **no bgp default ipv4-unicast** command.

The **address-family ipv4** command replaces the **match nlri** and **set nlri** commands.

Examples

The following example places the router in address family configuration mode for the IP Version 4 address family:

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv4
Router(config-router-af)#
```

The following example places the router in address family configuration mode and specifies multicast address prefixes for the IP Version 4 address family:

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv4 multicast
Router(config-router-af)#
```

The following example places the router in address family configuration mode and specifies unicast address prefixes for the IP Version 4 address family:

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv4 unicast
Router(config-router-af)#
```

The following example places the router in address family configuration mode and specifies cisco as the name of the VRF instance to associate with subsequent IP Version 4 address family configuration mode commands:

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf cisco
Router(config-router-af)#
```

Use this form of the command, which specifies a VRF, only to configure routing exchanges between provider edge (PE) and customer edge (CE) devices.

Related Commands

Command	Description
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
neighbor activate	Enables the exchange of information with a BGP neighboring router.

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** command in router configuration mode. 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.

Defaults

VPN Version 4 address prefixes are not enabled. Unicast address prefixes are the default when VPN Version 4 address prefixes are configured.

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

The **address-family vpnv4** command places the router in address family configuration mode (prompt: `config-router-af`), from which you can configure routing sessions that use VPN Version 4 address prefixes. To leave address family configuration mode and return to router configuration mode, type **exit**.

The **address-family vpnv4** command replaces the **match nlri** and **set nlri** commands.

Examples

The following example places the router in address family configuration mode for the VPN Version 4 address family:

```
Router(config)# router bgp 100
(config-router)# address-family vpnv4
(config-router-af)#
```

The following example places the router in address family configuration mode for the unicast VPN Version 4 address family:

```
Router(config)# router bgp 100
(config-router)# address-family vpnv4 unicast
(config-router-af)#
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
neighbor activate	Enables the exchange of information with a BGP neighboring router.

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** command in interface configuration mode. (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

metric	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 *map-name*	(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 *access-list-number*	(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.
protocol	(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.
process-id	(Optional) Process ID number of the unicast routing protocol.
dvmrp	(Optional) Allows routes from the DVMRP routing table to be advertised with the configured *metric* value, or filtered.

Defaults

No metric is preconfigured. Only directly connected subnets and networks are advertised to neighboring DVMRP routers.

Command Modes

Interface configuration

Command History

Release	Modification
10.2	This command was introduced.
11.1	The **route-map** keyword was added.
11.1(20)CC	This **mbgp** keyword was added.
12.0(7)T	This **mbgp** keyword was added.

Usage Guidelines

When Protocol Independent Multicast (PIM) is configured on an interface and DVMRP neighbors are discovered, the Cisco IOS software sends DVMRP report messages for directly connected networks. The **ip dvmrp metric** command enables DVMRP report messages for multicast destinations that match the access list. Usually, the metric for these routes is 1. Under certain circumstances, you might want to tailor the metric used for various unicast routes. This command lets you configure the metric associated with a set of destinations for report messages sent out this interface.

You can use the *access-list-number* argument in conjunction with the *protocol* and *process-id* arguments to selectively list the destinations learned from a given routing protocol.

To display DVMRP activity, use the **debug ip dvmrp** command.

Examples

The following example connects a PIM cloud to a DVMRP cloud. Access list 1 permits the sending of DVMRP reports to the DVMRP routers advertising all sources in the 172.16.35.0 network with a metric of 1. Access list 2 permits all other destinations, but the metric of 0 means that no DVMRP reports are sent for these destinations.

```
access-list 1 permit 172.16.35.0 0.0.0.255
access-list 1 deny 0.0.0.0 255.255.255.255
access-list 2 permit 0.0.0.0 255.255.255.255
interface tunnel 0
 ip dvmrp metric 1 list 1
 ip dvmrp metric 0 list 2
```

The following example redistributes IP Version 4 multicast routes into DVMRP neighbors with a metric of 1:

```
interface tunnel 0
 ip dvmrp metric 1 mbgp
```

Related Commands

Command	Description
debug ip dvmrp	Displays information on DVMRP packets received and sent.
ip dvmrp accept-filter	Configures an acceptance filter for incoming DVMRP reports.

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.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
11.1(20)CC	The **rtp** keyword was added.
12.0(7)T	The **rtp** keyword was added.

Usage Guidelines

You can store IP Version 4 multicast packet headers in a cache and then display them to determine the following information:

- Who is sending IP multicast packets to which groups
- Interpacket delay
- Duplicate IP multicast packets (if any)
- Multicast forwarding loops in your network (if any)
- Scope of the group
- User Datagram Protocol (UDP) port numbers
- Packet length

Note This feature allocates a circular buffer of approximately 32 KB. Do not configure this feature if the router is low on memory.

Use the **show ip mpacket** command to display the buffer.

Examples

The following example allocates a buffer to store IP Version 4 multicast packet headers:

```
ip multicast cache-headers
```

Related Commands

Command	Description
show ip mpacket	Displays the contents of the circular cache-header buffer.

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 *map-name*	(Optional) Name of the route map that contains various BGP attribute settings.

Defaults

DVMRP routes are not redistributed into multiprotocol BGP.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
11.1(20)CC	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Usage Guidelines

Use this command if you have a subset of DVMRP routes in an autonomous system that you want to take the multiprotocol BGP path. Define a route map to further specify which DVMRP routes get redistributed.

Examples

The following router configuration mode example redistributes DVMRP routes to BGP peers that match access list 1:

```
router bgp 109
 redistribute dvmrp route-map dvmrp-into-mbgp
route-map dvmrp-into-mbgp
 match ip address 1
```

The following address family configuration mode example redistributes DVMRP routes to multiprotocol BGP peers that match access list 1:

```
router bgp 109
address-family ipv4 multicast
 redistribute dvmrp route-map dvmrp-into-mbgp

route-map dvmrp-into-mbgp
 match ip address 1
```

set nlri

The **set 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.

show ip mbgp

The **show ip mgbp** 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** command in EXEC mode.

show ip bgp ipv4 multicast [*command*]

Syntax Description

command	(Optional) Any multiprotocol BGP command supported by the **show ip bgp ipv4 multicast** command.

Command Modes

EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.

Usage Guidelines

Use this command in conjunction with the **show ip rpf** command to determine if IP multicast routing is using multiprotocol BGP routes.

To determine which multiprotocol BGP commands are supported by the **show ip bgp ipv4 multicast** command, enter the following command while in EXEC mode:

```
Router# show ip bgp ipv4 multicast ?
```

The **show ip bgp ipv4 multicast** command replaces the **show ip mbgp** command.

Examples

The following is sample output from the **show ip bgp ipv4 multicast** command:

```
Router# show ip bgp ipv4 multicast

MBGP table version is 6, local router ID is 192.168.200.66
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*> 10.0.20.16/28     0.0.0.0                0      0 32768 i
*> 10.0.35.16/28     0.0.0.0                0      0 32768 i
*> 10.0.36.0/28      0.0.0.0                0      0 32768 i
*> 10.0.48.16/28     0.0.0.0                0      0 32768 i
*> 10.2.0.0/16       0.0.0.0                0      0 32768 i
*> 10.2.1.0/24       0.0.0.0                0      0 32768 i
*> 10.2.2.0/24       0.0.0.0                0      0 32768 i
*> 10.2.3.0/24       0.0.0.0                0      0 32768 i
*> 10.2.7.0/24       0.0.0.0                0      0 32768 i
*> 10.2.8.0/24       0.0.0.0                0      0 32768 i
*> 10.2.10.0/24      0.0.0.0                0      0 32768 i
*> 10.2.11.0/24      0.0.0.0                0      0 32768 i
*> 10.2.12.0/24      0.0.0.0                0      0 32768 i
*> 10.2.13.0/24      0.0.0.0                0      0 32768 i
```

Table 46 describes the significant fields shown in the display.

Table 46 show ip bgp ipv4 multicast Field Descriptions

Field	Description
MBGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is historical. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration or address family configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

Related Commands

Command	Description
show ip rpf	Displays how IP multicast routing does RPF.

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** command in EXEC mode.

show ip bgp ipv4 multicast summary

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.

Usage Guidelines

The **show ip bgp ipv4 multicast summary** command replaces the **show ip mbgp summary** command.

Examples

The following is sample output from the **show ip bgp ipv4 multicast summary** command:

```
Router# show ip bgp ipv4 multicast summary

BGP router identifier 10.0.33.34, local AS number 34
BGP table version is 5, main routing table version 1
4 network entries and 6 paths using 604 bytes of memory
5 BGP path attribute entries using 260 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
2 BGP community entries using 48 bytes of memory
2 BGP route-map cache entries using 32 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP activity 8/28 prefixes, 12/0 paths, scan interval 15 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.33.35      4    35     624     624        5    0    0 10:13:46        3
```

Table 47 describes the significant fields shown in the display.

Table 47 show ip bgp ipv4 multicast summary Field Descriptions

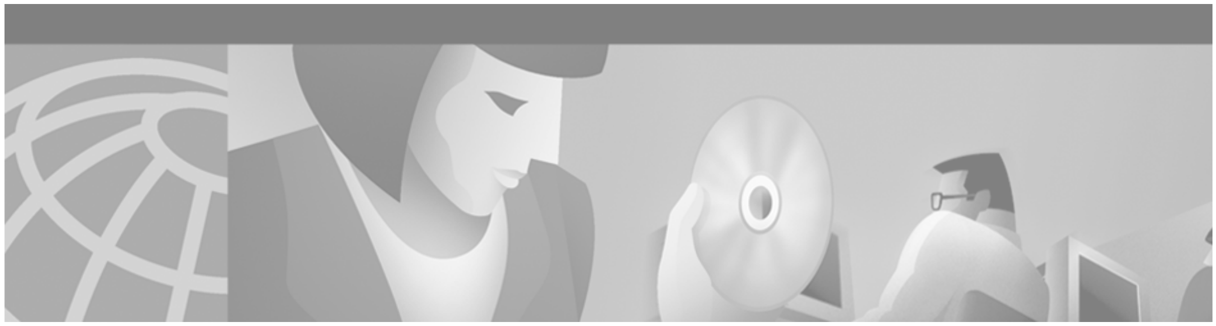
Field	Description
Neighbor	IP address of configured neighbor in the multicast routing table.
V	Version of multiprotocol BGP used.
AS	Autonomous system to which the neighbor belongs.
MsgRcvd	Number of messages received from the neighbor.
MsgSent	Number of messages sent to the neighbor.
TblVer	Number of the table version, which is incremented each time the table changes.
InQ	Number of messages received in the input queue.

Table 47 show ip bgp ipv4 multicast summary Field Descriptions (continued)

Field	Description
OutQ	Number of messages ready to go in the output queue.
Up/Down	Days and hours that the neighbor has been up or down (no information in the State column means the connection is up).
State/PfxRcd	State of the neighbor/number of routes received. If no state is indicated, the state is up.

Related Commands

Command	Description
show ip rpf	Displays how IP multicast routing does RPF.



IP Routing Protocol-Independent Commands

Use the commands in this chapter to configure and monitor the features that are routing protocol-independent. For configuration information and examples on IP routing protocol-independent features, refer to the "Configuring IP Routing Protocol-Independent Features" chapter of the *Cisco IOS IP Configuration Guide*.

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

start-time	Beginning time that the key specified by the **key** command is valid to be received. The syntax can be either of the following: *hh:mm:ss Month date year* *hh:mm:ss date Month year* *hh*—hours *mm*—minutes *ss*—seconds *Month*—first three letters of the month *date*—date (1-31) *year*—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 *start-time* value on.
end-time	Key is valid to be received from the *start-time* value until the *end-time* value. The syntax is the same as that for the *start-time* value. The *end-time* value must be after the *start-time* value. The default end time is an infinite time period.
duration *seconds*	Length of time (in seconds) that the key is valid to be received.

Defaults

Forever (the starting time is January 1, 1993, and ending time is infinite)

Command Modes

Key chain key configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Only DRP Agent, Enhanced IGRP (EIGRP), and Routing Information Protocol (RIP) Version 2 use key chains.

Specify a *start-time* value and one of the following values: **infinite**, *end-time*, or **duration** *seconds.*

We recommend running Network Time Protocol (NTP) or some other time synchronization method if you assign a lifetime to a key.

If the last key expires, authentication will continue and an error message will be generated. To disable authentication, you must manually delete the last valid key.

Examples

The following example configures a key chain called trees. The key named chestnut will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named birch will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or discrepancies in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
interface ethernet 0
 ip rip authentication key-chain trees
 ip rip authentication mode md5
!
router rip
 network 172.19.0.0
 version 2
!
key chain trees
 key 1
 key-string chestnut
 accept-lifetime 13:30:00 Jan 25 1996 duration 7200
 send-lifetime 14:00:00 Jan 25 1996 duration 3600
 key 2
 key-string birch
 accept-lifetime 14:30:00 Jan 25 1996 duration 7200
 send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
key	Identifies an authentication key on a key chain.
key chain	Enables authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show key chain	Displays authentication key information.

distance (IP)

To define an administrative distance, use the **distance** command in router configuration mode. To remove a distance definition, use the **no** form of this command.

distance {*ip-address* {*wildcard-mask*}} [*ip-standard-list*] [*ip-extended-list*]

no distance {*ip-address* {*wildcard-mask*}} [*ip-standard-list*] [*ip-extended-list*]

Syntax Description

ip-address	IP address in four-part, dotted notation.
wildcard-mask	Wild card mask in four-part, dotted decimal format. A bit set to 1 in the *mask* argument instructs the software to ignore the corresponding bit in the address value.
ip-standard-list *ip-extended-list*	(Optional) Number or name of a standard or extended IP access list to be applied to incoming routing updates.

Defaults

For more information on default administrative distance, see "Usage Guidelines."

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-number* | *name* argument was added.
11.3	The *access-list-number* | *name* argument was removed.
11.3	The **ip** keyword was removed.
12.0	The *ip-standard-list* and *ip-extended-list* arguments were added.

Usage Guidelines

Table 48 lists default administrative distances.

Table 48 Default Administrative Distances

Route Source	Default Distance
Connected interface	0
Static route	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (eBGP)	20
Internal Enhanced IGRP	90
IGRP	100
Open Shortest Path First (OSPF)	110
Intermediate System-to-Intermediate System (IS-IS)	115

Table 48 Default Administrative Distances (continued)

Route Source	Default Distance
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
EIGRP external route	170
Internal BGP	200
Unknown	255

Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means that the routing information source cannot be trusted at all and should be ignored.

When the optional access list number is used with this command, it is applied when a network is being inserted into the routing table. This behavior allows filtering of networks according to the IP address of the router supplying the routing information. This option could be used, as an example, to filter out possibly incorrect routing information from routers not under your administrative control.

The order in which you enter **distance** commands can affect the assigned administrative distances in unexpected ways (see the “Examples” section for further clarification).

For BGP, the **distance** command sets the administrative distance of the External BGP (EBGP) route.

The **show ip protocols** EXEC command displays the default administrative distance for a specified routing process.

Always set the administrative distance from the least to the most specific network.

Note The weight of a route can no longer be set with the **distance** command. To set the weight for a route, use a route-map.

Examples

In the following example, the **router igrp** global configuration command sets up IGRP routing in autonomous system number 109. The **network** router configuration commands specify IGRP routing on networks 192.168.7.0 and 172.16.0.0. The first **distance** router configuration command sets the default administrative distance to 255, which instructs the Cisco IOS software to ignore all routing updates from routers for which an explicit distance has not been set. The second **distance** command sets the administrative distance for all routers on the Class C network 192.168.7.0 to 90. The third **distance** command sets the administrative distance for the router with the address 172.16.1.3 to 120.

```
router igrp 109
 network 192.168.7.0
 network 172.16.0.0
 distance 255
 distance 90 192.168.7.0 0.0.0.255
 distance 120 172.16.1.3 0.0.0.0
```

In the following example, the set distance is from the least to the most specific network:

```
router igrp 100
 network 10.0.0.0
 distance 22 10.0.0.0
 distance 33 10.11.0.0 0.0.255.255
 distance 44 10.11.12.0 0.0.0.255
```

Note In this example, adding distance 255 to the end of the list would override the distance values for all networks within the range specified in the example. The result is that the distance values are set to 255.

Related Commands

Command	Description
distance bgp	Allows the use of external, internal, and local administrative distances that could be a better route to a node.

distribute-list in (IP)

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* | *access-list-name*} **in** [*interface-type interface-number*]

no distribute-list {*access-list-number* | *access-list-name*} **in** [*interface-type interface-number*]

Syntax Description

access-list-number | *access-list-name*	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.
interface-type	(Optional) Interface type.
interface-number	(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.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-name*, *interface-type*, and *interface-number* arguments were added.

Usage Guidelines

This command is not supported in Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF). OSPF routes cannot be filtered from entering the OSPF database. If you use this command for OSPF, it only filters routes from the routing table; it does not prevent link-state packets from being propagated. We recommend this command not be used for OSPF.

Examples

In the following example, the Enhanced IGRP routing process accepts only two networks—network 0.0.0.0 and network 10.108.0.0:

```
access-list 1 permit 0.0.0.0
access-list 1 permit 10.108.0.0
access-list 1 deny 0.0.0.0 255.255.255.255
router eigrp
 network 10.108.0.0
 distribute-list 1 in
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

distribute-list out (IP)

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* | *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

access-list-number | *access-list-name*	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.
interface-name	(Optional) Name of a particular interface.
routing-process	(Optional) Name of a particular routing process, or the **static** or **connected** keyword.
as-number	(Optional) Autonomous system number.

Defaults

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-name* argument was added.

Usage Guidelines

When networks are redistributed, a routing process name can be specified as an optional trailing argument to the **distribute-list** command. Specifying this option causes the access list to be applied to only those routes derived from the specified routing process. After the process-specific access list is applied, any access list specified by a **distribute-list** command without a process name argument will be applied. Addresses not specified in the **distribute-list** command will not be advertised in outgoing routing updates.

Note To filter networks received in updates, use the **distribute-list in** command.

Examples

The following example would cause only one network to be advertised by a RIP routing process, network 10.108.0.0:

```
access-list 1 permit 10.108.0.0
access-list 1 deny 0.0.0.0 255.255.255.255
router rip
 network 10.108.0.0
 distribute-list 1 out
```

The following example applies access list 1 to outgoing routing updates and enables Intermediate System-to-Intermediate System (IS-IS) on Ethernet interface 0. Only network 10.10.101.0 will be advertised in outgoing IS-IS routing updates.

```
router isis
 redistribute ospf 109
 distribute-list 1 out
interface Ethernet 0
 ip router isis
access-list 1 permit 10.10.101.0 0.0.0.255
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
distribute-list in (IP)	Filters networks received in updates.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

ip default-network

To select a network as a candidate route for computing the gateway of last resort, use the **ip default-network** command in global configuration mode. To remove a route, use the **no** form of this command.

ip default-network *network-number*

no ip default-network *network-number*

Syntax Description

network-number	Number of the network.

Defaults

If the router has a directly connected interface onto the specified network, the dynamic routing protocols running on that router will generate (or source) a default route. For Router Information Protocol (RIP), this is flagged as the pseudonetwork 0.0.0.0; for Interior Gateway Routing Protocol (IGRP), it is the network itself, flagged as an exterior route.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The Cisco IOS software uses both administrative distance and metric information to determine the default route. Multiple **ip default-network** commands can be given. All candidate default routes, both static (that is, flagged by the **ip default-network** command) and dynamic, appear in the routing table preceded by an asterisk.

If the IP routing table indicates that the specified network number is subnetted and a nonzero subnet number is specified, then the system will automatically configure a static summary route. This static summary route is configured instead of a default network. The effect of the static summary route is to cause traffic destined for subnets that are not explicitly listed in the IP routing table to be routed using the specified subnet.

Examples

The following example defines a static route to network 10.0.0.0 as the static default route:

```
ip route 10.0.0.0 255.0.0.0 10.108.3.4
ip default-network 10.0.0.0
```

If the following command was issued on a router not connected to network 10.140.0.0, the software might choose the path to that network as a default route when the network appeared in the routing table:

```
ip default-network 10.140.0.0
```

Related Commands

Command	Description
show ip route	Displays the current state of the routing table.

ip local policy route-map

To identify a route map to use for local policy routing, use the **ip local policy route-map** command in global configuration mode. 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

map-tag	Name of the route map to use for local policy routing. The name must match a *map-tag* value specified by a **route-map** command.

Defaults

Packets that are generated by the router are not policy routed.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Packets that are generated by the router are not normally policy routed. However, you can use this command to policy route such packets. You might enable local policy routing if you want packets originated at the router to take a route other than the obvious shortest path.

The **ip local policy route-map** command identifies a route map to use for local policy routing. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which packets should be policy routed. The **set** commands specify the *set actions*—the particular policy routing actions to perform if the criteria enforced by the **match** commands are met. The **no ip local policy route-map** command deletes the reference to the route map and disables local policy routing.

Examples

The following example sends packets with a destination IP address matching that allowed by extended access list 131 to the router at IP address 172.130.3.20:

```
ip local policy route-map xyz
!
route-map xyz
 match ip address 131
 set ip next-hop 172.130.3.20
```

Related Commands

Command	Description
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.
set ip default next-hop verify-availability	Indicates 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.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
show ip local policy	Displays the route map used for local policy routing.

ip policy route-map

To identify a route map to use for policy routing on an interface, use the **ip policy route-map** command in interface configuration mode. 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

map-tag	Name of the route map to use for policy routing. The name must match a *map-tag* value specified by a **route-map** command.

Defaults

No policy routing occurs on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

You might enable policy routing if you want your packets to take a route other than the obvious shortest path.

The **ip policy route-map** command identifies a route map to use for policy routing. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which policy routing is allowed for the interface. The **set** commands specify the *set actions*—the particular policy routing actions to perform if the criteria enforced by the **match** commands are met. The **no ip policy route-map** command deletes the pointer to the route map.

Policy routing can be performed on any match criteria that can be defined in an extended IP access list when using the **match ip address** command and referencing an extended IP access list.

Examples

The following example sends packets with the destination IP address of 172.120.16.18 to a router at IP address 172.130.3.20:

```
interface serial 0
 ip policy route-map wethersfield
!
route-map wethersfield
 match ip address 172.120.16.18
 set ip next-hop 172.130.3.20
```

Related Commands

Command	Description
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.
set ip default next-hop verify-availability	Indicates 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.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.

ip route

To establish static routes, use the **ip route** command in global configuration mode. To remove static routes, use the **no** form of this command.

ip route *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [*distance*] [**name**] [**permanent**] [**tag** *tag*]

no ip route *prefix mask*

Syntax Description

prefix	IP route prefix for the destination.
mask	Prefix mask for the destination.
ip-address	IP address of the next hop that can be used to reach that network.
interface-type interface-number	Network interface type and interface number.
distance	(Optional) An administrative distance.
name	(Optional)Applies a name to the specified route.
permanent	(Optional) Specifies that the route will not be removed, even if the interface shuts down.
tag *tag*	(Optional) Tag value that can be used as a "match" value for controlling redistribution via route maps.

Defaults

No static routes are established.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The establishment of a static route is appropriate when the Cisco IOS software cannot dynamically build a route to the destination.

If you specify an administrative distance, you are flagging a static route that can be overridden by dynamic information. For example, IGRP-derived routes have a default administrative distance of 100. To have a static route that would be overridden by an IGRP dynamic route, specify an administrative distance greater than 100. Static routes have a default administrative distance of 1.

Static routes that point to an interface on a connected router will be advertised by way of Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), and Exterior Gateway Routing Protocol (EIGRP) regardless of whether **redistribute static** commands were specified for those routing protocols. This situation occurs because static routes that point to an interface are considered in the routing table to be connected and hence lose their static nature. Also, the target of the static route should be included in the network command. If this condition is not met, no dynamic routing protocol will advertise the route unless a **redistribute static** command is specified for these protocols. With the following configuration:

```
rtr1 (serial 172.140..188.1/30)--------------> rtr2(Fast Ethernet 172.150.1.1/30) ------>

router [rip | eigrp | igrp]
net 172.140..188.0
net 172.150.0.0
```

- RIP and IGRP redistribute the route if the route is pointing to the Fast Ethernet interface:

  ```
  ip route 172.140..188.252 255.255.255.252 FastEthernet0/0
  ```

  RIP and IGRP do not redistribute the route with the following **ip route** command because of the split horizon algorithm:

  ```
  ip route 172.140..188.252 255.255.255.252 s2/1
  ```

- EIGRP redistributes the route with both of the following commands:

  ```
  ip route 172.140..188.252 255.255.255.252 FastEthernet0/0
  ip route 172.140..188.252 255.255.255.252 s2/1
  ```

With Open Shortest Path First (OSPF), static routes that point to an interface are not advertised unless a **redistribute static** command is specified.

Adding a static route to an Ethernet or other broadcast interface (for example, **ip route** 0.0.0.0 0.0.0.0 **Ethernet** 1/2) will cause the route to be inserted into the routing table only when the interface is up. This configuration is not generally recommended. When the next hop of a static route points to an interface, the router considers each of the hosts within the range of the route to be directly connected through that interface, and therefore it will send ARP requests to any destination addresses that route through the static route.

The practical implication of configuring "**ip route** 0.0.0.0 0.0.0.0 **Ethernet** 1/2" is that the router will consider all of the destinations that the router does not know how to reach through some other route as directly connected to Ethernet 1/2. So the router will send an ARP request for each host for which it receives packets on this network segment. This configuration can cause high processor utilization and a very large ARP cache (along with attendant memory allocation failures). Configuring a default route or other static route that directs the router to forward packets for a large range of destinations to a connected broadcast network segment can cause your router to reload.

Specifying a numerical next hop that is on a directly connected interface will prevent the router from using Proxy ARP. However, if the interface with the next hop goes down and the numerical next hop can be reached through a recursive route, you may specify both the next hop and interface (for example "**ip route** 0.0.0.0 0.0.0.0 **Ethernet**1/2 10.1.2.3") with a static route to prevent routes from passing through an unintended interface.

Examples

The following example chooses an administrative distance of 110. In this case, packets for network 10.0.0.0 will be routed through to a router at 172.31.3.4 if dynamic information with administrative distance less than 110 is not available.

```
ip route 10.0.0.0 255.0.0.0 172.31.3.4 110
```

Note Specifying the next hop without specifying an interface when configuring a static route can cause traffic to pass through an unintended interface if the default interface goes down.

The following example routes packets for network 172.31.0.0 to a router at 172.31.6.6:

```
ip route 172.31.0.0 255.255.0.0 172.31.6.6
```

The following example routes packets for network 192.168.1.0 directly to the next hop at 10.1.2.3. If the interface goes down, this route is removed from the routing table and will not be restored unless the interface comes back up.

```
ip route 192.168.1.0 255.255.0.0 Ethernet0 10.1.2.3
```

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

key-id	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.

Defaults

No key exists on the key chain.

Command Modes

key-chain configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Only DRP Agent, Enhanced IGRP (EIGRP), and Routing Information Protocol (RIP) Version 2 use key chains.

It is useful to have multiple keys on a key chain so that the software can sequence through the keys as they become invalid after time, based on the **accept-lifetime** and **send-lifetime** key chain key command settings.

Each key has its own key identifier, which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and Message Digest 5 (MD5) authentication key in use. Only one authentication packet is sent, regardless of the number of valid keys. The software starts looking at the lowest key identifier number and uses the first valid key.

If the last key expires, authentication will continue and an error message will be generated. To disable authentication, you must manually delete the last valid key.

To remove all keys, remove the key chain by using the **no key chain** command.

Examples

The following example configures a key chain named trees. The key named chestnut will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named birch will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
interface ethernet 0
 ip rip authentication key-chain trees
 ip rip authentication mode md5
!
router rip
 network 172.19.0.0
 version 2
!
key chain trees
 key 1
 key-string chestnut
 accept-lifetime 13:30:00 Jan 25 1996 duration 7200
 send-lifetime 14:00:00 Jan 25 1996 duration 3600
 key 2
 key-string birch
 accept-lifetime 14:30:00 Jan 25 1996 duration 7200
 send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
key chain	Enables authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show key chain	Displays authentication key information.

key chain

To enable authentication for routing protocols, identify a group of authentication keys by using the **key chain** command in global configuration mode. 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

name-of-chain	Name of a key chain. A key chain must have at least one key and can have up to 2,147,483,647 keys.

Defaults

No key chain exists.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Only DRP Agent, Enhanced IGRP (EIGRP), and Routing Information Protocol (RIP) Version 2 use key chains.

You must configure a key chain with keys to enable authentication.

Although you can identify multiple key chains, we recommend using one key chain per interface per routing protocol. Upon specifying the **key chain** command, you enter key-chain configuration mode.

Examples

The following example configures a key chain named trees. The key named chestnut will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named birch will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
interface ethernet 0
 ip rip authentication key-chain trees
 ip rip authentication mode md5
!
router rip
 network 172.19.0.0
 version 2
!
key chain trees
 key 1
 key-string chestnut
 accept-lifetime 13:30:00 Jan 25 1996 duration 7200
 send-lifetime 14:00:00 Jan 25 1996 duration 3600
  key 2
  key-string birch
  accept-lifetime 14:30:00 Jan 25 1996 duration 7200
  send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ip rip authentication key-chain	Enables authentication for RIP Version 2 packets and specifies the set of keys that can be used on an interface.
key	Identifies an authentication key on a key chain.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show key chain	Displays authentication key information.

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

text	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.

Defaults

No key exists.

Command Modes

Key chain key configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Only DRP Agent, Enhanced IGRP (EIGRP), and Routing Information Protocol (RIP) Version 2 use key chains. Each key can have only one key string.

If password encryption is configured (with the **service password-encryption** command), the software saves the key string as encrypted text. When you write to the terminal with the **more system:running-config** command, the software displays key-string 7 encrypted text.

Examples

The following example configures a key chain named trees. The key named chestnut will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named birch will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
interface ethernet 0
 ip rip authentication key-chain trees
 ip rip authentication mode md5
!
router rip
 network 172.19.0.0
 version 2
!
key chain trees
 key 1
 key-string chestnut
 accept-lifetime 13:30:00 Jan 25 1996 duration 7200
 send-lifetime 14:00:00 Jan 25 1996 duration 3600
 key 2
 key-string birch
 accept-lifetime 14:30:00 Jan 25 1996 duration 7200
 send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication for routing protocols.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
service password-encryption	Encrypts passwords.
show key chain	Displays authentication key information.

match interface (IP)

To distribute any routes that have their next hop out one of the interfaces specified, use the **match interface** command in route-map configuration mode. 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

interface-type	Interface type.
interface-number	Interface number.

Defaults

No match interfaces are defined.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *interface-type interface-number* arguments.

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands may be given in any order, and all **match** commands must "pass" to cause the route to be redistributed according to the *set actions* given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

A route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

Examples

In the following example, routes that have their next hop out Ethernet interface 0 will be distributed:

```
route-map name
 match interface ethernet 0
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community-list	Matches a BGP community.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

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** command in route-map configuration mode. 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

access-list-number	Number of a standard or extended access list. It can be an integer from 1 to 199.
access-list-name	Name of a standard or extended access list. It can be an integer from 1 to 199.

Defaults

No access list numbers are specified.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *access-list-number* or *access-list-name* argument.

Like matches in the same route map subblock are filtered with “or” semantics. If any one match clause is matched in the entire route map subblock, this match is treated as a successful match. Dissimilar match clauses are filtered with “and” semantics. So dissimilar matches are filtered logically. If the first set of conditions is not met, the second match clause is filtered. This process continues until a match occurs or there are no more match clauses.

Use route maps to redistribute routes or to subject packets to policy routing. Both purposes are described in this section.

Redistribution

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must "pass" to cause the route to be redistributed according to the *set actions* given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

Policy Routing

Another purpose of route maps is to enable policy routing. The **match ip address** command allows you to policy route packets based on criteria that can be matched with an extended access list. For example, a protocol, protocol service, and source or destination IP address. To define the conditions for policy routing packets, use the **ip policy route-map** interface configuration command, in addition to the **route-map** global configuration command, and the **match** and **set** route-map configuration commands. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which policy routing occurs. The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met. You might want to policy route packets based on their source, for example, using an access list.

Examples

In the following example, routes that have addresses specified by access list numbers 5 or 80 will be matched:

```
route-map name
 match ip address 5 80
```

In the following policy routing example, packets that have addresses specified by access list numbers 6 or 25 will be routed to Ethernet interface 0:

```
interface serial 0
 ip policy route-map chicago
!
route-map chicago
 match ip address 6 25
 set interface ethernet 0
```

Related Commands

Command	Description
ip local policy route-map	Identifies a route map to use for policy routing on an interface.
match as-path	Matches a BGP autonomous system path access list.
match community-list	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match length	Bases policy routing on the Level 3 length of a packet.
match metric (IP)	Redistributes routes with the metric specified.

Command	Description
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ip default next-hop verify-availability	Indicates 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.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

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** command in route-map configuration mode. 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

access-list-number | *access-list-name*	Number or name of a standard or extended access list. It can be an integer from 1 to 199.

Defaults

Routes are distributed freely, without being required to match a next hop address.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *access-list-number* or *access-list-name* argument.

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must "pass" to cause the route to be redistributed according to the *set actions* given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

Examples

The following example distributes routes that have a next hop router address passed by access list 5 or 80 will be distributed:

```
route-map name
 match ip next-hop 5 80
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community-list	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

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** command in route-map configuration mode. 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

access-list-number | *access-list-name*	Number or name of a standard or extended access list. It can be an integer from 1 to 199.

Defaults

No filtering on route source.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *access-list-number* or *access-list-name* argument.

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must "pass" to cause the route to be redistributed according to the *set actions* given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

A route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure second route map section with an explicit match specified.

There are situations in which the next hop and source router address of the route are not the same.

Examples

The following example distributes routes that have been advertised by routers and access servers at the addresses specified by access lists 5 and 80:

```
route-map name
 match ip route-source 5 80
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community-list	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

match length

To base policy routing on the Level 3 length of a packet, use the **match length** command in route-map configuration mode. 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

minimum-length	Minimum Level 3 length of the packet, inclusive, allowed for a match. Range is from 0 to 0x7FFFFFFF.
maximum-length	Maximum Level 3 length of the packet, inclusive, allowed for a match. Range is from 0 to 0x7FFFFFFF.

Defaults

No policy routing on the length of a packet.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for policy routing packets. The **ip policy route-map** command identifies a route map by name. Each **route-map** has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which policy routing occurs. The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must "pass" to cause the packet to be routed according to the *set actions* given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

You might want to base your policy routing on the length of packets so that your interactive traffic and bulk traffic are directed to different routers.

Examples

In the following example, packets 3 to 200 bytes long, inclusive, will be routed to FDDI interface 0:

```
interface serial 0
 ip policy route-map interactive
!
route-map interactive
 match length 3 200
 set interface fddi 0
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.
set ip default next-hop verify-availability	Indicates 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.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.

match metric (IP)

To redistribute routes with the metric specified, use the **match metric** command in route-map configuration mode. To remove the entry, use the **no** form of this command.

match metric *metric-value*

no match metric *metric-value*

Syntax Description

metric-value	Route metric, which can be an IGRP five-part metric. It is a metric value from 0 to 4294967295.

Defaults

No filtering on a metric value.

Command Modes

Route-map configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must “pass” to cause the route to be redistributed according to the *set actions* given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

A route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure second route map section with an explicit match specified.

Examples

In the following example, routes with the metric 5 will be redistributed:

```
route-map name
 match metric 5
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community-list	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

match route-type (IP)

To redistribute routes of the specified type, use the **match route-type** command in route-map configuration mode. 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.

Defaults

This command is disabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The **local** and **external** [**type-1** | **type-2**] keywords were added.

Usage Guidelines

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must “pass” to cause the route to be redistributed according to the *set actions* given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

A route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure second route map section with an explicit match specified.

Examples

The following example redistributes internal routes:

```
route-map name
 match route-type internal
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community-list	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

match tag

To redistribute routes in the routing table that match the specified tags, use the **match tag** command in route-map configuration mode. 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

tag-value	List of one or more route tag values. Each can be an integer from 0 to 4294967295.

Defaults

No match tag values are defined.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *tag-value* argument.

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must "pass" to cause the route to be redistributed according to the *set actions* given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

A route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure second route map section with an explicit match specified.

Examples

The following example redistributes routes stored in the routing table with tag 5:

```
route-map name
 match tag 5
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community-list	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

maximum-paths

To control the maximum number of parallel routes an IP routing protocol can support, use the **maximum-paths** command in router configuration mode. To restore the default value, use the **no** form of this command.

maximum-paths *number-paths*

no maximum-paths

Syntax Description

number-paths	Maximum number of parallel routes an IP routing protocol installs in a routing table, in the range from 1 to 6.

Defaults

The default for Border Gateway Protocol (BGP) is one path. The default for all other IP routing protocols is four paths.

Command Modes

Router configuration

Command History

Release	Modification
11.2	This command was introduced.

Examples

The following example allows a maximum of two paths to a destination:

```
maximum-paths 2
```

passive-interface

To disable sending routing updates on an interface, use the **passive-interface** command in router configuration mode. To reenable 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.
interface-type	Interface type.
interface-number	Interface number.

Defaults

Routing updates are sent on the interface.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0	The **default** keyword was added.

Usage Guidelines

If you disable the sending of routing updates on an interface, the particular subnet will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

The **default** keyword sets all interfaces as passive by default. You can then configure individual interfaces where adjacencies are desired using the **no passive-interface** command. The **default** keyword is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

For the Open Shortest Path First (OSPF) protocol, OSPF routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the OSPF domain.

For the Intermediate System-to-Intermediate System (IS-IS) protocol, this command instructs IS-IS to advertise the IP addresses for the specified interface without actually running IS-IS on that interface. The **no** form of this command for IS-IS disables advertising IP addresses for the specified address.

Enhanced Interior Gateway Routing Protocol (EIGRP) is disabled on an interface that is configured as passive although it advertises the route.

Examples

The following example sends IGRP updates to all interfaces on network 10.108.0.0 except Ethernet interface 1:

```
router igrp 109
 network 10.108.0.0
 passive-interface ethernet 1
```

The following configuration enables IS-IS on Ethernet interface 1 and serial interface 0 and advertises the IP addresses of Ethernet interface 0 in its link-state protocol data units (PDUs):

```
router isis Finance
 passive-interface Ethernet 0
interface Ethernet 1
 ip router isis Finance
interface serial 0
 ip router isis Finance
```

The following example sets all interfaces as passive, then activates Ethernet interface 0:

```
router ospf 100
passive-interface default
no passive-interface ethernet0
network 10.108.0.1 0.0.0.255 area 0
```

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*] [**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*] [**subnets**]

Syntax Description

protocol	Source protocol from which routes are being redistributed. It can be one of the following keywords: **bgp**, **connected**, **egp**, **igrp**, **isis**, **mobile**, **ospf**, **static** [**ip**], or **rip**. 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. 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.
process-id	(Optional) For the **bgp**, **egp**, or **igrp** keyword, this is an autonomous system number, which is a 16-bit decimal number. 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. 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. For the **rip** keyword, no *process-id* value is needed.
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.
as-number	(Opitonal) Autonomous system number for the redistributed route.
metric *metric-value*	(Optional) When redistributing from one OSPF process to another OSPF process on the same router, the metric will be carried through from one process to the other if no metric value is specified. When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified.

metric-type *type-value*	(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: • **1**—Type 1 external route • **2**—Type 2 external route If a **metric-type** is not specified, the Cisco IOS software adopts a Type 2 external route. For IS-IS, it can be one of two values: • **internal**—IS-IS metric that is < 63. • **external**—IS-IS metric that is > 64 < 128. The default is **internal**.
match {**internal** | **external 1** | **external 2**}	(Optional) For the criteria by which OSPF routes are redistributed into other routing domains. It can be one of the following: • **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 *tag-value*	(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.
route-map	(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.
map-tag	(Optional) Identifier of a configured route map.
subnets	(Optional) For redistributing routes into OSPF, the scope of redistribution for the specified protocol.

Defaults

Route redistribution is disabled.

protocol: No source protocol is defined.

process-id: No process ID is defined.

metric *metric-value*: 0

metric-type *type-value*: Type 2 external route

match internal | external: Internal, external 1, external 2

external: Internal

tag *tag-value*: If no value is specified, the remote autonomous system number is used for routes from BGP and EGP; for other protocols, the default is 0.

route-map *map-tag*: If the **route-map** keyword is not entered, all routes are redistributed; if no *map-tag* value is entered, no routes are imported.

subnets: No subnets are defined.

Command Modes

Router configuration

Address family configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	Address family configuration mode was added.

Usage Guidelines

Changing or disabling any keyword will not affect the state of other keywords.

A router receiving a link-state protocol with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric only considers the advertised metric to reach the destination.

Routes learned from IP routing protocols can be redistributed at Level 1 into an attached area or at Level 2. The **level-1-2** keyword allows both Level 1 and Level 2 routes in a single command.

Redistributed routing information must be filtered by the **distribute-list out** router configuration command. This guideline ensures that only those routes intended by the administrator are passed along to the receiving routing protocol.

Whenever you use the **redistribute** or the **default-information** router configuration commands to redistribute routes into an OSPF routing domain, the router automatically becomes an ASBR. However, an ASBR does not, by default, generate a *default route* into the OSPF routing domain.

When routes are redistributed between OSPF processes, no OSPF metrics are preserved.

When routes are redistributed into OSPF and no metric is specified in the **metric** keyword, OSPF uses the default metric 20 for routes from all protocols except BGP, which gets a metric of 1. Furthermore, when the router redistributes from one OSPF process to another OSPF process on the same router, and if no default metric is specified, the metrics in one process are carried to the redistributing process.

When routes are redistributed into OSPF, only routes that are not subnetted are redistributed if the **subnets** keyword is not specified.

Routes configured with the **connected** keyword affected by this **redistribute** command are the routes not specified by the **network** router configuration command.

You cannot use the **default-metric** command to affect the metric used to advertise **connected** routes.

Note The **metric** value specified in the **redistribute** command supersedes the **metric** value specified using the **default-metric** command.

Default redistribution of IGPs or EGP into BGP is not allowed unless the **default-information originate** router configuration command is specified.

Examples

The following example causes OSPF routes to be redistributed into a BGP domain:

```
router bgp 109
 redistribute ospf
```

The following example causes Interior Gateway Routing Protocol (IGRP) routes to be redistributed into an OSPF domain:

```
router ospf 110
 redistribute igrp
```

The following example causes the specified IGRP process routes to be redistributed into an OSPF domain. The IGRP-derived metric will be remapped to 100 and RIP routes to 200.

```
router ospf 109
 redistribute igrp 108 metric 100 subnets
 redistribute rip metric 200 subnets
```

The following example configures BGP routes to be redistributed into IS-IS. The link-state cost is specified as 5, and the metric type will be set to external, indicating that it has lower priority than internal metrics.

```
router isis
 redistribute bgp 120 metric 5 metric-type external
```

In the following example, network 172.16.0.0 will appear as an external link-state advertisement (LSA) in OSPF 1 with a cost of 100 (the cost is preserved):

```
interface ethernet 0
 ip address 172.16.0.1 255.0.0.0
 ip ospf cost 100
interface ethernet 1
 ip address 10.0.0.1 255.0.0.0
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 redistribute ospf 2 subnet
router ospf 2
 network 172.16.0.0 0.255.255.255 area 0
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
default-information originate (BGP)	Allows the redistribution of network 0.0.0.0 into BGP.
default-information originate (IS-IS)	Generates a default route into an IS-IS routing domain.
default-information originate (OSPF)	Generates a default route into an OSPF routing domain.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
show route-map	Displays all route maps configured or only the one specified.

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** command in global configuration mode and the **match** and **set** command in route-map configuration modes. 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

map-tag	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. 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.
sequence-number	(Optional) Number that indicates the position a new route map will 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.

Defaults

No default is available.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use route maps to redistribute routes or to subject packets to policy routing. Both purposes are described in this section.

Redistribution

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. The **match** commands can be given in any order, and all **match** commands must "pass" to cause the route to be redistributed according to the *set actions* given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

Use route maps when you want detailed control over how routes are redistributed between routing processes. The destination routing protocol is the one you specify with the **router** global configuration command. The source routing protocol is the one you specify with the **redistribute** router configuration command. See the "Examples" section for an illustration of how route maps are configured.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

Policy Routing

Another purpose of route maps is to enable policy routing. Use the **ip policy route-map** command, in addition to the **route-map** command, and the **match** and **set** commands to define the conditions for policy routing packets. The **match** commands specify the conditions under which policy routing occurs. The **set** commands specify the routing actions to perform if the criteria enforced by the **match** commands are met. You might want to policy route packets some way other than the obvious shortest path.

The *sequence-number* argument works as follows:

1. If no entry is defined with the supplied tag, an entry is created with the *sequence-number* argument set to 10.
2. If only one entry is defined with the supplied tag, that entry becomes the default entry for the following **route-map** command. The *sequence-number* argument of this entry is unchanged.
3. If more than one entry is defined with the supplied tag, an error message is printed to indicate that the *sequence-number* argument is required.

If the **no route-map** *map-tag* command is specified (with no *sequence-number* argument), the whole route map is deleted.

Examples

The following example redistributes Routing Information Protocol (RIP) routes with a hop count equal to 1 into Open Shortest Path First (OSPF). These routes will be redistributed into OSPF as external link-state advertisements (LSAs) with a metric of 5, metric type of Type 1, and a tag equal to 1.

```
router ospf 109
 redistribute rip route-map rip-to-ospf

route-map rip-to-ospf permit
 match metric 1
 set metric 5
 set metric-type type1
 set tag 1
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
match as-path	Matches a BGP autonomous system path access list.
match community-list	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match length	Bases policy routing on the Level 3 length of a packet.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ip default next-hop verify-availability	Indicates 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.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.

Command	Description
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.
show route-map	Displays all route maps configured or only the one specified.

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

start-time	Beginning time that the key specified by the **key** command is valid to be sent. The syntax can be either of the following: *hh*:*mm*:*ss Month date year* *hh*:*mm*:*ss date Month year* *hh*—hours *mm*—minutes *ss*—seconds *Month*—first three letters of the month *date*—date (1-31) *year*—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 *start-time* value on.
end-time	Key is valid to be sent from the *start-time* value until the *end-time* value. The syntax is the same as that for the *start-time* value. The *end-time* value must be after the *start-time* value. The default end time is an infinite time period.
duration *seconds*	Length of time (in seconds) that the key is valid to be sent.

Defaults

Forever (the starting time is January 1, 1993, and the ending time is infinite)

Command Modes

Key chain key configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

Specify a *start-time* value and one of the following values: **infinite**, *end-time*, or **duration** *seconds*.

We recommend running Network Time Protocol (NTP) or some other time synchronization method if you intend to set lifetimes on keys.

If the last key expires, authentication will continue and an error message will be generated. To disable authentication, you must manually delete the last valid key.

Examples

The following example configures a key chain called trees. The key named chestnut will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named birch will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or discrepancies in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
interface ethernet 0
 ip rip authentication key-chain trees
 ip rip authentication mode md5
!
router rip
 network 172.19.0.0
 version 2
!
key chain trees
 key 1
 key-string chestnut
 accept-lifetime 13:30:00 Jan 25 1996 duration 7200
 send-lifetime 14:00:00 Jan 25 1996 duration 3600
 key 2
 key-string birch
 accept-lifetime 14:30:00 Jan 25 1996 duration 7200
 send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
show key chain	Displays authentication key information.

set automatic-tag

To automatically compute the tag value, use the **set automatic-tag** command in route-map configuration mode. 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.

Defaults

This command is disabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You must have a match clause (even if it points to a "permit everything" list) if you want to set tags.

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution *set actions* to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

The following example configures the Cisco IOS software to automatically compute the tag value for the Border Gateway Protocol (BGP) learned routes:

```
route-map tag
 match as path 10
 set automatic-tag
!
router bgp 100
 table-map tag
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community-list	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.
show route-map	Displays all route maps configured or only the one specified.

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** command in route-map configuration mode. 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

interface-type	Interface type, used with the interface number, to which packets are output.
interface-number	Interface number, used with the interface type, to which packets are output.

Defaults

This command is disabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *interface-type interface-number* arguments.

Use this command to provide certain users a different default route. If the Cisco IOS software has no explicit route for the destination, then it routes the packet to this interface. The first interface specified with the **set default interface** command that is up is used. The optionally specified interfaces are tried in turn.

Use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for policy routing packets. The **ip policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which policy routing occurs. The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ip next-hop**
2. **set interface**
3. **set ip default next-hop**
4. **set default interface**

Examples

In the following example, packets that have a Level 3 length of 3 to 50 bytes and for which the software has no explicit route to the destination are output to Ethernet interface 0:

```
interface serial 0
 ip policy route-map brighton
!
route-map brighton
 match length 3 50
 set default interface ethernet 0
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.
set ip default next-hop verify-availability	Indicates 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.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.

set interface

To indicate where to output packets that pass a match clause of a route map for policy routing, use the **set interface** command in route-map configuration mode. 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

interface-type	Interface type, used with the interface number, to which packets are output.
interface-number	Interface number, used with the interface type, to which packets are output.

Defaults

This command is disabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *interface-type interface-number* arguments.

Use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for policy routing packets. The **ip policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which policy routing occurs. The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

If the first interface specified with the **set interface** command is down, the optionally specified interfaces are tried in turn.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ip next-hop**
2. **set interface**
3. **set ip default next-hop**
4. **set default interface**

A useful next hop implies an interface. As soon as a next hop and an interface are found, the packet is routed.

Specifying the **set interface null 0** command is a way to write a policy that the packet be dropped and an “unreachable” message be generated.

Note The **set interface** command is supported only over a point-to-point link, unless a route-cache entry exists using the same interface specified in the **set interface** command in the route map.

Examples

In the following example, packets with a Level 3 length of 3 to 50 bytes are output to Ethernet interface 0:

```
interface serial 0
 ip policy route-map testing
!
route-map testing
 match length 3 50
 set interface ethernet 0
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set ip default next-hop verify-availability	Indicates 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.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.

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** command in route-map configuration mode. 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

ip-address	IP address of the next hop to which packets are output.The next hop must be an adjacent router.

Defaults

This command is disabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *ip-address* argument.

Use this command to provide certain users a different default route. If the software has no explicit route for the destination in the packet, then it routes the packet to this next hop. The first next hop specified with the **set ip default next-hop** command needs to be adjacent to the router. The optional specified IP addresses are tried in turn.

Use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for policy routing packets. The **ip policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which policy routing occurs. The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ip next-hop**
2. **set interface**
3. **set ip default next-hop**
4. **set default interface**

Note The **set ip next-hop** and **set ip default next-hop** are similar commands but have a different order of operations. Configuring the **set ip next-hop** command causes the system to use policy routing first and then use the routing table. Configuring the **set ip default next-hop** command causes the system to use the routing table first and then policy route the specified next hop.

Examples

The following example provides two sources with equal access to two different service providers. Packets arriving on asynchronous interface 1 from the source 10.1.1.1 are sent to the router at 172.16.6.6 if the software has no explicit route for the destination of the packet. Packets arriving from the source 10.2.2.2 are sent to the router at 172.17.7.7 if the software has no explicit route for the destination of the packet. All other packets for which the software has no explicit route to the destination are discarded.

```
access-list 1 permit ip 10.1.1.1 0.0.0.0
access-list 2 permit ip 10.2.2.2 0.0.0.0
!
interface async 1
 ip policy route-map equal-access
!
route-map equal-access permit 10
 match ip address 1
 set ip default next-hop 172.16.6.6
route-map equal-access permit 20
 match ip address 2
 set ip default next-hop 172.17.7.7
 route-map equal-access permit 30
 set default interface null0
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.

set ip default next-hop verify-availability

To configure a router, for policy routing, to check the CDP database for the availability of an entry for the default next hop that is specified by the **set ip default next-hop** command, use the **set ip default next-hop verify-availability** route map configuration command. To disable this function, use the no form of this command.

set ip default next-hop verify-availability

no set ip default next-hop verify-availability

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
12.1(1.05)T	This command was introduced.

Usage Guidelines

Use this command to force the configured policy routing to check the CDP database to determine if an entry is available for the next hop that is specified by the **set ip default next-hop** command. This command is used to prevent traffic from being "black holed" if the configured next hop becomes unavailable.

Examples

The following example :

```
Router(config-route-map)# set ip default next-hop verify-availability
```

Related Commands

Command	Description
set ip next-hop verify-availability	Configures policy routing to verify if the next hops of a route map are CDP neighbors before policy routing to those next hops.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.

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** command in route-map configuration mode. 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

ip-address	IP address of the next hop to which packets are output. The next hop must be an adjacent router.

Defaults

This command is disabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *ip-address* argument.

Use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for policy routing packets. The **ip policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which policy routing occurs. The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

If the interface associated with the first next hop specified with the **set ip next-hop** command is down, the optionally specified IP addresses are tried in turn.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ip next-hop**
2. **set interface**
3. **set ip default next-hop**
4. **set default interface**

Note The **set ip next-hop** and **set ip default next-hop** are similar commands but have a different order of operations. Configuring the **set ip next-hop** command causes the system to use policy routing first and then use the routing table. Configuring the **set ip default next-hop** command causes the system to use the routing table first and then policy route the specified next hop.

Examples

In the following example, packets with a Level 3 length of 3 to 50 bytes are output to the router at IP address 10.14.2.2:

```
interface serial 0
 ip policy route-map thataway
!
route-map thataway
 match length 3 50
 set ip next-hop 10.14.2.2
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.
set ip default next-hop verify-availability	Indicates 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.

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** command in route-map configuration mode.

set ip next-hop verify-availability

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

One example of when you might configure this command is if you have some traffic traveling via a satellite to a next hop. It might be prudent to verify that the next hop is reachable before trying to policy route to it.

This command has the following restrictions:

- It causes some performance degradation.
- CDP must be configured on the interface.
- The next hop must be a Cisco device with CDP enabled.
- It is supported in process switching and Cisco express forwarding (CEF) policy routing, but not available in dCEF, due to the dependency of the CDP neighbor database.

If the router is policy routing packets to the next hop and the next hop happens to be down, the router will try unsuccessfully to use Address Resolution Protocol (ARP) for the next hop (which is down). This behavior will continue forever.

To prevent this situation, use this command to configure the router to first verify that the next hops of the route map are the CDP neighbors of the router before routing to those next hops.

This command is optional because some media or encapsulations do not support CDP, or it may not be a Cisco device that is sending the router traffic.

If this command is set and the next hop is not a CDP neighbor, the router looks to the subsequent next hop, if there is one. If there is none, the packets simply are not policy routed.

If this command is not set, the packets are either successfully policy routed or remain forever unrouted.

If you want to selectively verify availability of only some next hops, you can configure different route map entries (under the same route map name) with different criteria (using access list matching or packet size matching), and use the **set ip next-hop verify-availability** command selectively.

Examples

The following example configures CEF, NetFlow, and NetFlow with flow acceleration. It also configures policy routing to verify that next hop 10.0.0.8 of the route map named test is a CDP neighbor before the router tries to policy route to it.

If the first packet is being policy routed via route map test sequence 10, the subsequent packets of the same flow always take the same route map test sequence 10, not route map test sequence 20, because they all match or pass the access list 1 check. Therefore, policy routing can be flow-accelerated by bypassing the access list check.

```
ip cef
ip flow-cache feature-accelerate
interface ethernet0/0/1
 ip route-cache flow
 ip policy route-map test
route-map test permit 10
 match ip address 1
 set ip precedence priority
 set ip next-hop 10.0.0.8
 set ip next-hop verify-availability
route-map test permit 20
 match ip address 101
 set interface Ethernet0/0/3
 set ip tos max-throughput
```

Related Commands

Command	Description
show route-map ipc	Displays counts of the one-way route map IPC messages sent from the RP to the VIP when NetFlow policy routing is configured.

set ip precedence

To set the precedence value in the IP header, use the **set ip precedence** command in route-map configuration mode. 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

number | *name*	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**

Defaults

This command has no default behavior.

Command Modes

Route-map configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

You can set the precedence using either a number or the corresponding name.

Note Setting the precedence bit affects weighted fair queueing (WFQ). It acts as a multiplier on the WFQ weighting, using a formula of 4096 divided by the IP Precedence value plus 1. For more information, see the **fair-queue** command.

The way the network gives priority (or some type of expedited handling) to the marked traffic is through the application of WFQ or weighted random early detection (WRED) at points downstream in the network. Typically, you would set IP precedence at the edge of the network (or administrative domain) and have queueing act on it thereafter. WFQ can speed up handling for high precedence traffic at congestion points. WRED ensures that high precedence traffic has lower loss rates than other traffic during times of congestion.

The mapping from keywords such as **routine** and **priority** to a precedence value is useful only in some instances. That is, the use of the precedence bit is evolving. The customer can define the meaning of a precedence value by enabling other features that use the value. In the case of Cisco high-end Internet quality of service (QoS), IP precedences can be used to establish classes of service that do not necessarily correspond numerically to better or worse handling in the network. For example, IP Precedence 2 can be given 90 percent of the bandwidth on output links in the network, and IP Precedence 6 can be given 5 percent using the distributed weight fair queueing (DWFQ) implementation on the Versatile Interface Processors (VIPs).

Use the **route-map** global configuration command with **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another, or for policy routing. Each **route-map** command has a list of **match** and **set** commands associated with it. The match commands specify the match criteria—the conditions under which redistribution or policy routing is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution or policy routing actions to perform if the criteria enforced by the match commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution set actions to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

The following example sets the IP Precedence value to 5 (critical) for packets that pass the route map match:

```
interface serial 0
 ip policy route-map texas
!
route-map texas
 match length 68 128
 set ip precedence 5
```

Related Commands

Command	Description
fair-queue (WFQ)	Enables WFQ for an interface.
ip policy route-map	Identifies a route map to use for policy routing on an interface.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

set level (IP)

To indicate where to import routes, use the **set level** command in route-map configuration mode. 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.

Defaults

This command is disabled by default.

For Intermediate System-to-Intermediate System (IS-IS) destinations, the default value is **level-2**. For OSPF destinations, the default value is **backbone**.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution *set actions* to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

In the following example, routes will be imported into the Level 1 area:

```
route-map name
 set level level-l
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community-list	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP communities attribute.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.
show route-map	Displays all route maps configured or only the one specified.

set local-preference

To specify a preference value for the autonomous system path, use the **set local-preference** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set local-preference *number-value*

no set local-preference *number-value*

Syntax Description

number-value	Preference value. An integer from 0 to 4294967295.

Defaults

Preference value of 100

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The preference is sent only to all routers in the local autonomous system.

You must have a match clause (even if it points to a "permit everything" list) if you want to set tags.

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution *set actions* to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

You can change the default preference value with the **bgp default local-preference** command.

Examples

The following example sets the local preference to 100 for all routes that are included in access list 1:

```
route-map map-preference
 match as-path 1
 set local-preference 100
```

Related Commands

Command	Description
bgp default local-preference	Changes the default local preference value.
match as-path	Matches a BGP autonomous system path access list.
match community-list	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set origin (BGP)	Sets the BGP origin code.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

set metric (BGP, OSPF, RIP)

To set the metric value for a routing protocol, use the **set metric** command in route-map configuration mode. 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

metric-value	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).

Defaults

The dynamically learned metric value.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

We recommend that you consult your Cisco technical support representative before changing the default value.

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution *set actions* to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

The following example sets the metric value for the routing protocol to 100:

```
route-map set-metric
 set metric 100
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community-list	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.
show route-map	Displays all route maps configured or only the one specified.

set metric-type

To set the metric type for the destination routing protocol, use the **set metric-type** command in route-map configuration mode. 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, or IGP metric as the MED for BGP.
external	IS-IS external metric.
type-1	Open Shortest Path First (OSPF) external Type 1 metric.
type-2	OSPF external Type 2 metric.

Defaults

This command is disabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use the **route-map** global configuration command with **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution *set actions* to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

The following example sets the metric type of the destination protocol to OSPF external Type 1:

```
route-map map-type
 set metric-type type-1
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community-list	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.
show route-map	Displays all route maps configured or only the one specified.

set next-hop

To specify the address of the next hop, use the **set next-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set next-hop *next-hop*

no set next-hop *next-hop*

Syntax Description

next-hop	IP address of the next hop router.

Defaults

Default next hop address.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You must have a match clause (even if it points to a “permit everything” list) if you want to set tags.

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution *set actions* to be performed when all the match criteria of the router are met. When all match criteria are met, all set actions are performed.

Examples

In the following example, routes that pass the access list have the next hop set to 172.160.70.24:

```
route-map map_hop
 match address 5
 set next-hop 172.160.70.24
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community-list	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.
show route-map	Displays all route maps configured or only the one specified.

set tag (IP)

To set a tag value of the destination routing protocol, use the **set tag** command in route-map configuration mode. To delete the entry, use the **no** form of this command.

set tag *tag-value*

no set tag *tag-value*

Syntax Description

tag-value	Name for the tag. Integer from 0 to 4294967295.

Defaults

If not specified, the default action is to *forward* the tag in the source routing protocol onto the new destination protocol.

Command Modes

Route-map configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution *set actions* to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

The following example sets the tag value of the destination routing protocol to 5:

```
route-map tag
 set tag 5
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community-list	Matches a BGP community.
match interface (IP)	Distributes any routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set tag (IP)	Sets a tag value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.
show route-map	Displays all route maps configured or only the one specified.

show ip cache policy

To display the cache entries in the policy route cache, use the **show ip cache policy** command in EXEC mode.

show ip cache policy

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3	This command was introduced.

Examples

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

```
Router# show ip cache policy

Total adds 10, total deletes 10

Type Routemap/sequence      Age       Interface       Next Hop
NH   george/10              00:04:31  Ethernet0       172.110.1.2
Int  george/30              00:01:23  Serial4         172.110.5.129
```

Table 49 describes the significant fields shown in the display.

Table 49 show ip cache policy Field Descriptions

Field	Description
Total adds	Number of times a cache entry was created.
total deletes	Number of times a cache entry or the entire cache was deleted.
Type	"NH" indicates the **set ip next-hop** command. "Int" indicates the **set interface** command.
Routemap	Name of the route map that created the entry; in this example, george.
sequence	Route map sequence number.
Age	Age of the cache entry.
Interface	Output interface type and number.
Next Hop	IP address of the next hop.

Related Commands

Command	Description
ip route-cache	Configures the router to export the flow cache entry to a workstation when a flow expires.

show ip local policy

To display the route map used for local policy routing, if any, use the **show ip local policy** command in EXEC mode.

show ip local policy

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.

Examples

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

```
Router# show ip local policy

Local policy routing is enabled, using route map equal
route-map equal, permit, sequence 10
  Match clauses:
    length 150 200
  Set clauses:
    ip next-hop 10.10.11.254
  Policy routing matches: 0 packets, 0 bytes
route-map equal, permit, sequence 20
  Match clauses:
    ip address (access-lists): 101
  Set clauses:
    ip next-hop 10.10.11.14
  Policy routing matches: 2 packets, 172 bytes
```

Table 50 describes the significant fields shown in the display.

Table 50 show ip local policy Field Descriptions

Field	Description
route-map equal	The name of the route map is equal.
permit	The route map contains permit statements.
sequence	The sequence number of the route map, which determines in what order it is processed among other route maps.
Match clauses:	Clauses in the route map that must be matched to satisfy the permit or deny action.
Set clauses:	Set clauses that will be put into place if the match clauses are met.
Policy routing matches: packets	Number of packets that meet the match clauses.
bytes	Number of bytes in the packets that meet the match clauses.

Related Commands

Command	Description
ip local policy route-map	Identifies a route map to use for local policy routing.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.
set ip default next-hop verify-availability	Indicates 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.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.

show ip policy

To display the route map used for policy routing, use the **show ip policy** command in EXEC mode.

show ip policy

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.

Examples

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

```
Router# show ip policy

Interface      Route map
local          equal
Ethernet0      equal
```

The following is sample output from the **show route-map** command, which relates to the preceding sample display:

```
Router# show route-map

route-map equal, permit, sequence 10
  Match clauses:
    length 150 200
  Set clauses:
    ip next-hop 10.10.11.254
  Policy routing matches: 0 packets, 0 bytes
route-map equal, permit, sequence 20
  Match clauses:
    ip address (access-lists): 101
  Set clauses:
    ip next-hop 10.10.11.14
  Policy routing matches: 144 packets, 15190 bytes
```

Table 51 describes the significant fields shown in the display.

Table 51 show ip policy Field Descriptions

Field	Description
route-map equal	The name of the route map is equal.
permit	The route map contains permit statements.
sequence	Sequence number of the route map, which determines in what order it is processed among other route maps.

Table 51 show ip policy Field Descriptions (continued)

Field	Description
Match clauses:	Clauses in the route map that must be matched to satisfy the permit or deny action.
Set clauses:	Set clauses that will be put into place if the match clauses are met.
Policy routing matches: packets	Number of packets that meet the match clauses.
bytes	Number of bytes in the packets that meet the match clauses.

Related Commands

Command	Description
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.
set ip default next-hop verify-availability	Indicates 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.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.

show ip protocols

To display the parameters and current state of the active routing protocol process, use the **show ip protocols** command in EXEC mode.

show ip protocols

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The information displayed by the **show ip protocols** command is useful in debugging routing operations. Information in the Routing Information Sources field of the **show ip protocols** output can help you identify a router suspected of delivering bad routing information.

Examples

The following is sample output from the **show ip protocols** command, showing Interior Gateway Routing Protocol (IGRP) processes:

```
Router# show ip protocols

Routing Protocol is "igrp 109"
  Sending updates every 90 seconds, next due in 44 seconds
  Invalid after 270 seconds, hold down 280, flushed after 630
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  IGRP maximum hopcount 100
  IGRP maximum metric variance 1
  Redistributing: igrp 109
  Routing for Networks:
    172.160.72.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.160.72.18         100      0:56:41
    172.160.72.19         100      6d19
    172.160.72.22         100      0:55:41
    172.160.72.20         100      0:01:04
    172.160.72.30         100      0:01:29
  Distance: (default is 100)

Routing Protocol is "bgp 1878"
  Sending updates every 60 seconds, next due in 0 seconds
  Outgoing update filter list for all interfaces is 1
  Incoming update filter list for all interfaces is not set
  Redistributing: igrp 109
```

```
 IGP synchronization is disabled
 Automatic route summarization is enabled
 Neighbor(s):
   Address          FiltIn FiltOut DistIn DistOut Weight RouteMap
   192.108.211.17                1
   192.108.213.89                1
   198.6.255.13                  1
   172.160.72.18                  1
   172.160.72.19
   172.160.84.17                  1
 Routing for Networks:
   192.108.209.0
   192.108.211.0
   198.6.254.0
 Routing Information Sources:
   Gateway         Distance      Last Update
   172.160.72.19          20      0:05:28
 Distance: external 20 internal 200 local 200
```

Table 52 describes the significant fields shown in the display.

Table 52 show ip protocols Field Descriptions for IGRP Processes

Field	Description
Routing Protocol is “igrp 109”	Specifies the routing protocol used.
Sending updates every 90 seconds	Specifies the time between sending updates.
next due in 44 seconds	Precisely when the next update is due to be sent.
Invalid after 270 seconds	Specifies the value of the invalid parameter.
hold down for 280	Specifies the current value of the hold-down parameter.
flushed after 630	Specifies the time (in seconds) after which the individual routing information will be thrown (flushed) out.
Outgoing update ...	Specifies whether the outgoing filtering list has been set.
Incoming update ...	Specifies whether the incoming filtering list has been set.
Default networks	Specifies how these networks will be handled in both incoming and outgoing updates.
IGRP metric	Specifies the value of the K0-K5 metrics, and the maximum hop count.
Redistributing	Lists the protocol that is being redistributed.
Routing	Specifies the networks for which the routing process is currently injecting routes.
Routing Information Sources	Lists all the routing sources the Cisco IOS software is using to build its routing table. For each source, you will see the following displayed: • IP address • Administrative distance • Time the last update was received from this source

The following is sample output from the **show ip protocols** command, showing Enhanced IGRP processes:

```
Router# show ip protocols

Routing Protocol is "eigrp 77"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: eigrp 77
  Automatic network summarization is in effect
  Routing for Networks:
    172.180.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.180.81.28          90      0:02:36
    172.180.80.28          90      0:03:04
    172.180.80.31          90      0:03:04
  Distance: internal 90 external 170
```

Table 53 describes the significant fields shown in the display.

Table 53 show ip protocols Field Descriptions for Enhanced IGRP Processes

Field	Description
Routing Protocol is "eigrp 77"	Name and autonomous system number of the currently running routing protocol.
Outgoing update filter list for all interfaces...	Indicates whether a filter for outgoing routing updates has been specified with the **distribute-list out** command.
Incoming update filter list for all interfaces...	Indicates whether a filter for incoming routing updates has been specified with the **distribute-list in** command.
Redistributing: eigrp 77	Indicates whether route redistribution has been enabled with the **redistribute** command.
Automatic network summarization...	Indicates whether route summarization has been enabled with the **auto-summary** command.
Routing for Networks:	Networks for which the routing process is currently injecting routes.
Routing Information Sources:	Lists all the routing sources that the Cisco IOS software is using to build its routing table. The following is displayed for each source: • IP address • Administrative distance • Time the last update was received from this source
Distance: internal 90 external 170	Internal and external distances of the router. Internal distance is the degree of preference given to Enhanced IGRP internal routes. External distance is the degree of preference given to Enhanced IGRP external routes.

The following is sample output from the **show ip protocols** command, showing Intermediate System-to-Intermediate System (IS-IS) processes:

```
Router# show ip protocols

Routing Protocol is "isis"
  Sending updates every 0 seconds
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: isis
  Address Summarization:
    None
  Routing for Networks:
    Serial0
  Routing Information Sources:
  Distance: (default is 115)
```

The following is sample output from the **show ip protocols** command, showing Routing Information Protocol (RIP) processes:

```
Router# show ip protocols

Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 2 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
    Ethernet0        2     2      trees
    Fddi0            2     2
  Routing for Networks:
    172.19.0.0
    2.0.0.0
    10.3.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 120)
```

show ip route

To display the current state of the routing table, use the **show ip route** command in EXEC mode.

show ip route [[*ip-address* [*mask*] [**longer-prefixes**]] | [*protocol* [*process-id*]] | [**list** access-list-number | access-list-name]]

Syntax Description

ip-address	(Optional) Address about which routing information should be displayed.
mask	(Optional) Argument for a subnet mask.
longer-prefixes	(Optional) Specifies that only routes matching the *ip-address* and *mask* pair should be displayed.
protocol	(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**.
process-id	(Optional) Number used to identify a process of the specified protocol.
list	(Optional) The **list** keyword is required to filter output by an access list name or number.
access-list-name	(Optional) Filters the displayed output from the routing table based on the specified access list name.
access-list-number	(Optional) Filters the displayed output from the routing table based on the specified access list number.

Command Modes

EXEC

Command History

Release	Modification
9.2	This command was introduced.
10.0	The “D—EIGRP, EX—EIGRP, N1—OSPF NSSA external type 1 route” and “N2—OSPF NSSA external type 2 route” codes were added to the command output.
10.3	The *process-id* argument was added.
11.0	The **longer-prefixes** keyword was added.
11.1	The “U—per-user static route” code was added to the command output.
11.2	The “o—on-demand routing” code was added to the command output.
11.3	The output from the **show ip route** *ip-address* command was enhanced to display the origination of an IP route in Intermediate System-to-Intermediate System (IS-IS) networks.
12.0(1)T	The “M—mobile” code was added to the command output.
12.0(3)T	The “P—periodic downloaded static route” code was added to the command output.
12.0(4)T	The “ia—IS-IS” code was added to the command output.

Examples

The following is sample output from the **show ip route** command when entered without an address:

```
Router# show ip route

Codes: I - IGRP derived, R - RIP derived, O - OSPF derived,
       C - connected, S - static, E - EGP derived, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is 10.119.254.240 to network 10.140.0.0

O E2 172.150.0.0 [160/5] via 10.119.254.6, 0:01:00, Ethernet2
E    172.17.10.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
O E2 172.70.132.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
O E2 10.130.0.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
E    172.30.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.129.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E    172.80.129.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.10.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    172.60.139.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    172.90.208.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    192.84.148.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    192.168.223.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    192.44.236.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.141.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E    141.140.0.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
```

The following is sample output that includes IS-IS Level 2 routes learned:

```
Router# show ip route

Codes: I - IGRP derived, R - RIP derived, O - OSPF derived,
       C - connected, S - static, E - EGP derived, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is not set

     172.180.0.0 is subnetted (mask is 255.255.255.0), 3 subnets
C       172.180.64.0 255.255.255.0 is possibly down,
          routing via 0.0.0.0, Ethernet0
i L2    172.180.67.0 [115/20] via 172.180.64.240, 0:00:12, Ethernet0
i L2    172.180.66.0 [115/20] via 172.180.64.240, 0:00:12, Ethernet0
```

Table 54 describes the significant fields shown in the displays.

Table 54 show ip route Field Descriptions

Field	Description
O	Indicates protocol that derived the route. Possible values include the following: I—Interior Gateway Routing Protocol (IGRP) derived R—Routing Information Protocol (RIP) derived O—Open Shortest Path First (OSPF) derived C—connected S—static E—Exterior Gateway Protocol (EGP) derived B—Border Gateway Protocol (BGP) derived D—Enhanced Interior Gateway Routing Protocol (EIGRP) EX—EIGRP external i—IS-IS derived ia—IS-IS M—mobile P—periodic downloaded static route U—per-user static route o—on-demand routing
E2	Type of route. Possible values include the following: *—Indicates the last path used when a packet was forwarded. It pertains only to the nonfast-switched packets. However, it does not indicate which path will be used next when forwarding a nonfast-switched packet, except when the paths are equal cost. IA—OSPF interarea route E1—OSPF external type 1 route E2—OSPF external type 2 route L1—IS-IS Level 1 route L2—IS-IS Level 2 route N1—OSPF not-so-stubby area (NSSA) external Type 1 route N2—OSPF NSSA external Type 2 route
172.150.0.0	Indicates the address of the remote network.
[160/5]	The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route.
via 10.119.254.6	Specifies the address of the next router to the remote network.
0:01:00	Specifies the last time the route was updated, in hours:minutes:seconds.
Ethernet2	Specifies the interface through which the specified network can be reached.

When you specify that you want information about a specific network displayed, more detailed statistics are shown. The following is sample output from the **show ip route** command when entered with the address 10.119.0.0:

```
Router# show ip route 10.119.0.0

Routing entry for 10.119.0.0 (mask 255.255.0.0)
   Known via "igrp 109", distance 100, metric 10989
   Tag 0
   Redistributing via igrp 109
   Last update from 10.108.35.13 on TokenRing0, 0:00:58 ago
   Routing Descriptor Blocks:
   * 10.108.35.13, from 10.108.35.13, 0:00:58 ago, via TokenRing0
      Route metric is 10989, traffic share count is 1
      Total delay is 45130 microseconds, minimum bandwidth is 1544 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 2/255, Hops 4
```

When an IS-IS router advertises its link-state information, it includes one of its own IP addresses to be used as the originator IP address. When other routers calculate IP routes, they can store the originator IP address with each route in the routing table.

The following example shows the output from the **show ip route** command when looking at an IP route generated by IS-IS. Each path that is shown under the Routing Descriptor Blocks report displays two IP addresses. The first address (10.22.22.2) is the next hop address, the second is the originator IP address from the advertising IS-IS router. This address helps you determine where a particular IP route has originated in your network. In the example the route to 10.0.0.1/32 was originated by a router with IP address 223.191.255.247.

```
Router# show ip route 10.0.0.1

Routing entry for 10.0.0.1/32
    Known via "isis", distance 115, metric 20, type level-1
    Redistributing via isis
    Last update from 223.191.255.251 on Fddi1/0, 00:00:13 ago
    Routing Descriptor Blocks:
    * 10.22.22.2, from 223.191.255.247, via Serial2/3
       Route metric is 20, traffic share count is 1
       223.191.255.251, from 223.191.255.247, via Fddi1/0
       Route metric is 20, traffic share count is 1
```

Compare the report using the **show ip route** command with an IP address to the following report using the **show ip route isis** command:

```
Router# show ip route isis

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
  i L1    10.0.0.1/32 [115/20] via 10.22.22.2, Serial2/3
                [115/20] via 223.191.255.251, Fddi1/0
    22.0.0.0/24 is subnetted, 2 subnets
i L1    22.22.23.0 [115/20] via 223.191.255.252, Fddi1/0
```

Table 55 describes the significant fields shown when using the **show ip route** command with an IP address (previous displays).

Table 55 show ip route with Address Field Descriptions

Field	Description
Routing entry for 10.119.0.0 (mask 255.255.0.0)	Network number and mask.
Known via ...	Indicates how the route was derived.
distance	Administrative distance of the information source.
Tag	Integer that is used to implement the route.
Redistributing via ...	Indicates the redistribution protocol.
Last update from 10.108.35.13 on ...	Indicates the IP address of a router that is the next hop to the remote network and the router interface on which the last update arrived.
0:00:58 ago	Specifies the last time the route was updated, in hours:minutes:seconds.
Routing Descriptor Blocks:	Displays the next hop IP address followed by the information source.
10.108.35.13, from 10.108.35.13, 0:00:58 ago	Indicates the next hop address, the address of the gateway that sent the update, and the time that has elapsed since this update was received, in hours:minutes:seconds.
from...via ...	The first address is the next hop IP address, and the other is the information source. This report is followed by the interface for this route.
Route metric	This value is the best metric for this routing descriptor block.
traffic share count	Number of uses for this routing descriptor block.
Total delay	Total propagation delay (in microseconds).
minimum bandwidth	Minimum bandwidth encountered when sending data along this route.
Reliability 255/255	Likelihood of successful packet transmission expressed as a number from 0 to 255 (255 is 100 percent reliability).
minimum MTU	Smallest maximum transmission unit (MTU) along the path.
Loading 2/255	Effective bandwidth of the route in kbps/255 is saturation.
Hops	Number of hops to the destination or to the router where the route first enters IGRP.

The following is sample output using the **longer-prefixes** keyword. When the **longer-prefixes** keyword is included, the address and mask pair becomes the prefix, and any address that matches that prefix is displayed. Therefore, multiple addresses are displayed.

In the following example, the logical AND operation is performed on the source address 128.0.0.0 and the mask 128.0.0.0, resulting in 128.0.0.0. Each destination in the routing table is also logically ANDed with the mask and compared to that result of 128.0.0.0. Any destinations that fall into that range are displayed in the output.

```
Router# show ip route 128.0.0.0 128.0.0.0 longer-prefixes

Codes: I - IGRP derived, R - RIP derived, O - OSPF derived,
       C - connected, S - static, E - EGP derived, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is not set

S    10.134.0.0 is directly connected, Ethernet0
S    10.10.0.0 is directly connected, Ethernet0
S    10.129.0.0 is directly connected, Ethernet0
S    172.30.0.0 is directly connected, Ethernet0
S    172.40.246.0 is directly connected, Ethernet0
S    172.20.97.0 is directly connected, Ethernet0
S    172.50.88.0 is directly connected, Ethernet0
S    172.19.141.0 is directly connected, Ethernet0
S    172.60.138.0 is directly connected, Ethernet0
S    192.44.237.0 is directly connected, Ethernet0
S    192.168.222.0 is directly connected, Ethernet0
S    172.90.209.0 is directly connected, Ethernet0
S    10.145.0.0 is directly connected, Ethernet0
S    10.141.0.0 is directly connected, Ethernet0
S    10.138.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
     172.19.0.0 255.255.255.0 is subnetted, 1 subnets
C       172.19.64.0 is directly connected, Ethernet0
     172.110.0.0 is variably subnetted, 2 subnets, 2 masks
C       172.110.232.32 255.255.255.240 is directly connected, Ethernet0
S       172.110.0.0 255.255.0.0 is directly connected, Ethernet0
Router#
```

Related Commands

Command	Description
show interfaces tunnel	Displays a list of tunnel interface information.
show ip route summary	Displays the current state of the routing table in summary format.

show ip route summary

To display the current state of the routing table, use the **show ip route summary** command in EXEC mode.

show ip route summary

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

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

```
Router# show ip route summary

Route Source    Networks    Subnets     Overhead    Memory (bytes)
connected       0           3           126         360
static          1           2           126         360
igrp 109        747         12          31878       91080
internal        3                                   360
Total           751         17          32130       92160
```

Table 56 describes the significant fields shown in the display.

Table 56 show ip route summary Field Descriptions

Field	Description
Route Source	Routing protocol name, or the **connected, static,** or **internal** keyword. "Internal" indicates those routes that are in the routing table that are not owned by any routing protocol.
Networks	Number of prefixes that are present in the routing table for each route source.
Subnets	Number of subnets that are present in the routing table for each route source, including host routes.
Overhead	Any additional memory involved in allocating the routes for the particular route source other than the memory specified in the Memory field.
Memory	Number of bytes allocated to maintain all the routes for the particular route source.

Related Commands

Command	Description
show ip route	Displays the current state of the routing table.

show ip route supernets-only

To display information about supernets, use the **show ip route supernets-only** privileged command in EXEC mode.

show ip route supernets-only

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show ip route supernets-only** command. This display shows supernets only; it does not show subnets.

```
Router# show ip route supernets-only

Codes: I - IGRP derived, R - RIP derived, O - OSPF derived
       C - connected, S - static, E - EGP derived, B - BGP derived
       i - IS-IS derived, D - EIGRP derived
       * - candidate default route, IA - OSPF inter area route
       E1 - OSPF external type 1 route, E2 - OSPF external type 2 route
       L1 - IS-IS level-1 route, L2 - IS-IS level-2 route
       EX - EIGRP external route

Gateway of last resort is not set

B    172.160.0.0 (mask is 255.255.0.0) [20/0] via 172.160.72.30, 0:00:50
B    192.0.0.0 (mask is 255.0.0.0) [20/0] via 172.160.72.24, 0:02:50
```

Table 57 describes the significant fields shown in the display.

Table 57 show ip route supernets-only Field Descriptions

Field	Description
B	Border Gateway Protocol (BGP) derived, as shown in list of codes.
172.160.0.0 (mask is 255.255.0.0)	Supernet IP address.
[20/0]	Administrative distance (external/internal).
via 172.160.72.30	Next hop IP address.
0:00:50	Age of the route (how long ago the update was received).

show key chain

To display authentication key information, use the **show key chain** command in EXEC mode.

show key chain [*name-of-chain*]

Syntax Description

name-of-chain	(Optional) Name of the key chain to display, as named in the **key chain** command.

Defaults

Information about all key chains is displayed.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.

Examples

The following is sample output from the **show key chain** command:

```
Router# show key chain

Key-chain trees:
    key 1 -- text "chestnut"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
    key 2 -- text "birch"
        accept lifetime (00:00:00 Dec 5 1995) - (23:59:59 Dec 5 1995)
        send lifetime (06:00:00 Dec 5 1995) - (18:00:00 Dec 5 1995)
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

show route-map

To display configured route maps, use the **show route-map** command in EXEC mode.

show route-map [*map-name*]

Syntax Description

map-name	(Optional) Name of a specific route map.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following is sample output from the **show route-map** command:

```
Router# show route-map

route-map abc, permit, sequence 10
  Match clauses:
    tag 1 2
  Set clauses:
    metric 5
route-map xyz, permit, sequence 20
  Match clauses:
    tag 3 4
  Set clauses:
    metric 6
```

Table 58 describes the significant fields shown in the display.

Table 58 show route-map Field Descriptions

Field	Description
route-map	Name of the route map.
permit	Indicates that the route is redistributed as controlled by the set actions.
sequence	Number that indicates the position a new route map is to have in the list of route maps already configured with the same name.
Match clauses tag	Match criteria—conditions under which redistribution is allowed for the current route map.
Set clauses metric	Set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met.

Related Commands

Command	Description
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

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** command in EXEC mode.

show route-map ipc

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

This command displays the counts of one-way route map IPC messages from the RP to the VIP when NetFlow policy routing is configured. If you execute this command on the RP, the messages are shown as “Sent.” If you execute this command on the VIP console, the IPC messages are shown as “Received.”

Examples

The following is sample output from the **show route-map ipc** command when it is executed on the RP:

```
Router# show route-map ipc

Route-map RP IPC Config Updates Sent
Name: 4
Match access-list: 2
Match length: 0
Set precedence: 1
Set tos: 0
Set nexthop: 4
Set interface: 0
Set default nexthop: 0
Set default interface: 1
Clean all: 2
```

The following is sample output from the **show route-map ipc** command when it is executed on the VIP:

```
VIP-Slot0# show route-map ipc

Route-map LC IPC Config Updates Received
Name: 4
Match access-list: 2
Match length: 0
Set precedence: 1
Set tos: 0
Set nexthop: 4
Set interface: 0
Set default nexthop: 0
Set default interface: 1
Clean all: 2
```

Table 59 describes the significant fields shown in the first display.

Table 59 show route-map ipc Field Descriptions

Field	Description
Route-map RP IPC Config Updates Sent	IPC messages are being sent from the RP to the VIP.
Name:	Number of IPC messages sent about the name of the route map.
Match access-list:	Number of IPC messages sent about the access list.
Match length:	Number of IPC messages sent about the length to match.
Set precedence:	Number of IPC messages sent about the precedence.
Set tos:	Number of IPC messages sent about the type of service (ToS).
Set nexthop:	Number of IPC messages sent about the next hop.
Set interface:	Number of IPC messages sent about the interface.
Set default nexthop:	Number of IPC messages sent about the default next hop.
Set default interface:	Number of IPC messages sent about the default interface.
Clean all:	Number of IPC messages sent about clearing the policy routing configuration from the VIP. When distributed Cisco express forwarding (DCEF) is disabled and reenabled, the configuration related to policy routing must be removed (cleaned) from the VIP before the new information is downloaded from the RP to the VIP.

Related Commands

Command	Description
set ip next-hop verify-availability	Configures policy routing to verify if the next hops of a route map are CDP neighbors before policy routing to that next hop.

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** command in router configuration mode. 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.

Defaults

Traffic is configured to use minimum cost paths.

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
11.0(3)	This command became protocol independent when the **across-interfaces** keyword was added.

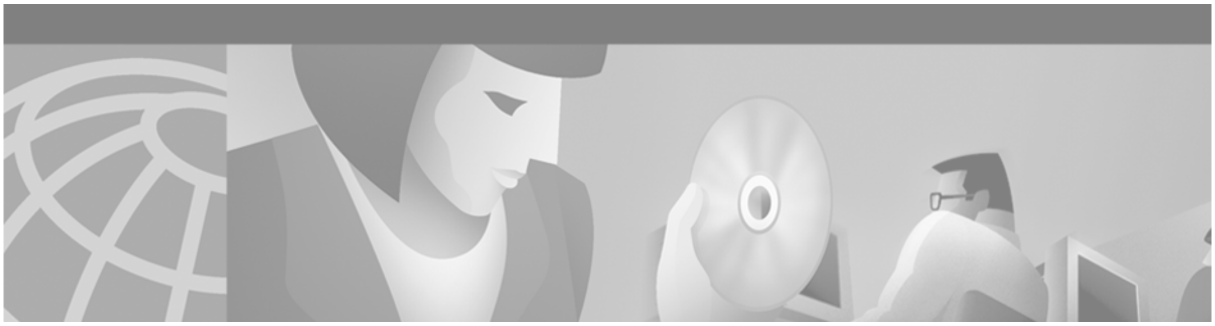
Usage Guidelines

The **traffic-share min** command causes the Cisco IOS software to divide traffic only among the routes with the best metric. Other routes will remain in the routing table, but will receive no traffic. Configuring this command with the **across-interfaces** keyword allows you to configure multi-interface load splitting on different interfaces with equal cost paths.

Examples

In the following example, multi-interface load splitting is configured on different interfaces with equal cost paths:

```
router ospf 5
 traffic-share min across-interfaces
```



INDEX

Symbols

A

B

K

L

M

N

O

S

T

U

V